Título: Guía de recomendaciones para la preservación de la prueba sobre el uso y acceso a los Sistemas de Información en un entorno corporativo.

Autor: Ing. Rosales María Fernanda

POSGRADO ESPECIALIZACIÓN EN INFORMÁTICA FORENSE

Facultad de ingeniería

Directora: Mg. Ing. Nievas Guillermina

Fecha de publicación: 19/08/2022

UNIVERSIDAD FASTA

FACULTAD DE INGENIERÍA

ÍNDICE

RESÚMEN

La guía de recomendaciones para la preservación de la prueba sobre el uso y acceso a los Sistemas de Información en un entorno corporativo es una herramienta para el Especialista en Informática Forense, en su rol de auditor, que le permite reunir y evaluar toda la información suficiente, pertinente y competente, para que se preserve como futura evidencia.

En el momento que el empleador sospecha que un empleado le está siendo infiel, puede recurrir a un Especialista en Informática Forense, que en ese mismo momento asegure y preserve la evidencia y guarde toda la información que servirá como primera respuesta para una pericia o incluso como evidencia para comenzar una causa.

La finalidad de la guía es relevar y preservar toda la información importante en caso de ser necesaria una futura pericia informática, mediante procesos de auditoría en el entorno de trabajo del empleado.

Abarca recomendaciones para la preservación de la evidencia y la asesoría como primera respuesta en las pericias que tengan que ver con el actuar del empleado sobre el uso y acceso al Sistemas de Información, a través de procesos relacionados a la forensia digital.

PALABRAS CLAVES

Guía – Perito – Auditoría – Infiel – Preservación

AGRADECIMIENTOS

Agradezco a la Universidad FASTA y a todos los docentes de la carrera, especialmente a la Mag. Ing. Guillermina Nievas, mi tutora, por su tiempo, dedicación y ayuda.

Al Ing. S Sergio Appendino y al Esp. Dr. Pablo Cistoldi, por el tiempo dedicado y sus conocimientos brindados.

A mis padres, quienes me inculcaron la importancia del estudio.

A mi marido y mis hijos, por acompañarme y apoyarme incondicionalmente.

A mi amiga Ana, que desde un principio me impulsó para hacer la especialización.

INTRODUCCIÓN

Los empleados son uno de los activos más valiosos que tiene una empresa, pero también a menudo las personas son el eslabón débil de la cadena. La infidelidad del empleado es un buen ejemplo de esto.

Un activo es cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o costo.

Una amenaza es una circunstancia desfavorable que puede ocurrir, y al materializarse tiene consecuencias negativas sobre los activos, provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

En este caso de estudio, la información inherente al usuario como lo es el sistema de información al que accede y la información relacionada con su puesto de trabajo, pasan a ser los activos que se deben proteger.

Cuando un empleador sospecha o descubre que un empleado le está siendo infiel comienza el litigio legal.

Las pericias son solicitadas un tiempo o años después, por lo tanto, mucha de la información que era de relevancia ya no existe en la empresa o es muy difícil de obtener.

En el momento que el empleador sospecha de su empleado, puede recurrir a un Especialista en Informática Forense, que en ese mismo momento asegure y preserve la evidencia y guarde toda la información que servirá como primera respuesta para una pericia o incluso como evidencia para comenzar una causa.

En este trabajo se desarrolla una Guía de Recomendaciones cuya finalidad es relevar y preservar toda la información relevante en caso de ser necesaria una futura pericia informática, mediante procesos de auditoría en el entorno de trabajo del empleado.

Abarca recomendaciones para la preservación de la evidencia y la asesoría como primera respuesta en las pericias que tengan que ver con el actuar del empleado sobre el uso y acceso al Sistemas de Información, a través de procesos relacionados a la forensia digital.

En la misma se detallan los pasos a seguir para que los principios de integridad, validez y disponibilidad, se cumplan, garantizando de esta forma que la información preservada sea válida a futuro caso de que prospere la acusación y se requiera la pericia para un juicio.

En este proceso de auditoría informática se busca recoger, agrupar y evaluar las evidencias a salvaguardarse, mantener la integridad de los datos y utilizar eficientemente los recursos para llevar a cabo el pedido de la organización.

Utilizando esta guía, el Especialista en Informática Forense, en su rol de auditor, puede reunir y evaluar toda la información suficiente, pertinente y competente, para que se preserve como futura evidencia.

MOTIVACIÓN

La actividad laboral y el ámbito en el que la autora desarrolla su actividad como Ingeniera en Informática, es mayormente el empresarial. Brinda asesoramiento y soporte a organizaciones en lo referente al hardware y equipamiento informático, sistemas operativos, software y redes. De este tipo de servicios surgen consultas que tienen que ver con la seguridad de los datos y su disponibilidad a futuro.

El cursado de la Especialización en Informática Forense, en especial la materia de Auditoría y Seguridad Informática, generó un especial interés como alternativa para dar soluciones a esos requerimientos.

Analizando las necesidades que tienen hoy en día los especialistas es esta área, se puso foco sobre la actuación del "empleado infiel" ya que los profesionales no cuentan con una guía para la recolección y preservación de la información relacionada a este tipo de delitos.

La relación entre estos dos intereses son el punto inicial para armar esta guía, en donde el proceso de búsqueda, selección, y copia de toda la información relevante sea planificado, ordenado y completo.

OBJETIVOS DEL TRABAJO

Objetivo general

Crear una Guía de recomendaciones para la preservación de los datos sobre el uso y acceso a los Sistemas de Información y al entorno de trabajo de un empleado corporativo sobre el que se cierne la sospecha de infidelidad.

Objetivos específicos

- Identificar los aspectos legales concernientes a las situaciones de Fraude y de Administración Fraudulenta, haciendo foco en delitos que puedan involucrar el actual de un empleado infiel.
- Establecer los criterios en la búsqueda de la información que permita ser utilizada para comprobar el comportamiento de un empleado cuyo empleador considera que está cometiendo actos que se consideran como defraudación dentro del perfil de un empleado infiel.
- Describir toda la información referida al empleado en relación a su puesto de trabajo, su ambiente de trabajo, el personal con el que interactúa, y su posición dentro de la empresa.
- Reconocer la información relevante para ser preservada y que pueda ser utilizada más adelante como primera evidencia en una etapa judicial.

- Proponer, utilizando técnicas de la informática forense, los pasos necesarios para la preservación de la información relacionada al puesto de trabajo (la computadora que usa el empleado), el sistema que utiliza y la base de datos a la que accede.
- Proponer, a partir de la información obtenida, la estructura para elaborar un informe final.

ALCANCE

Los temas que se incluyen en la guía son:

- La recolección de la información que hace referencia al puesto de trabajo del empleado dentro de la empresa.
- La realización de la copia forense del equipo del usuario. Entendiéndose como equipo del usuario, la computadora que utilice para su trabajo, dentro de la empresa u organización.
- La realización de copias de seguridad del sistema informático y/o las bases de datos del mismo, que utiliza el usuario para su trabajo cotidiano. Puede ser un módulo dentro de todo un sistema o al sistema informático en su totalidad, los que podrán estar instalados en forma local en el equipo del usuario, o en un servidor: local o remoto.
- La utilización de técnicas de auditoría para reunir toda la documentación referida al sistema y a las bases de datos.
- El marco y estructura del informe de auditoría propuesto para ser devuelto a la gerencia.

