Módulo 4. Introducción al análisis de auditoría y forense

CÓRDOBA CREA FUTURO

"**El tiempo que pasa es la verdad que huye**" (Locard, como se citó en Escalona Acuña, 2014, https://n9.cl/b8k413). Esta frase aplicada al ámbito digital podría no tener el mismo impacto que tenía en su origen. Cierta evidencia digital puede ser clonada repetidamente y conservada intacta por un largo período de tiempo mediante la realización de la copia bit a bit de discos duros, tarjetas de memoria, pendrives, etc. Por medio del código *hash* es posible comprobar la autenticidad y originalidad de la información.

Cuando un evento de ciberseguridad es detectado en una organización, todo lo que involucra al mismo, es posible que se transforme en evidencia digital. Como en casi todos los casos, las medias preventivas en la planificación y organización en el armado de la red, servidor, *backups*, información, etc., es decir, lo que involucra a la infraestructura crítica en general, si es debidamente calculada considerando la posibilidad de éxito del mayor riesgo posible, aceleran la investigación forense y mejora la *performance* de todo el proceso de un peritaje ya que la preservación de la información, su análisis, etc. es crítico en sistemas de tiempo real.

En este sentido, **aunque no siempre sea posible evitar un ciberataque se concrete, sí podemos procurar una rápida recuperación del sistema**. La necesidad de realizar un análisis forense sobre equipos que han sufrido algún

tipo ciberataque en sistemas de tiempo real como bancos comerciales, aerolíneas de aviación, hospitales, etc., debe ser realizada evitando que el mismo provoque una operación traumática que deje fuera de línea o ralentice el sistema. Para ello, es necesario que las medidas de contingencia proactivas estén adecuadamente documentadas y que consideren los distintos escenarios posibles con sus debidas soluciones que permitan la recuperación del sistema en el menor tiempo posible. La medición del tiempo debe ser coordinada con la organización a efectos de llevar a cabo la simulación y efectividad del proceso de recuperación del sistema que deberá tener la evidencia digital para una intervención pericial en caso de ser necesario.

Esta previsión no solo permitiría continuar con el normal funcionamiento de la organización, sino que el inicio de la pericia informática, al formar parte de ese plan de trabajo, permitiría que el sistema siga trabajando normalmente, y quedará disponible toda la documentación necesaria.

La pericia informática puede ser iniciada por varias motivaciones:

- La necesidad de una organización.
- Un particular para iniciar un juicio.
- Solicitud de un juez.
- Etc.

La pericia informática por parte de un organismo oficial del poder judicial es lo más frecuente en estos casos, donde equipos que han sido secuestrados por personal policial son analizados cumpliendo un pedido de un juez. En estos casos, las pericias informáticas se realizan en dispositivos móviles tales como celulares, computadoras, *notebooks*, impresoras, redes sociales, sistemas de mensajería, etc.

También se realizan peritajes informáticos solicitados por particulares. Algunos de estos casos escalan hasta llegar a la justicia como denuncias o son acompañados en informes que solicitan los abogados para respaldar su estrategia.

1. Medidas de protección recomendadas

Medidas de protección recomendadas

Para trabajar de manera preventiva en sistemas de tiempo real, es recomendable basarse en normas y guías estándares de protección que se utilizan en las amenazas; algunos son:

- ISO/IEC 27002:2014. Código de prácticas para controles de seguridad de la información.
- ISO/IEC 27033:2012. Guía para diseño e implementación de seguridad en Red.
- ISO/IEC 27034:2011. Seguridad en Aplicaciones.
- ISACA COBIT v.5:2012. Seguridad de la Información. Objetivos de control.
- MAGERIT v.3:2012. Libro 1 – Método. Capítulo 6. Catálogo de Elementos.

- NIST Cibersecurity Framework. Guías y Prácticas para infraestructuras críticas.
- PCI-DSS v.3.2:2016. Industria de Tarjetas de Pago. Normas de Seguridad de Datos.
- ITIL v3:2011. Capítulo 3.4 - Gestión de la Seguridad.

Seleccionando los elementos

Ya que la cantidad de elementos a proteger puede formar parte de una gran cantidad de elementos a tener en cuenta, para ser eficientes, es necesario realizar una selección que tenga en cuenta aspectos importantes, por ejemplo, centrarse en las amenazas que presentan mayor probabilidad de concretarse y las que requieren medidas de seguridad.

Cada activo requiere medidas específicas de seguridad; por ende, es necesario clasificarlas y centrarse en aquellos que se consideren más valiosos y dejar de lado los menos relevantes. Por otro lado, las medidas de seguridad deben ser auditadas y lo realizado debe contar con los parámetros cuantificables que permitan evaluar el grado de eficacia.