MARCO TEÓRICO

A los efectos de establecer un marco de conocimiento al trabajo se desarrollarán los siguientes tópicos:

- Aspectos legales sobre el delito de defraudación por administración fraudulenta, poniendo el foco en el caso especial del empleado infiel.
- Conceptos relacionados con la informática forense.
- La auditoría como herramienta para el Especialista en Informática Forense.
- Etapas de un proceso de auditoría.

La finalidad de este marco teórico es brindar una lectura explicativa que guíe en las relaciones entre el delito de defraudación y la necesidad de la actuación de un Especialista en Informática Forense como auditor para la recolección y preservación de la información como posible evidencia.

Estafas y defraudaciones

El Art 172 del Código Penal Argentino cita: *"Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño*."

En el Código Penal Argentino: Ley 11.179; Libro Segundo; Título VI; Capítulo IV; se agrupan diferentes figuras delictivas bajo la denominación común de "Estafas y otras defraudaciones". Todos los ilícitos previstos en este título son defraudaciones y, dentro de ellas se encuentran las estafas.

Casos especiales por defraudación

Para el desarrollo del siguiente tema, se abordará el enfoque de Figari, R. (2016).

En el Código Penal de la Nación Argentina, en su Art. 173 se describen tipos especiales de estafa. Se analizarán dos incisos del mencionado artículo en los que encuadra el tema del empleado infiel.

Art. 173, Inc. 7 - Defraudación por administración fraudulenta

Conforme el orden establecido en el Código Penal, en su Art. 173, Inc. 7, *la defraudación por administración fraudulenta es un delito contra la propiedad que se concreta cuando una persona a cargo del manejo, la administración o el cuidado de bienes o intereses pecuniarios ajenos, y con el fin de procurar para sí o para un tercero un lucro indebido o para causar daño, viola sus deberes y perjudica los intereses confiados u obliga al titular de éstos con abuso de confianza.*

En base a lo que se describe en el Art. 173, el derecho le ha dado diferentes denominaciones a este delito. Así se lo conoce como: “Administración fraudulenta”; “Administración infiel”; “Defraudación por infidelidad o abuso”; “Defraudación por deslealtad en el manejo de bienes ajenos”.

Tiene como finalidad perjudicar el patrimonio ajeno por medio de un abuso de confianza. El punto central del delito es el de dañar al deber jurídico de cuidar el patrimonio de otro.

Aspecto objetivo de la Ley

Acciones típicas

Se trata de un tipo penal mixto alternativo, pues la ley describe dos conductas distintas, pero resulta indiferente que se realice una u otra, o todas ellas, porque no se añade mayor desvalor al injusto.

Las dos conductas anteriormente mencionadas se estudian bajo la denominación de “infidelidad defraudatoria” y “abuso defraudatorio”.

La infidelidad defraudatoria hace referencia a la conducta de perjudicar los intereses confiados; la segunda, el abuso defraudatorio, por su lado, hace referencia a la conducta de obligar abusivamente al dueño de los intereses confiados.

Ambos hechos, faltan a la fidelidad que el del autor del ilícito debe mantener por el grado de responsabilidad dado para cumplir sus obligaciones.

Los sujetos

En el derecho penal, se conoce como sujeto activo, aquel que comete un delito.

Sólo puede ser sujeto activo del delito la persona física que, por disposición de la ley, de la autoridad o por un acto jurídico, tiene a su cargo el manejo, la administración o el cuidado de bienes o intereses pecuniarios ajenos. (Figari, 2016)

Sujeto pasivo del delito es el titular de los intereses confiados al sujeto activo. El titular del patrimonio confiado al sujeto activo puede ser una persona física o una persona de existencia ideal (persona moral o jurídica). Como ejemplo de esto podemos mencionar: las sociedades anónimas, la administración pública, entes descentralizados o autárquicos.

Los objetos materiales del delito

El objeto material del delito es la persona, cosa, bien o interés penalmente protegido, sobre la que se produce el delito.

El sujeto activo como administrador

Es cuando el sujeto activo tiene la responsabilidad sobre el patrimonio ajeno, y la facultad de regir y gobernar dicho patrimonio pudiendo arbitrar los medios destinados a la conservación del mismo, como así también a su realización.

Como ejemplo se pueden mencionar a los gerentes de la sociedad de responsabilidad limitada (art. 157 L.S.), al directorio de una sociedad anónima (art. 255 L.S.), entre otros.

El sujeto activo como cuidador

En esta circunstancia más bien se trata de la persona que sin tener necesariamente poder sobre los bienes, tiene en cambio, la vigilancia y protección de los mismos.

El deber de cuidar, a diferencia de la administración, no requiere ninguna actividad operativa por parte de quien lo tiene a su cargo, bastando la relación pasiva, o sea, la vigilancia.

Aspecto subjetivo de la Ley

El tipo subjetivo de la administración fraudulenta requiere que la acción típica sea dolosa, es decir, que el sujeto activo tenga conocimiento de que está perjudicando los bienes del sujeto pasivo.

Quien comete el delito tiene pleno conocimiento que está causando un daño o perjuicio, que está violando el deber de cuidado en el manejo de administración del patrimonio ajeno que se le ha confiado.

Cuando la acción busca un fin de lucro se lo conoce como dolo especializado.

Art. 173, Inc. 16 - Estafa Informática

Para el desarrollo del siguiente tema, se abordará el enfoque de Rodríguez, P. (2015)

El inciso 16 del art. 173 del Código Penal, incorporado por la ley 26.338 introduce la denominada estafa informática, conforme el cual se reprime al "que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".

El autor logra estafar, a través de manipulación de sistemas informáticos alterando el normal funcionamiento de los mismos, provocando el traspaso de bienes en beneficio propio o de terceros.

El tipo objetivo incrimina las defraudaciones cometidas mediante cualquier técnica de manipulación informática esto es, cualquier modificación del resultado de un proceso automatizado de datos sea que se produzca a través de la introducción de nuevos datos, de la alteración de los existentes en el computador, en cualquier de las fases de su procesamiento o tratamiento informático. Pero sólo las que alteran el normal funcionamiento del sistema informático o la transmisión de datos, no aquellas en que la defraudación, que es en definitiva aquí la transferencia o disposición patrimonial, es

ejecutada por la propia víctima engañada por el autor a través de medios informáticos. (Rodríguez, P. 2015)

Debe quedar en claro que estas figuras no se aplican a los casos en que la informática es utilizada como medio para llevar a cabo el ardid o engaño.

Estrictamente es toda aquella maniobra que incluya en su esencia, acceder en forma oculta a bases de datos. Esto puede llevarse a cabo modificando el código del programa, reemplazando la identidad de una persona real o inexistente o enviando datos falsos. También puede considerarse la introducción de virus que afecten el normal funcionamiento del sistema.