Esto nos conduce hacia dos tipos de definiciones para excluir una cierta medida del conjunto de las que conviene analizar:

- No aplica. Cuando una medida no es oportuna dado que técnicamente es inadecuada al activo que se pretende proteger, no ofrece el servicio de seguridad necesario o no ofrece seguridad ante la amenaza evaluada.
- No se justifica. Cuando la medida ofrece la protección pretendida, pero su implementación implica recursos superiores al valor del activo que se pretende proteger.

Al considerar estos aspectos, se dispondrá de una **declaración de aplicabilidad** de medidas que deben ser analizadas como posibles componentes del sistema de protección.

Efectos de las medidas de protección

El cálculo de riesgo en este contexto tiene medidas de protección que afectan de dos maneras (Ministerio de Hacienda y Administraciones Públicas, 2012):

1. Reducen la probabilidad de las amenazas. Se conocen como medidas preventivas. Las medidas ideales tienen la capacidad de impedir la materialización de la amenaza.

2. Limitan el daño provocado. Existen medidas que limitan la posible degradación, mientras que otras permiten detectar el ataque y evitar que la degradación se profundice. Existen

> medidas que se limitan a realizar una restauración del sistema en caso de que una amenaza lo destruya.

"En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan". (Ruge Pinzon, 2011, p. 43).

Tipos de medidas de protección

Conocer qué tipo de protección otorga una medida determinada permite entender de qué forma se aborda una amenaza. La siguiente tipificación es muy útil para reconocer cada tipología.

Tabla 1: Tipos de medidas de protección

Categoría	Descripción
Prevención	Se considera preventiva toda medida orientada a disminuir la probabilidad de que un incidente llegue a producirse.
Disuasión	Una medida cumple una función disuasoria cuando genera un efecto inhibidor en los potenciales atacantes, desalentando la ejecución del ataque.

Eliminación	Una medida elimina una amenaza cuando bloquea completamente la posibilidad de que esta se concrete.
Minimización o limitación del impacto	Estas medidas buscan reducir el alcance y las consecuencias negativas derivadas de la materialización de una amenaza.
Corrección	Son acciones correctivas aquellas que, una vez ocurrido el incidente, permiten subsanar o reparar el daño ocasionado.
Recuperación	Una medida de recuperación facilita el restablecimiento del sistema a las condiciones previas al evento adverso.
Monitorización	Incluye mecanismos destinados a observar y registrar de manera continua o retrospectiva el comportamiento del sistema.
Detección	Se trata de medidas que identifican un ataque en curso y alertan sobre su ocurrencia en tiempo real o cercano al evento.
Concientización	Comprende actividades de capacitación y sensibilización dirigidas a las personas que interactúan con el sistema y pueden influir en su seguridad.

Administración	Agrupa las medidas vinculadas a la gestión y mantenimiento de los elementos de seguridad que conforman el sistema.

Fuente: elaboración propia.

Pericia

La realización de una pericia informática suele exceder el área de incumbencia informática y se menciona aquí “para contar con un panorama general de las necesidades de un sistema eficiente de búsqueda y empleo de evidencia digital:

1. **Punto de contacto permanente (cf. art. 35 del Convenio de Budapest sobre cibercriminalidad)**: En el citado Convenio europeo se prevé la conformación de una red de puntos de contacto de los distintos Estados Parte, localizable las 24 horas del día, y los siete días de la semana, para asegurar la asistencia inmediata en la investigación. Sus funciones son las de aportación de consejos técnicos, la conservación de datos, la recogida de pruebas, aportación de información de carácter jurídico y localización de sospechosos. Si el punto de contacto no depende de las autoridades responsables de la cooperación internacional o de la

extradición, deberá establecerse un procedimiento acelerado que asegure la actuación coordinada. Es importante que en Argentina se establezca una red semejante en el ámbito interjurisdiccional interno y en relación con otros Estados.

2 **Analistas de información criminal**: La utilidad de esta experticia no se agota en el estudio de problemáticas delictivas y en la ayuda para establecer prioridades y estrategias en materia de políticas de persecución penal. Su empleo también puede ser muy provechoso a la hora de analizar e interpretar grandes volúmenes de datos en casos complejos, o cuando se intenta detectar patrones delictivos asociables al accionar de un grupo criminal o sospechoso, asociar casos conexos, dar consistencia al material probatorio, etc.

3 **Punto neutro judicial**: Se trata de infraestructuras únicas que permiten accesos directos a aplicaciones y bases del sistema judicial, de organismos estatales y de otras instituciones, facilitando y agilizando la obtención de información en tiempo real, la gestión de comunicaciones y solicitudes entre distintos organismos, etc.

4

Desarrolladores de herramientas de análisis forense: Su campo de acción representa un insumo para la realización de las labores regidas por este protocolo. Es especialmente necesario cuando las prestaciones del *software* de análisis disponible no abarcan determinadas tareas o no son del todo fiables". (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, 2019, p. 6)

La evidencia digital

"Puede definirse como evidencia digital al conjunto de datos e información, relevantes para una investigación, que se encuentra almacenada en o es transmitida por una computadora o dispositivo electrónico" (Ministerio Público Fiscal, 2014, p. 9).

"Se considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático (computadoras, celulares, aparatos de video digital, etc.). Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. La evidencia digital presenta características que la diferencian de las restantes clases de evidencia física. Se la puede duplicar de manera exacta (permitiendo manipular la réplica sin alterar el

original), está sujeta a riesgos específicos de posible alteración y/o eliminación, su localización puede ser muy dificultosa, entre otras.

Asimismo, el empleo de la evidencia digital en los procesos judiciales —especialmente en los casos penales— presenta complejos problemas jurídicos vinculados con el derecho a la intimidad y al secreto de las comunicaciones, las posibles afectaciones a terceras personas, etc." (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, 2019, p. 8)

Principios generales en el manejo de evidencia digital

"Existen reglas comunes que rigen la labor de los especialistas e idóneos en las diferentes fases de actuación. La evidencia digital debe poseer cuatro características esenciales: relevancia, suficiencia, validez legal y confiabilidad.

- **Relevancia**. La evidencia debe ser útil para las necesidades investigativas y/o los puntos probatorios de cada caso concreto. Ha de revestir pertinencia respecto de dichos fines y no ser sobreabundante o superflua (ver art. 338 del CPP). Este principio opera fundamentalmente como criterio de selección de evidencia. El experto debería saber qué lugar ocupa una determinada evidencia en el

plan de investigación penal y/o en la actividad de litigación del fiscal en cada caso concreto. Ante la duda, o si se estimara que podría ser útil, el especialista debe consultar con el director de la investigación, aportándole su opinión técnica.

- **Suficiencia**. Este principio complementa al anterior. Las evidencias obtenidas y eventualmente analizadas deberían ser suficientes para lograr los fines investigativos buscados mediante ellas, y/o para convencer al tribunal acerca de los puntos para los cuales fueron ofrecidas como prueba. Frente a situaciones dudosas, deberá consultarse con el director de la investigación.

- **Validez legal**. Para que la evidencia sea admisible, debe haber sido obtenida respetando las garantías y formas legales. Por ello:

  - El experto debe cumplir con las disposiciones legales y reglamentarias propias de su actuación.
  - Cuando una acción implique injerencia en derechos fundamentales (secuestro de dispositivos, análisis de comunicaciones personales, etc.), se deberá constatar la

previa autorización judicial o la orden del director de la investigación.

- No debe adoptar decisiones ni llevar a cabo acciones que sean ajenas al área de la propia incumbencia

- **Confiabilidad**. La evidencia debe ser convincente, apta para probar lo que se pretende con ella. Esto se refiere no solo a las características que una evidencia digital posee en sí misma, sino también a los procedimientos de obtención, preservación, análisis y presentación ante el tribunal. Para asegurar la confiabilidad, el proceso de manejo de evidencia digital debe ser justificable, auditable, repetible y reproducible:

  - **Justificable**: Se debe poder justificar todos los métodos y acciones realizadas en el manejo de la posible evidencia digital. La justificación puede darse demostrando que las acciones y métodos utilizados son el mejor curso de acción posible, o bien que otro especialista valide y verifique el proceso realizado.

  - **Auditable**: El especialista en adquisición (EA) y el especialista en evidencia digital (EED) deben documentar todas las

acciones que realizan y justificar todas sus decisiones en las etapas del proceso. Se busca que cualquier especialista externo (consultor o perito de parte) pueda ser capaz de evaluar el proceso y determinar si se ha aplicado una metodología, técnica o proceso adecuado.

- **Repetible**: Se deben obtener los mismos resultados si se aplica el mismo procedimiento, con las mismas herramientas, en las mismas condiciones, en cualquier momento. Si un EA o EED repite los procedimientos documentados, debe arribar a los mismos resultados que el especialista que llevó a cabo el análisis.

- **Reproducible**: Se deben obtener los mismos resultados si se aplica el mismo procedimiento, con herramientas distintas, en condiciones distintas, en cualquier momento.