El otro medio típico es la manipulación informática que altera la transmisión de datos con las que operan los sistemas, donde no se modifica el código o alguna de las técnicas mencionadas en el primer caso, sino que, se interfieren los datos que intercambia el sistema con los usuarios. Busca modificarlos y producir desplazamientos de contenido patrimonial.

Es sujeto activo es cualquier persona que tenga o no autorización para el ingreso al sistema.

El empleado infiel y la Ley de Contrato de Trabajo

Para el desarrollo del siguiente tema, se abordará el enfoque de Butlow, R. (2017)

Se denomina empleado infiel a aquella persona que ha incumplido los deberes de fidelidad y de buena fe que están establecidos en la ley de contrato de trabajo (N° 20744), artículos 63 y 85.

El artículo 63 de la ley de contrato de trabajo expone: “Las partes están obligadas a obrar de buena fe, ajustando su conducta a lo que es propio de un buen empleador y de un buen trabajador, tanto al celebrar, ejecutar o extinguir el contrato o la relación de trabajo.”

De la lectura del párrafo anterior, se puede inferir que hay, entre el empleador y el trabajador, una obligación mutua de obrar de buena fe, lealmente, sin faltar al cumplimiento del contrato de trabajo celebrado entre ambos. Si alguno no actúa de manera leal, se extingue el vínculo laboral entre ambos.

En cuanto al artículo 85 expresa: “El trabajador debe observar todos aquellos deberes de fidelidad que deriven de la índole de las tareas que tenga asignadas, guardando reserva o secreto de las informaciones a que tenga acceso y exijan tal comportamiento de su parte.”

La fidelidad, como un deber, se constituye como una obligación fundamental en un esquema de relación de trabajo. El trabajador al insertarse en el organigrama de la organización, accede a determinada información por lo general de carácter comercial y/o técnicas que al empresariado le interesa mantener confidencial a favor de su propio interés.

El deber de fidelidad consiste de parte del empleado en no realizar ningún tipo de acto que perjudique los intereses de su empleador.

Quien tenga un comportamiento desleal hacia su empleador, está actuando sin dudas de mala fe. Mediante ardides o engaños, oculta al empleador, hechos o situaciones, que van en perjuicio de sus intereses.

La buena fe, debe conducir las relaciones laborales. Exige de parte del empleador reglas claras y razonables que se establezcan de acuerdo a los fines de la empresa y las exigencias de la producción, y por el lado del empleado exige la fidelidad para no perjudicar el patrimonio ajeno.

Indicio, evidencia y prueba

Según Castillero Mimenza, O. (2018), las palabras indicio, prueba y evidencia pueden ser utilizadas en nuestro vocabulario habitual, pero están principalmente vinculadas con el ámbito judicial. En este aspecto, se emplean dichos términos con el fin de hacer referencia a todos aquellos elementos que sirven para establecer relaciones entre elementos concretos de un caso e hipotetizar, reconstruir y demostrar dichas relaciones.

El indicio es un indicador de que un hecho ocurrió.

La evidencia es un indicio analizado científicamente para aseverar algo sobre ese hecho. La prueba es un argumento demostrativo que permite comprobar la existencia o no del hecho que se presume.

La evidencia sólo se constituye en una prueba cuando el juez la admite como parte del proceso.

La evidencia digital

De acuerdo con la ISO/IEC 27037:2012 la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia.
Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, bien ésta sea utilizada para que sea admisible en corte o no.

- La relevancia es una condición técnicamente jurídica, que hace referencia a aquellos elementos que son significativos a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos. Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio.

- La confiabilidad busca que en el proceso aplicado para obtener evidencia digital se puedan validar la repetibilidad y auditabilidad, es decir, que la evidencia que se obtiene es lo que deber ser y que, si un tercero sigue el mismo proceso, deberá obtener los mismos resultados verificables y comprobables.

- La suficiencia, está relacionada con la completitud de la evidencia digital, es decir que, con las evidencias que se recolectaron y analizaron se tiene suficientes elementos para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada.

La Informática Forense

"*La informática forense se refiere a un conjunto de procedimientos y técnicas metodológicas para identificar, recolectar, preservar, extraer, interpretar, documentar y presentar las evidencias que se encuentran almacenadas en un medio digital*". (UNIR,2021)

La informática es una parte muy importante en la investigación forense dentro del ámbito digital, ya que está específicamente enfocada en los delitos cometidos mediante el uso de dispositivos de computación, como redes, computadoras, y medios de almacenamiento digital. Se tiene en cuenta aquellos casos que involucran a la tecnología como fuente o víctima de un delito.

Rol del Informático Forense en el Proceso Penal

En un proceso penal podemos encontrar al Informático Forense actuando en una o más de estas tres tareas:

- **Rol de Asesoramiento:** El experto actúa como ayuda para quien dirige la investigación, desarrollando tareas de planificación, investigativas o probatorias.
- **Rol Investigativo:** El especialista en este rol ejecuta medidas de investigación.
- **Rol Pericial:** El experto aporta sus experiencia y conocimientos en la materia, para conocer o apreciar algún hecho o circunstancia pertinentes a la causa.

En nuestro caso de estudio, como todavía no se sabe si se va a llevar un proceso penal podemos decir que el Especialista en Informática Forense actuará en su rol de asesor e investigador.

La auditoría como herramienta para el Especialista en Informática Forense

Es una herramienta y/o técnica de verificación o análisis de fases y procesos que le permitirá al Especialista en Informática Forense, corroborar los posibles delitos y/o fraude cometido, ya sea por error involuntario o no, cualquiera sea la consecuencia del acto cometido.

El Especialista en Informática Forense puede utilizar estas herramientas para el caso de estudio de este trabajo, para cumplimentar a través de fases y procesos la recolección y preservación de la información, como así también, la elaboración del informe correspondiente.

Auditoría

Auditoría es el proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría (SO/IEC 27000:2014)

La Auditoría Informática

Para el desarrollo del siguiente tema, se abordará el enfoque de Facultad de Ciencias Exactas, Ingeniería y Agrimensura, UNR. (s.f.).

La Auditoría Informática, es un proceso evolutivo que "mediante técnicas y procedimientos aplicados en una organización por personal independiente a la operación de la misma, evalúa la función de tecnología de información y su aportación al cumplimiento de los objetivos institucionales; emite una opinión al respecto y efectúa recomendaciones para mejorar el nivel de apoyo al cumplimiento de dichos objetivos". (Fernández Granjales, 2005)

Los objetivos de la auditoría informática son:

- El control de la función informática.
- El análisis de la eficiencia de los Sistemas Informáticos.
- La verificación del cumplimiento de la normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos.

Etapas de una auditoría

1. Planificación

La primera etapa en la realización de la auditoría es la planificación. Esta fase tendrá en cuenta dos aspectos claves: el administrativo y el específico de la auditoría.

El aspecto administrativo tiene que ver con la asignación de los recursos necesarios, financieros, humanos, materiales, planificación temporal, etc.

El otro aspecto, el específico de la auditoría, tiene que ver con las tareas a llevarse a cabo para poder realizar una auditoría de calidad.

2. Ejecución

Las auditorías de tecnología de Información se realizan recolectando información y documentación de todo tipo y de interés para el caso.

El trabajo de campo del auditor consiste en lograr recabar toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos que se puedan demostrar.

Se pueden utilizar diferentes técnicas para realizar el trabajo. Cada una de ellas dependerá del campo de actuación.

Los resultados de este proceso de recopilación, análisis e interpretación de la información deben documentarse en papeles de trabajo. Estos documentarán en forma clara y precisa: la descripción de los procedimientos aplicados, los análisis efectuados y las conclusiones que sustentarán las observaciones y recomendaciones.

3. El Informe

El informe es el Producto final de la auditoría, es el vehículo que el auditor utiliza para exponer su trabajo y avala personal y profesionalmente su juicio.

El informe de auditoría deberá ser:

- Claro
- Adecuado
- Suficiente
- Comprensible
- Realizado con un formato que refleje una presentación lógica y organizada

GLOSARIO

El siguiente glosario fue desarrollado para acompañar el entendimiento de la guía, en el mismo encontrará definiciones y terminología que fue obtenida mediante la búsqueda en diccionarios, como el de la RAE, entre otros, y algunos términos son elaboración del autor.

B

- **Backup**: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Base de datos**: Es una recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático.
- **Bloqueador de escritura**: Es una herramienta que utiliza el perito informático, que le permite analizar un disco rígido en modo de bloqueo de escritura, es decir, sin tener que preocuparse de que algún sector del disco pueda ser escrito en forma accidental.
- **Bolsa antiestática**: Bolsa que se utiliza para almacenar componentes electrónicos, que son propensos a sufrir daños causados por descargas electrostáticas.

C

- **Cláusula de confidencialidad**: Un acuerdo de confidencialidad, o cláusula de confidencialidad, es una manifestación de la voluntad de las partes involucradas que busca que se produzca la obligación de guardar y no revelar a terceros información que una de las partes desea proteger, y que se puede desarrollar en una etapa precontractual o incluir dentro de un contrato.
- **Clonador de disco:** Es un dispositivo conocido también como duplicador. Se utiliza para realizar la copia de una unidad de almacenamiento en otra.
- **Copia forense:** También llamada imagen forense. Es el resultado del proceso de llevar a cabo una copia exacta de un medio de almacenamiento digital.

E

- **EIF:** Especialista en Informática Forense. Es el profesional que utiliza un conjunto de procedimientos y técnicas metodológicas para identificar, recolectar, preservar, extraer, interpretar, documentar y presentar las evidencias del equipamiento de computación de manera que estas evidencias sean aceptables durante un procedimiento legal o administrativo.

- **Escribano:** Notario o funcionario público que da fe de los actos realizados ante él y que redacta los documentos correspondientes.
- **Extracción:** Es un tipo de recuperación de la información cuyo objetivo es extraer automáticamente información estructurada o semiestructurada desde documentos legibles por una computadora.

F

- **Factor de forma:** Son los estándares que definen algunas características físicas de los dispositivos de una computadora.
- **Firma digital:** Es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje, y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador.

H

- **Hash:** Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

I

- **Incidente de seguridad:** Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad.

L

- **Logs de auditoría:** Registra los cambios que hacen los usuarios. Cada vez que se agrega, actualiza o elimina un elemento, se registra una entrada para hacer el seguimiento de los cambios y conservar un historial completo de los datos de su organización.

M

- **Manual de procesos:** Es el documento que permite a las personas que utilizan los sistemas de información su entendimiento y uso de las funcionalidades que este posee. Además, es una guía de asistencia para el usuario final sobre el funcionamiento de los aplicativos y de solución a los problemas más comunes.
- **Mapa conceptual de transacciones de base de datos:** Indica en forma gráfica las transacciones que existen en una base de datos, compuesta por varios procesos que se han de aplicar uno después del otro.

- **Mapa de relaciones base de datos:** Indica qué tablas o relaciones componen la base de datos, así como los campos incluidos en cada tabla.

O

- **Organigrama:** Es una representación gráfica de la estructura jerárquica y funcional de una organización, permitiendo entenderla rápidamente de manera visual. Es una herramienta que permite a las empresas entender mejor su estructura y cómo se distribuyen las funciones y responsabilidades en la cadena de mando.

P

- **Perfiles de usuario:** Los perfiles de usuario contienen la información que el sistema necesita para permitir a los usuarios iniciar una sesión en el sistema, para acceder a su propia sesión personalizada
- **Perito contador:** un especialista que se encargará de esclarecer hechos contables que se encuentren en una controversia judicial.
- **Puntos de estudio del caso:** son las preguntas iniciales o incógnitas de interés que debe responder el especialista en informática forense, al momento de realizar la investigación.

R

- **RAID:** Es un proceso utilizado para combinar varios discos duros y que éstos funcionen de manera coordinada para formar una única unidad lógica en la que almacenar los datos.

S

- **Servidor:** Hace referencia a la computadora que pone recursos a disposición a través de una red. Proporciona recursos, datos, servicios o programas a otros equipos, conocidos como clientes, a través de una red. En teoría, se consideran servidores aquellos equipos que comparten recursos con máquinas cliente.
- **Servidor Cloud:** Un servidor de nube es un recurso de servidor centralizado y agrupado que se aloja y distribuye a través de una red (generalmente Internet) y al que pueden acceder múltiples usuarios cuando lo necesiten.
- **Servidor Virtualizado:** Un servidor virtual recrea la funcionalidad de un servidor físico. Existe de manera transparente para los usuarios como un espacio de partición dentro de un servidor físico. La virtualización de los servidores facilita la reasignación de recursos y la adaptación a las cargas de trabajo dinámicas.

DESARROLLO DE LA GUÍA

La ejecución de la guía, se ordena en tres etapas o fases que permitan cumplir con el proceso integral del trabajo para que devengue en una recolección y preservación de la información exitosa.

Es importante aclarar que, las buenas prácticas por parte del profesional en informática forense, en cada una de estas etapas garantizará el éxito del proceso en general.

En la elaboración de la guía se utilizó al modelo PURI[1] como marco de desarrollo para las actividades propuestas, con el fin de darle un marco teórico a la misma.

Teniendo como base los procesos de auditoría informática se definen tres etapas:

1. Etapa de Planificación
2. Etapa de Ejecución
3. Elaboración del Informe

Se puede encontrar una concordancia entre la Etapa de Planificación de esta guía con la Fase de Relevamiento de PURI, la etapa de Ejecución con las fases de Recolección y Adquisición y la etapa de Elaboración del Informe con la fase de Presentación.

1. Etapa de Planificación

Esta primera etapa tiene como finalidad la descripción de la actuación del perito en informática forense, en adelante EIF, frente a las tareas que se deberán realizar y organizar para el posterior proceso de recolección.

De la buena planificación y el buen diálogo con la gerencia y personal a cargo dependerá el alcance de los objetivos planteados.

Dentro de esta etapa se diferencian dos sub etapas:

1.1 Reunión con la gerencia.

1.2 Planificación para la recolección y preservación de la información.

1.1 Reunión con la gerencia

La reunión de apertura con la gerencia tendrá principalmente las siguientes funciones:

- Presentación del Especialista en Informática Forense, y de su equipo de trabajo.