A fin de cumplir con esas cuatro reglas de manejo de la evidencia digital, se han de observar las siguientes pautas:

- Debe minimizarse el manejo de la evidencia digital original con valor investigativo y/o probatorio. Si es necesario acceder a los datos originales, el especialista debe ser competente

para hacerlo y capaz de atestiguar, explicando la importancia y las implicaciones de sus acciones.

- Cualquier acción que implique una alteración irreversible de la evidencia debe ser previamente informada al director de la investigación, y debidamente documentada (ver art. 248 del CPP).

- Quien realice cada acción o cambio vinculado con evidencia digital debe responsabilizarse de lo actuado y documentarlo en forma fidedigna". (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, 2019, pp. 9-10).

Lectura sugerida

Baca Urbina, G. (2016). *Introducción a la Seguridad Informática*. Capítulo 6 (pp. 230-279). Grupo Editorial Patria. https://n9.cl/5dcgq.

Toda acción de investigación en la legislación argentina se lleva a cabo por orden judicial y la realiza un **perito informático**.

CONTINUAR

2. Digital forensics

Digital *forensics*

En esta lectura se describe la importancia del área de la ciberseguridad llamada análisis forense digital o *digital forensics* que cumple una importante función en el ámbito forense y aplica para las pericias en el quinto dominio donde, por lo general, el campo de acción se traslada a la nube.

Peritaje informático

Digital forensics (DF) es parte de la ciberseguridad y abarca distintas áreas. Se destaca, entre ellas, el análisis de *malware* que analiza la compilación y decompilación de programas ejecutables en búsquedas de rastros o indicios que indiquen la procedencia de un *malware*, su vector de ataque, modo de propagación u otros aspectos (Kundro, 2020).

Un ejemplo del trabajo que realiza el área de Digital Forensic fue el estudio del ciberataque del *ransomware wanna cry* (Latto, 2021)

que afectó a más de 150 países. También se realizan trabajos de análisis forense en servidores Cloud y locales, *hacking*, análisis de correos electrónicos, etc.

Figura 1: Peritaje informático

Fuente: elaboración propia.

El análisis forense digital (DF) también se realiza sobre casos de delitos contra la integridad sexual de menores, de evasión financiera, evasión de impuestos, propiedad intelectual, fuga o robo de información, ciberterrorismo, ciberdefensa, etc.

Perito informático

El perito informático es un auxiliar de la justicia y realiza tareas de investigación en casos ordenados por un juez. Las tareas que lleva a cabo un perito informático son variadas y se rigen por la

legislación vigente en el país en que se realiza la pericia. Su función es extraer y analizar por medio de algún *software* homologado con licencia de uso habilitante. Este *software*, por lo general, es acompañado por cierto *hardware* específico, como conectores USB que se emplean para conectarse a teléfonos móviles (celulares), discos duros, discos SSD, computadoras, *notebooks*, *tablet*s, etc. También es posible analizar las impresiones realizadas por una impresora de chorro de tinta, láser, analizar la memoria RAM, ROM, cámaras de foto, sistemas de videovigilancia, entre otros.

Una vez que el *software* extrae la información, se analiza de acuerdo a lo que indica el pedido del juez. Se suele solicitar el análisis de mensajes de texto de dos o más personas en una determinada fecha, corroborar si había contenido violento en esos mensajes, analizar las imágenes para determinar si corresponden a las publicadas en una determinada red social, etc. Una vez finalizado el trabajo, se eleva un informe al juez de la causa que lo solicitó.

En la siguiente imagen se pueden apreciar los accesorios de *hardware* que usan algunos departamentos judiciales de Argentina y que permiten conectar el dispositivo al que se le realizará la pericia con la computadora que contiene el *software* de extracción.

Figura 2: ***Hardware*** **para realizar peritaje informático**

Fuente: elaboración propia.