[1] Proceso Unificado de Recuperación de Información.

- Que el EIF se ponga en autos acerca del caso sobre el que deberá trabajar.
- Conocer la empresa o institución, su organigrama y el rol que ocupaba el empleado en cuestión, dentro de ella.
- Establecer los objetivos, el alcance y los puntos de estudio del caso.
- Diseñar un plan preliminar de trabajo y los canales de comunicación.
- Explicar las actividades y cómo se llevarán a cabo.
- Resolver dudas e inquietudes de la gerencia.

Para dar claridad en cuanto a los temas y actividades de la reunión de apertura, se detallan los siguientes ítems:

Sobre el caso:

- Informarse sobre el caso, la sospecha, el empleado y su relación con el caso.
- Confirmar el objetivo, el alcance y los criterios de los puntos de estudio del caso.
- Enumerar los criterios de los puntos de estudio del caso.
- Solicitar, si se conocen, las posibles fechas en las que pudo haber ocurrido el ilícito.

Sobre el trabajo del EIF:

- Determinar si el EIF trabajará sólo o cómo estará conformado el equipo de trabajo.
- Explicar a la gerencia la metodología de trabajo del EIF.

Sobre el puesto de trabajo:

- Obtener el organigrama y esquemas organizacionales de la empresa, para lograr establecer cuál es el puesto de trabajo del empleado dentro de ella.
- Solicitar el manual que contenga las funciones del usuario o la descripción del puesto de trabajo.
- Conocer y describir el ambiente físico en el que el ilícito pudo haber ocurrido para comprender acabadamente el caso. Como ambiente físico se comprende:
    - El lugar donde se encuentra el puesto de trabajo.
    - Medidas de seguridad de acceso al lugar.
    - Presencia o no de cámaras de seguridad.
    - Miembros con los que comparte la oficina.
    - Movimiento del personal en el área de trabajo del empleado.

- Con qué otras personas o áreas se relaciona el empleado habitualmente para realizar sus tareas tanto dentro como fuera de la empresa.

- Informarse sobre el horario laboral del empleado.
- Conocer y describir los procesos internos, desde el puesto de trabajo del usuario hasta su punto final en el trabajo.

Sobre los otros profesionales con los que se trabajará:

- Determinar un enlace o responsable de la institución con quien el EIF dialogará y quien será el nexo con los empleados y la gerencia.
- Evaluar si hace falta contratar un perito contador: un profesional en Ciencias Económicas, con conocimiento y experiencia respecto a procesos administrativos y contables.
- Requerir la presencia de un escribano para que dé fe del actuar del EIF en cada momento de la recolección y extracción, para ello:
  - Establecer quién contratará al escribano, si la empresa será quien lo provea o si será parte del equipo de trabajo del EIF.
  - Siendo el caso que el escribano sea contratado por la empresa, establecer cómo y a través de quién será el contacto con el mismo.
  - Informarse si el escribano con quien se trabajará posee firma digital.
- En caso de que la empresa tenga asignado un abogado para el caso en cuestión, establecer cómo y a través de quién será el contacto con el mismo, para conocer la posible estrategia del caso.

Sobre el equipamiento informático:

- Obtener por escrito, los permisos por parte de la gerencia, para relevar todos los equipos informáticos que hagan falta en el proceso de recolección.
- Obtener por escrito los permisos para acceder al software y a las bases de datos donde se encuentra la información a resguardar.
- En caso de que la extracción no se realice in situ, obtener los permisos para el retiro de los equipos y/o dispositivos.
- Si alguno de los equipos es propiedad del usuario sospechado, verificar si existen permisos firmados para que se pueda acceder a los equipos.
- En caso de que la extracción de la información no se pueda realizar mientras la empresa está en operaciones, coordinar el correspondiente corte de operaciones para garantizar la extracción de la información.

- Obtener los requerimientos necesarios que posee la empresa para entrar al lugar para realizar el trabajo: seguro personal, elementos de seguridad, etc.

Sobre las copias forenses que se realizarán:

- Determinar quién o quiénes guardarán la o las copias.
- Coordinar quién se encargará de la compra de los medios de almacenamiento de resguardo.

Sobre el sistema informático y las bases de datos:

- Informarse sobre el uso que el usuario le da al sistema informático.
- Solicitar los manuales del sistema informático y de los procesos.
- Solicitar el mapa de relaciones de la base de datos.
- Solicitar el mapa conceptual o de las transacciones de la base de datos.
- Describir la plataforma sobre la que trabaja el software a analizar, si es local en el equipo del usuario o si está dentro de una estructura cliente/servidor. En caso de que sea este último caso, tener en claro dónde se encuentra el servidor y de qué tipo:
    - Físicamente en el mismo lugar que el equipo del cliente.
    - Si hay un RAID en el servidor.
    - Si es un servidor virtualizado.
    - Si el servidor es un servidor Cloud.

Sobre las regulaciones, planes y políticas de seguridad:

- Solicitar si tienen plan de seguridad de la información y auditoría.
- Solicitar las políticas de seguridad de la empresa.
- Solicitar las regulaciones que están relacionadas a la operatoria de la empresa o institución.
- Determinar del contexto normativo, se debe especificar las normas que rigen en el contexto en que se utilizan los sistemas informáticos
- En caso de que sea una institución del sector público, solicitar las regulaciones pertinentes.
- En caso de que existiera una legislación y/o leyes externas a la empresa, para el sistema informático, informarse y especificar si el sistema los cumple.

- Se debe averiguar y describir si existen políticas de gestión y actuación, y qué procedimientos se emplean en los sistemas informáticos.
- Si existieran solicitar informes de auditorías informáticas previas.
- Si existieran, solicitar incidentes de seguridad previos.

Sobre las cláusulas de confidencialidad:

- Establecer cláusula de confidencialidad en la que se acuerda que toda la información obtenida y recolectada no será divulgada ni publicada a terceros por parte del EIF.
- Establecer cláusula de confidencialidad en la que se acuerda que, una vez realizado el informe, el EIF elimina cualquier copia de la información que haya quedado en sus equipos personales.
- Si se va a firmar un contrato de trabajo entre la gerencia y el EIF, colocar las cláusulas de confidencialidad dentro del mismo. Si no va a existir un contrato entre las partes, se recomienda que las cláusulas mencionadas anteriormente queden firmadas en un convenio de confidencialidad.

1.2 Planificación para la recolección y preservación de la información

- Determinar, en base a lo pactado con la gerencia, fecha y hora para la recolección
- Coordinar con el escribano y el resto del personal técnico en caso de ser necesario además del EIF.
- Recolectar las características de hardware del equipo o de los equipos sobre los que se va a trabajar para tener en cuenta los recursos requeridos para el trabajo.
- Verificar los recursos requeridos para la extracción:
  - Sobres de papel.
  - Etiquetas para identificación.
  - Discos limpios para realizar las copias.
  - Fajas de seguridad.
  - Bloqueadores de escritura.
  - Clonadores de discos.
  - Cables, conectores y adaptadores de disco, para los distintos factores de forma y conexión.
  - Herramientas como destornilladores, pinzas, etc.

- Bolsas antiestáticas.
- Cámara fotográfica o dispositivo para fotografiar y/o filmar.
- Notebook o equipo para hacer la recolección.
- Software y herramientas informáticas forenses

- Definir si alguna tarea de extracción de información digital no se llevará a cabo en el lugar del hecho y si se procederá en el laboratorio del EIF. En ese caso documentar sobre qué equipos o dispositivos se hará.

2. Etapa de Ejecución

En esta etapa se hace referencia a la recolección de la información relevante para cumplir con los puntos de estudio del caso que se especificaron en la entrevista, con la gerencia.

En todo momento contar con la presencia del escribano, que mediante el labrado de un acta de fe de cada uno de los procesos y pasos que se realizan, desde que comienza el trabajo hasta que se dé por concluida la recolección.

Tener en cuenta que todas las copias forenses o de la información que se realicen durante este proceso deben quedar bajo la custodia del escribano o de quien haya quedado establecido en la reunión inicial.

Esta etapa se va a dividir en cuatro sub etapas que contemplan:

2.1 Pautas para la realización de la copia forense del equipo del usuario.

2.2 Relevamiento sobre el trabajo del usuario.

2.3 Relevamiento sobre el sistema informático y bases de datos.

2.4 Relevamiento sobre el sistema operativo en el equipo del usuario.

2.1 Pautas para la realización de la copia forense del equipo del usuario.

En este paso se tiene en cuenta que se debe guardar y preservar una copia de todo el disco del usuario.

Este proceso puede darse sobre un sólo disco de almacenamiento, o sobre más de uno, según los que tenga el equipo del usuario. Es importante seguir la guía para cada uno de ellos.

Se pueden presentar dos posibles situaciones:

2.1.1 Realización de la copia forense en la empresa.

2.1.2 Recolección del equipo o unidades de almacenamiento para luego realizar la copia forense en el laboratorio del EIF.

2.1.1 Realización de la copia forense en la empresa.

A. Registrar la identificación del equipo:
   - Número de registro dentro de la empresa.
   - Marca.
   - Modelo.
   - Número de serie.
   - Propietario.
   - Nombre del usuario.
   - Rótulo o nombre con el que quedará registrado para el EIF.
   - Fotografiar las etiquetas de los equipos.

B. Si el equipo se encuentra conectado a la red, anotar la configuración de red: dirección IP, máscara de subred, puerta de enlace, nombre y grupo de trabajo.

C. Desconectar todos los dispositivos inalámbricos.

D. Verificar que la cámara o el dispositivo que se use para fotografiar tenga bien configurada la fecha y la hora.

E. Fotografiar la pantalla, las conexiones y los cables.

F. Fotografiar y/o grabar, según sea conveniente todo el proceso desde el equipo cerrado hasta la extracción del medio de almacenamiento.

G. Registrar toda la información relevante acerca de las unidades de almacenamiento:
   - Equipo al que pertenece
     - Identificación para la empresa
     - Identificación para el EIF
   - Marca
   - Modelo
   - Número de Serie
   - Factor de forma
   - Conexión

- Capacidad
- Tecnología

H. Fotografiar las etiquetas de los discos.

I. En caso de que se posea, bloquear el disco contra escritura con los bloqueadores de escritura.

J. Colocar etiquetas de identificación a los discos y documentar en una planilla los datos que asocien al disco con la etiqueta correspondiente.

K. Fotografiar la conexión del disco al momento de la copia, ya sea que se haya conectado a un clonador de discos o a un equipo.

L. Realizar una copia forense del disco del usuario en el disco destinado para dicho fin.

M. Calcular el hash de la copia forense.

N. Realizar una segunda copia para tener en el equipo de trabajo del EIF.

O. Calcular el hash de dicha copia.

P. Si el usuario tiene impresora o accede a una, registrar:

- Marca, modelo y número de serie.
- Número de registro dentro de la empresa.
- Fotografiar la etiqueta de la impresora
- Imprimir una página de prueba en la impresora.

Material resultante de esta etapa para ser preservado y custodiado:
- Dispositivo de almacenamiento que contiene la copia forense del equipo del usuario.
- Hash de la copia forense.
- Fotografías y videos obtenidos de esta etapa.
- Al momento de entregar las fotografías, si existe la posibilidad, firmarlas digitalmente.
- Hoja de prueba de la impresora.

2.1.2 Recolección del equipo o unidades de almacenamiento para luego realizar la copia forense en el laboratorio del EIF.

Trabajo en el lugar del hecho:

A. Los equipos o dispositivos de almacenamiento que se retiren en esta etapa, deben quedar registrados por el escribano quien tome nota de todo el procedimiento.

B. Verificar que la cámara o el dispositivo que se use para fotografiar tenga bien configurada la fecha y la hora.

C. Para el retiro de equipos tener en cuenta:

- Fotografíe la pantalla, las conexiones y los cables.
- Rotular cada equipo por separado.
- Registrar la identificación del equipo (en caso de que sea en más de un equipo, repetir el proceso para cada uno de ellos):
  - Número de registro dentro de la empresa
  - Marca
  - Modelo
  - Número de serie
  - Propietario
  - Especificar ubicación física del equipo
  - Nombre del usuario
  - Número del rótulo con el que quedará registrado para el EIF
  - Fotografiar las etiquetas de los equipos.
- Si el equipo se encuentra conectado a la red, anotar la configuración de red: IP, máscara de subred, puerta de enlace, nombre y grupo de trabajo.

D. Para el retiro de unidades de almacenamiento tener en cuenta:

- Registrar toda la información relevante acerca de las unidades de almacenamiento:
  - Equipo al que pertenece
    - Identificación para la empresa
    - Identificación para el EIF
  - Marca

- Modelo
- Número de Serie
- Factor de forma
- Conexión
- Capacidad
- Tecnología

  - Fotografiar las etiquetas de los discos.
  - Fotografiar y/o grabar, según sea conveniente todo el proceso desde el equipo cerrado hasta la extracción del medio de almacenamiento.
  - Usar bolsas especiales antiestáticas para almacenar los dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se tiene, pueden utilizarse bolsas de papel madera).

E. Si el usuario tiene impresora o accede a una, registrar:

  - Marca, modelo y número de serie.
  - Número de registro dentro de la empresa.
  - Fotografiar la etiqueta de la impresora.
  - Imprimir una página de prueba en la impresora.

Trabajo en el laboratorio:

A. Realizar una copia forense del disco del usuario en el disco destinado para dicho fin.

B. Calcular el hash de la copia.

C. Realizar una segunda copia para tener en el equipo de trabajo del EIF.

D. Calcular el hash de la copia.

Material resultante de esta etapa para ser preservado y custodiado:
- Dispositivo de almacenamiento que contiene la copia forense del equipo del usuario.
- Hash de la copia forense.
- Fotografías y videos obtenidos de esta etapa.
- Al momento de entregar las fotografías, si existe la posibilidad, firmarlas digitalmente.
- Hoja de prueba de la impresora.