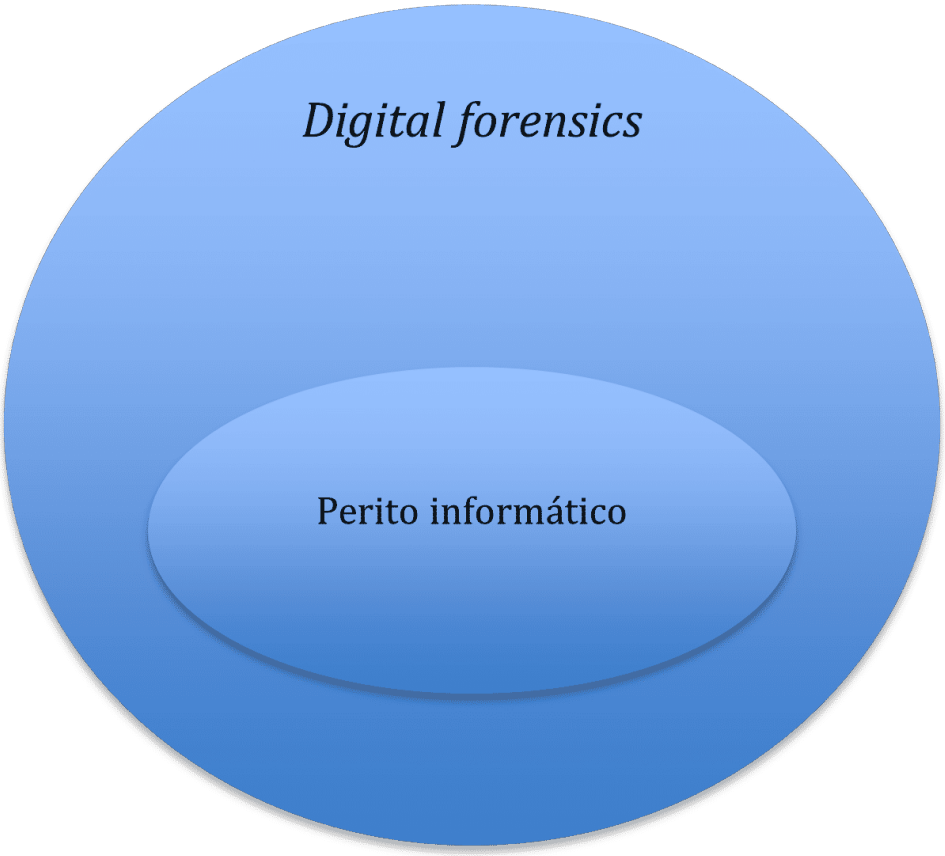
El *software* que usa un perito informático permite recuperar información almacenada, borrada de medios de almacenamiento como discos duros u otros medios de almacenamiento, que, además, pueden haber sido formateados o haberles eliminado sus particiones. Estas aplicaciones facilitan la tarea de investigación y administrativa del perito informático, ya que pueden realizar búsquedas específicas dentro de los archivos digitales que se recuperan y/o extraen, facilitan la elaboración de informes, etc.

Aprender a usar este tipo de herramientas es una tarea muy sencilla para cualquier informático.

Obligaciones del perito informático

El perito informático está obligado a cumplir con las normativas legales que rigen durante todo el proceso judicial. El trabajo inicia con la designación en la causa y, luego de analizar la misma, armará su plan de trabajo y finalizará el proceso de investigación con el informe final que se eleva al juez de una causa. El perito debe conservar discrecionalidad en todo momento de la investigación, así también de otras causas finalizadas, porque la información involucrada en la causa es considerada sensible y debe mantenerse en confidencialidad para cuidar la privacidad de las personas.

Figura 3: Rol del perito informático



Fuente: elaboración propia.

Los equipos de trabajo de *digital forensics* están formados por especialistas de varias áreas de ciberseguridad. También participan personas de distintas profesiones que enriquecen la tarea de todo el equipo. En Argentina, los peritos informáticos:

- Son los de oficio que, por lo general, pertenecen a un departamento interno de la justicia.
- Los abogados pueden solicitar que se incorporen peritos de parte, y estos, luego de

acreditar idoneidad, podrán ser aceptados por el juez.

- Los peritos designados, en conjunto, analizan e investigan la información que entrega el *software* de recuperación en busca de lo ordenado por el juez y marcan a su beneficio lo que puede serle útil a cada uno. Al final, presentan un informe que debe estar firmado por el perito.

- Realizan importantes tareas, pero no tan complejas como las de DF.

- El perito, dependiendo de la causa, podrá participar del análisis de la evidencia junto a otros profesionales de otras áreas, por ejemplo, del campo de la electrónica, comunicaciones, telecomunicaciones, etc.

Algunas agencias internacionales, tales como Europol (Oficina Europea de Policía), OEA (Organización de los Estados Americanos) y NSA (Agencia de Seguridad Nacional de los Estados Unidos), entre otras, cuentan con equipos de trabajo interdisciplinario que colaboran estrechamente en distintos asuntos delictivos.

Las acciones contra la integridad sexual de menores (pornografía infantil) pueden llegar a los juzgados argentinos por colaboración internacional de organismos de Estados Unidos que acompañan imágenes, números IP, etc. Con esta información, los juzgados suelen emitir las órdenes de allanamiento y/o detención correspondiente.