2.2 Relevamiento sobre el trabajo del usuario

A. Realizar una descripción del lugar donde se encuentra, dentro de la empresa, la oficina que ocupa el empleado.
B. Describir las medidas de seguridad que tiene el acceso a la oficina.
C. Describir si hay cámaras de seguridad existentes en la oficina.
D. Identificar las personas con las que el usuario comparte el espacio de trabajo.
E. Describir el movimiento de personal dentro de la oficina.
F. Registrar el horario laboral del usuario.
G. Realizar una descripción de su área y cargos dentro del organigrama de la empresa.
H. Realizar una descripción de las funciones según la descripción de su puesto de trabajo.
I. Contrastar y registrar sí coinciden las funciones reales que realiza el empleado con las que se encuentran detalladas en la descripción del puesto de trabajo.
J. Realizar la descripción de los procesos administrativos, contables e informáticos en los que participa el usuario y que son de interés en el hecho.
K. Listar con qué otras personas o áreas se relaciona el empleado habitualmente para realizar sus tareas tanto dentro como fuera de la empresa: áreas dentro de la misma empresa, proveedores, clientes, etc.

2.3 Relevamiento sobre el sistema informático y las bases de datos

A. Para esta etapa, solicitar al enlace la posibilidad de interactuar, si existe, con el referente del área de sistemas.
B. Enumerar todos los sistemas informáticos involucrados y que tengan conexión con el sistema informático que se analiza en particular.
C. Describir si se va a trabajar con una parte o subsistema que forma parte de un sistema integral con el que trabaja la empresa.
D. Si la gerencia lo facilitó, analizar los manuales del sistema y de los procesos.
E. Determinar cuáles son las características funcionales y técnicas de dicho software, la vinculación que tiene con otros sistemas de la organización y el ambiente en el que opera.
F. Analizar y describir los procesos administrativos y contables involucrados en el hecho, con el detalle de las funciones de los sistemas informáticos que utiliza cada proceso, áreas y sectores involucrados en el proceso, cargo y perfil en el sistema del empleado en cuestión.

G. Describir y especificar la funcionalidad de los sistemas informáticos involucrados en el hecho, detallando en particular aquellos que tengan relación con la denuncia y que puedan revelar el modus operandi.

H. Especificar cómo implementa seguridad del software. Si requiere usuario y contraseña de acceso, tabla de perfiles de usuarios, grupos y permisos dentro del sistema informático.

I. En base a las políticas de seguridad obtenidas por parte de la gerencia detallar:
    - Cada cuánto se debe cambiar la contraseña
    - ¿El usuario puede cambiar el nombre?

J. Obtener si existen, logs de auditoría donde se registran los cambios que hacen los usuarios.

K. Revisar y relevar si existen procesos de auditoría sobre el sistema informático.

L. Solicitar si se cuenta con copias de seguridad del sistema informático y de la base de datos. Tener en cuenta si esos backup son completos o incrementales.
    - Hacer una copia de los backup.
    - Calcular el hash de los backup.

M. Obtener el mapa de relaciones de la base de datos.

N. Obtener el mapa conceptual de las transacciones de la base de datos.

O. Determinar cómo se conecta el software a la base de datos.

P. Determinar si es un sistema multiusuario:
    - Si es multiusuario:
        - Registrar cómo ingresa el usuario al sistema si es a través de usuario y contraseña.
        - Obtener el usuario y de ser posible la contraseña de acceso
        - Registrar si cada usuario del sistema informático usa su propio nombre y contraseña o lo comparten entre usuarios.
        - Registrar si con el usuario y la contraseña de ese usuario se puede acceder desde otro equipo.
        - Registrar la frecuencia en el cambio de la contraseña.
    - Si es monousuario:
        - Registrar si más de un usuario utiliza el sistema.
        - Registrar la frecuencia en el cambio de la contraseña

Q. Si el sistema informático y la base de datos está instalado en el equipo del usuario en forma local:

- Realizar copia del sistema informático y/o de las bases de datos que se encuentran en dicho servidor.
- Calcular el hash de la copia.
- Realizar una segunda copia para tener en el equipo de trabajo del EIF.
- Calcular el hash de la segunda copia.

R. Si el sistema informático y la base de datos se encuentra instalado en un servidor o en otro equipo dentro de la red local:

- Registrar nombre del servidor o equipo al que se accede y del recurso compartido.
- Usuario y contraseña de acceso.
- Solicitar al encargado del servidor la creación de un usuario con el mismo perfil que el usuario en cuestión.
- Realizar copia del sistema informático y/o de las bases de datos que se encuentran en dicho servidor.
- Calcular el hash de la copia.
- Realizar una segunda copia para tener en el equipo de trabajo del EIF.
- Calcular el hash de la segunda copia.

S. Si el sistema informático y la base de datos se encuentran alojados en un web hosting:

- Pedir al encargado del alojamiento una copia de la base de datos:
- Calcular el hash de la copia.
- Realizar una segunda copia para tener en el equipo de trabajo del EIF.
- Calcular el hash de la segunda copia.
- Solicitar al encargado del alojamiento la creación de un usuario que tenga el mismo perfil que el usuario involucrado.

T. De acuerdo a la envergadura de la organización, se pueden encontrar con distintos tipos de circuitos. Por un lado, existirán los circuitos formales, comúnmente implementados a través de los comprobantes físicos en papel, y los circuitos lógicos, representados por los registros informáticos:

- Solicitar todo lo se obtenga de los circuitos formales, resguardando la emisión de comprobantes impresos si los hubiere.
- A partir de la información obtenida de la gerencia, describir si, los circuitos que surgen de la operatoria cotidiana, las funciones y responsabilidades asociadas al empleado sospechoso, los controles que se realizan sobre su actividad, cumplen con las regulaciones pertinentes.

Material resultante de esta etapa para ser preservado y custodiado:

- Copia de los backup anteriores.
- Hash de los backup.
- Copia del sistema informático y/o de las bases de datos.
- Hash de la copia del sistema informático y/o de las bases de datos.

2.4 Relevamiento sobre el sistema operativo en el equipo del usuario

A. Nombre del sistema operativo
B. Versión
C. Número de licencia
D. Esquema de perfiles: usuarios, grupos y permisos.
E. Obtener en caso de ser posible las contraseñas de acceso.
F. Documentar los registros de los accesos al sistema.
G. Registrar políticas referidas a la frecuencia de cambio de clave.
H. Determinar si existen conexiones de acceso remoto o escritorio remoto a ese equipo.
I. Describir la seguridad del sistema operativo
    - Software antivirus instalado
    - Configuración del firewall.

3. Elaboración del Informe

El informe es la última etapa en esta guía. Es el documento que refleja los objetivos, alcances, observaciones, recomendaciones y conclusiones del proceso de recolección de información relacionados con el caso.

En el informe debe quedar plasmada la información que se obtuvo durante el proceso de relevamiento y resguardo de la información, como así también el detalle de la resolución para cada uno de los puntos de estudio del caso que fueron establecidos en la reunión con la gerencia.