Lectura sugerida:

Del Pino, S. (s. f.). *Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0*. OAS. https://n9.cl/l4agl.

Cadena de custodia y preservación

"La cadena de custodia es una secuencia o serie de recaudos destinados a asegurar el origen, identidad e integridad de la evidencia, evitando que esta se pierda, destruya o altere. Se aplica a todo acto de aseguramiento, identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis de la evidencia, preservando su fuerza probatoria. Permite, además, hacer transparente todo eventual cambio o alteración del material probatorio. Asimismo, posibilita un mejor control de la debida reserva de aquella evidencia que pueda contener datos personales o sensibles, o correspondencia electrónica (art. 2° de la Ley nro. 25.326 de Protección de Datos Personales; arts. 18, 21, 50 de la Ley Nacional de Telecomunicaciones nro. 19.798; arts. 153 a 157 bis del Código Penal). [Deberán seguirse las orientaciones

generales establecidas en la Res. 889/15 (“Protocolo de Cadena de Custodia”) en tanto no se opongan a las contenidas en la presente Guía.]

La cadena de custodia comienza desde el momento de hallazgo o recepción de la evidencia y finaliza cuando la autoridad judicial competente decida sobre su destino.

> La individualización y preservación de evidencia informática forense presenta particularidades y requerimientos específicos. Es necesario adoptar recaudos no solo sobre dispositivos o artefactos, sino además sobre la evidencia digital. Esta última puede estar contenida en aquellos o ser extraída de los mismos. En especial, la evidencia digital es sensible a fenómenos electromagnéticos, y puede ser eliminada o alterada a distancia”. (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, 2019, pp. 21-22)

Cabe aclarar que la cadena de custodia debe mantenerse y no puede romperse en ningún momento, incluso en los lapsos de tiempo en que esta no es consultada ni utilizada.

Por otra parte, el depósito y preservación de la evidencia digital y de sus contenedores requiere contar con entornos adecuados (en cuanto a seguridad y reserva de los datos), suficiente capacidad

de almacenamiento físico y virtual, y una precisa delimitación de roles. Estas cuestiones generales escapan al manejo de un caso concreto, y van más allá de los límites de esta guía. Sin embargo, no deben ser desatendidas por las autoridades del Ministerio Público Fiscal.

“En la cadena de custodia participan todos los funcionarios y/o empleados que intervengan durante las diferentes etapas del proceso judicial sobre las evidencias.

Según la estrategia del fiscal, podrá o no requerirse a uno o más funcionarios que hayan intervenido en la recolección, recepción y/o análisis de dispositivos y/o evidencia digital, que acrediten ante el tribunal el origen e integridad de dicha prueba (ver arts. 342 bis inc. 5.° y 360 último párrafo del CPP; art. 55 de la Ley nro. 13.634).

El procedimiento de cadena de custodia no obstará a la adopción de otros recaudos complementarios que sean adecuados a cada caso (validación mediante algoritmos de hash, reconocimiento de evidencias por testigos, etc.)” (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, 2019, p. 22).

Fase de *digital forensics*

Los nombres de las distintas fases forenses del peritaje informático pueden variar según la mirada personal del autor de

cada referencia y en donde, si se comparan, podrá observarse que algunos ponen más énfasis en alguna en particular.

A continuación, se enuncian las fases:

- **Identificación:** Identificar los artefactos, dispositivos u otros elementos que podrían servir a la causa.
- **Preservación**: Los datos están guardados, seguros y preservados.
- **Análisis:** Identificar herramientas y técnicas a utilizar. Procesar datos. Interpretar los resultados del análisis.
- **Documentación:** Documentación de la escena del crimen junto con fotografías, bocetos y mapeo de la escena del crimen.
- **Preservación:** El proceso de resumen y explicación de las conclusiones se realiza con la ayuda de recopilar hechos.

La última etapa o fase consiste en la documentación (informe) que se entrega al juez. Todo lo actuado debe ser rigurosamente elaborado e informado con características científicas, sin ningún

tipo de especulación u opinión subjetiva, para que el informe sea contundente e inobjetable.

¿Qué es la informática forense?

“La informática forense se define como la disciplina que combina los elementos del derecho y la informática para recopilar y analizar datos de sistemas informáticos, redes, comunicaciones inalámbricas y dispositivos de almacenamiento de una manera que sea admisible como prueba en un tribunal de justicia”. (Equipo Expresión Forense, 2022, https://n9.cl/7z2d8)

¿Para qué sirve la informática forense?

“La informática forense es una ciencia y un arte que requiere el uso de técnicas especiales para recuperar, autenticar y analizar datos electrónicos relacionados con delitos informáticos” (RecFaces, 2021, https://n9.cl/tl6yn).

Lectura sugerida: (Negro, s.f.) y capítulo 9 de (Di Lorio, 2016)

Negro, A. I. (s. f.). *El análisis integral de la evidencia digital*. Universidad Nacional de La Plata. https://n9.cl/4io3y.

Di Iorio, C. et al. y. (Noviembre de 2016). *El Rastro Digital del Delito*. Universidad de FASTA. https://n9.cl/blmll.

Herramientas forenses

La Carnegie Mellon University pone a disposición herramientas de *software* forense que, según explicaba Lawrence R. Rogers, expositor en disertación que organizó la Organización de Estados Americanos (OEA) en 2021, son utilizadas por organismos de Estados Unidos como FBI, NSA entre otros. Se puede acceder a estas herramientas desde el enlace: https://forensics.cert.org/. También en este *link* se encuentra un repositorio Linux llamado **The CERT Linux Forensics Tools Repository (LiFTeR)** que muestra aplicaciones tales como AUTOPSY (*digital forensics*), Volatility, entre otras.

Para los más curiosos que quieran conocer algo de la creación de descripciones de la familia de *malware*, les dejamos el siguiente *link*: https://n9.cl/aooxj y el correo info@cert.org para enviar consultas directamente al Sr. Lawrence. Además, se pueden solicitar allí las credenciales para descargar el *software* que se menciona en el siguiente *link*: https://n9.cl/wc7wa7.

Uno de los *softwares* de peritaje informático que actualmente emplean algunos departamentos judiciales forenses en Argentina es el **Cellebrite.** Tiene una versión de pago y se descarga en el siguiente enlace: https://www.cellebrite.com/.

Existen herramientas gratuitas que permiten llevar a cabo análisis forenses, entre ellas:

- **DUMPZILLA** está desarrollada en Python 3.x y es usada con el objetivo de extraer toda la información forense de los navegadores Firefox, Iceweasel y Seamonkey. Enlace: dumpzilla.org.

- **Phantom,** librería de procesamiento forense de imágenes. “Calcula hashes perceptuales (detección de contenido), aplicar detección y encoding de rostros, y transformaciones geométricas” (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, s. f., https://n9.cl/xbwwe).

- **BIP-M,** *framework* de análisis forense de memoria RAM. “Toma una imagen de memoria y permite encontrar procesos en ejecución, entre finalizados y ocultos, y extraer información. Se puede usar en investigaciones para determinar conexiones de internet activas (y con quién), *malware* en un dispositivo, recuperar contenido RAM y obtener contraseñas o claves de cifrado” (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, s.f., https://n9.cl/xbwwe).

- **Diskdigger** recupera imágenes de teléfonos móviles y PC.

- **Dfir**, el sitio web mantiene una lista de imágenes para practicar análisis forense digital como las que puede obtener en el siguiente enlace: https://n9.cl/ap13ky.

- Como punto final, dejamos el *link* para acceder a *software* de uso público de la Agencia de Seguridad Nacional (NSA), donde podrá encontrar distintas soluciones: https://code.nsa.gov/.

¿Qué es la auditoría en informática?

Una auditoría informática es un examen sistemático y exhaustivo de los sistemas, redes y procesos tecnológicos de una organización para evaluar su seguridad, eficiencia, cumplimiento normativo y alineación con los objetivos del negocio. Su objetivo es identificar riesgos, vulnerabilidades y deficiencias para recomendar acciones correctivas, asegurando que la tecnología proteja los activos, mantenga la integridad de los datos y optimice los recursos.

¿Qué evalúa?

Se evalúan los siguientes puntos:

- **Seguridad**: Vulnerabilidades en la infraestructura, controles de acceso,

protección contra ciberataques.

- **Eficiencia y rendimiento**: Optimización del uso de recursos (*hardware*, *software*) y **aplicaciones.**
- **Cumplimiento**: Adherencia a leyes, regulaciones y políticas internas.
- **Integridad de datos**: Protección y consistencia de la información.
- **Continuidad del negocio**: Planes de recuperación ante fallos.

¿Para qué sirve?

- **Detectar problemas**: Identifica fallos técnicos, errores humanos y debilidades en los procesos antes de que se conviertan en incidentes graves.

- **Mejorar la toma de decisiones**: Proporciona información valiosa para optimizar la inversión en TI.

- **Reducir riesgos**: Disminuye la probabilidad de brechas de seguridad y pérdida de datos.

¿Quién la realiza?

- **Auditores internos**: Personal de la propia empresa o especialistas en tecnología de la información (TI).

- **Auditores externos**: Profesionales contratados desde fuera para una evaluación imparcial.

Objetivos principales:

- Proteger los activos informáticos

- Asegurar la efectividad de los controles
- Verificar el cumplimiento legal y normativo
- Evaluar la eficiencia y eficacia de los sistemas
- Identificar riesgos y proponer mejoras

Tipos de auditoría informática

- **Auditoría de seguridad**: Control de accesos, vulnerabilidades, ciberseguridad.
- **Auditoría de sistemas:** Evaluación de infraestructura, redes, *hardware/software*.
- **Auditoría de desarrollo**: Revisión de ciclos de vida de *software*.
- **Auditoría de operaciones**: Procesos de TI, gestión de incidentes, respaldos.
- **Auditoría de cumplimiento**: Verificación de normas (ISO 27001, GDPR, SOX, etc.)
- **Auditoría forense**: Investigación de incidentes o delitos informáticos.

Fases del proceso de auditoría

- **Planificación**: Definir alcance, objetivos, recursos y cronograma.
- **Ejecución**: Recolección de evidencia mediante entrevistas, revisión documental, pruebas técnicas.
- **Análisis**: Evaluación de la información recopilada.
- **Informe**: Documentar hallazgos, conclusiones y recomendaciones.
- **Seguimiento**: Verificar la implementación de las recomendaciones.

Herramientas y técnicas

- Herramientas de análisis de red: Wireshark, Nmap.
- Escáneres de vulnerabilidades: Nessus, OpenVAS.

- Software de auditoría de sistemas: Auditoría de *logs*, monitoreo.
- Técnicas de recolección: Entrevistas, cuestionarios, muestreo, observación.
- Marcos de referencia: COBIT, ITIL, ISO/IEC 27000, NIST.

Perfil del auditor informático

- Conocimientos técnicos y legales.
- Habilidades analíticas y de comunicación.
- Ética profesional e independencia.
- Certificaciones relevantes: CISA, CISSP, CEH, ISO 27001 Lead Auditor.

Normativas y estándares clave

- ISO/IEC 27001: Seguridad de la información.
- COBIT: Gobierno de TI.

- NIST Cybersecurity Framework: Mejores prácticas en ciberseguridad.
- Leyes locales: Protección de datos personales (ej. GDPR en Europa y la de nuestro país)

Según el tipo de auditoría a ejecutar, se desprende una línea de estudio que supera el contenido de este apunte y se sugiere que los alumnos estudien cada línea de acuerdo con su motivación propia.

Como cierre de conclusiones sobre la auditoría, dejamos los siguientes puntos de relevancia para que sean tenidos en cuenta:

- La auditoría informática es esencial para la gestión de riesgos y la continuidad del negocio.
- Requiere un enfoque multidisciplinario (tecnología, leyes, procesos).
- Su objetivo no es “culpar”, sino mejorar y prevenir.
- Invitar a la reflexión sobre la importancia de la ciberseguridad en el mundo actual.

CONTINUAR

Referencias

Equipo Expresión Forense (2022). *Informática Forense*. Expresión Forense. https://www.expresionforense.com/blog/informatica-forense.

Escalona Acuña, H. (2014). *El tiempo que pasa es la verdad que huye (I)*. Aporrea. https://www.aporrea.org/ddhh/a197747.html.

Kundro, D. (5 de junio de 2020). *Cómo descompilar un ejecutable malicioso (.exe) escrito en Python*. ESET. https://www.welivesecurity.com/la-es/2020/06/05/como-descompilar-ejecutable-malicioso-exe-python/

Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (2019). *Guía integral de empleo de la informática forense en el proceso penal*. Pensamiento Penal. https://www.pensamientopenal.com.ar/system/files/2019/02/doctrina47360.pdf .

Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (s. f.). *Software*. Info Lab. https://info-lab.org.ar/descargas/software.

Latto, N. (5 de agosto de 2021). *¿Qué es WannaCry?* Avast. https://www.avast.com/es-es/c-wannacry#gref

Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Ministerio de Hacienda y Administraciones Públicas. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

Ministerio Público Fiscal (2014). *La evidencia digital*. Fiscales. https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf.

RecFaces (2021). *Informática forense: ¿qué es en 2021-2022?* RecFaces. https://recfaces.com/es/articles/informatica-forense.

Ruge Pinzón, J. (2011). Metodología para la identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00000744.pdf.

Urbina, G. B. (2016). *Seguridad Informática*. Grupo Editorial Patria.

CONTINUAR

Descarga en PDF