Fecha del informe
Título apropiado y distintivo
Identificación de los destinatarios a los que va dirigido el informe
Identificación del enlace o responsable de la organización
Identificación del escribano
Identificación de quién almacenará las copias forenses y la documentación que se entrega
Identificación del perito contador (en caso de que se hubiese necesitado)
Identificación de los abogados (en caso de que fuera parte de la tarea)
Fecha de Inicio del trabajo
Fecha de Finalización
Introducción
En base a lo acordado con la gerencia especificar el alcance del trabajo realizado.
En base a lo acordado con la gerencia especificar y describir los objetivos del trabajo realizado.
Enumerar los puntos de estudio del caso solicitados en la reunión con la gerencia.
Desarrollo
<u>Sobre la recolección de la información del equipo de usuario</u> ● Enumerar y describir cada uno de los equipos sobre los que se trabajaron, teniendo en cuenta: ○ Número de registro dentro de la empresa

- Marca
- Modelo
- Número de serie
- Propietario
- Nombre del usuario
- Número con el que quedará registrado para el EIF y con el que será referenciado en todo el informe.
- Nombre del responsable que hizo la recolección en ese equipo.
- Configuración de red: IP, máscara de subred, puerta de enlace, nombre y grupo de trabajo.

- Enumerar y describir de cada una de las unidades de almacenamiento:
  - Equipo al que pertenece
    - Identificación para la empresa
    - Identificación para el EIF y con el que será referenciado en todo el informe.
  - Marca
  - Modelo
  - Número de Serie
  - Factor de forma
  - Conexión
  - Capacidad
  - Tecnología
- Describir de la impresora del usuario:
  - Marca
  - Modelo
  - Número de serie
  - Número de registro dentro de la empresa

<u>Sobre el relevamiento en el trabajo del usuario</u>

- Describir el área, cargos y funciones del usuario.
- Describir las medidas de seguridad que tiene el acceso a la oficina.

• Describir si hay cámaras de seguridad existentes en la oficina. • Listar y nombrar las personas con las que el usuario comparte el espacio de trabajo. • Describir el movimiento de personal dentro de la oficina. • Documentar el horario laboral del usuario. • Describir su área de trabajo y cargos dentro del organigrama de la empresa. • Describir las funciones según la descripción de su puesto de trabajo. • Describir sí coinciden las funciones reales que realiza su trabajo con las que se encuentran detalladas en la descripción del puesto de trabajo. • Describir los procesos administrativos, contables e informáticos en los que participa el usuario y que son de interés en el hecho denunciado. • Listar las personas o áreas con las que el empleado se relaciona habitualmente para realizar sus tareas tanto dentro como fuera de la empresa.	
<u>Sobre el relevamiento sobre el sistema informático</u> • Enumerar todos los sistemas informáticos involucrados y que tengan conexión con el sistema informático que se analiza en particular. • Describir si se va a trabajar con una parte o subsistema que forma parte de un sistema integral con el que trabaja la empresa. • Describir cuáles son las características funcionales y técnicas del software, la vinculación que tiene con otros sistemas de la organización y el ambiente en el que opera. • Describir los procesos administrativos y contables involucrados en el hecho, con el detalle de las funciones de los sistemas informáticos que utiliza cada proceso, áreas y sectores involucrados en el proceso, cargo y perfil en el sistema del empleado en cuestión. • Describir y especificar la funcionalidad de los sistemas informáticos involucrados en el hecho, detallando en particular aquellos que tengan relación con la denuncia y que puedan revelar el modus operandi. • Describir cómo implementa seguridad del software. Si requiere usuario y contraseña de acceso, tabla de perfiles de usuarios, grupos y permisos dentro del sistema informático. • Documentar y anexar si existen procesos de auditoría sobre el sistema informático.	

- Describir si se cuenta con copias de seguridad del sistema informático y de la base de datos especificando:
    - Fecha y hora en la que se hicieron las copias
    - Tipo de copias
    - Tamaño de las mismas
    - Hash
- Describir dónde se encuentra instalado el sistema informático y la base de datos.
    - Si se encuentra almacenado en un servidor, detallar:
        - Nombre del servidor o equipo al que se accede y del recurso compartido.
        - Usuario y contraseña de acceso.
- Describir cómo se conecta el software a la base de datos.
- Describir las políticas de cambio de contraseña.
- Describir tipo de sistema: multiusuario o monousuario
    - Si es multiusuario:
        - Describir cómo ingresa el usuario al sistema si es a través de usuario y contraseña.
        - Especificar el usuario y de ser posible la contraseña de acceso
        - Especificar si cada usuario del sistema informático usa su propio nombre y contraseña o lo comparten entre usuarios.
        - Especificar la frecuencia en el cambio de la contraseña.
    - Si es monousuario:
        - Detallar si más de un usuario utiliza el sistema.
        - Especificar la frecuencia en el cambio de la contraseña
- Describir las funciones y responsabilidades asociadas al empleado sospechoso, los controles que se realizan sobre su actividad y si cumplen con las regulaciones pertinentes.

<u>Sobre el relevamiento del sistema operativo</u>

- Describir: Nombre del sistema operativo, versión y número de licencia
- Describir el esquema de perfiles: usuarios, grupos y permisos.
- Registrar, de haberse obtenido las contraseñas de acceso.

- Especificar los registros de los accesos al sistema.
- Describir las políticas referidas a la frecuencia de cambio de clave.
- Describir si existen conexiones de acceso remoto o escritorio remoto a ese equipo.
- Describir la seguridad del sistema operativo.

Para cada uno de los criterios de los puntos de estudio del caso describir:

- Sobre qué equipo se trabajó
- Sobre qué unidad de almacenamiento se trabajó
- Herramientas forenses utilizadas
- Qué se logró obtener
- Describir los procesos para la obtención de los resultados.
- Si no se pudo cumplir con el criterio, establecer cuál fue el motivo.

Descripción de las copias entregadas al escribano

- Copia forense del equipo del usuario
  - Nombre del archivo
  - Tamaño de archivo
  - Hash
- Copia del sistema informático
  - Nombre del archivo
  - Tamaño del archivo
  - Hash
- Backup existentes de la base de datos
  - Nombre del archivo
  - Tamaño del archivo
  - Hash
- Copia de la base de datos
  - Nombre del archivo
  - Tamaño del archivo
  - Hash

Descripción de la documentación entregada al escribano

- Fotografías de todo el proceso de recolección y preservación sacadas durante el proceso.
- Manuales del sistema informático y de los procesos.

• Mapa conceptual de las transacciones de la base de datos. • Mapa de relaciones de la base de datos. • Mapa conceptual de las transacciones de la base de datos. • Logs de auditoría. • Registros de acceso al sistema. • Tablas de perfiles de usuarios, grupos y permisos. • Comprobantes impresos.
Respuesta del EIF
Realizar un resumen del trabajo realizado
Resumen
Referencias a cualquier otro informe separado que deba considerarse
Nombre del EIF responsable del informe

CONCLUSIONES

A partir de los objetivos propuestos, se ha elaborado una guía que abarca los lineamientos y recomendaciones para la obtención y la preservación de la evidencia, como primera respuesta en las pericias que tengan que ver con el actuar del empleado sobre el uso y acceso al Sistemas de Información, a través de procesos utilizados en forensia digital. De este trabajo resulta un modelo, que hasta el momento carecían los Especialistas en Informática Forense para recabar la información ante la necesidad del actuar del perito, en delitos de defraudación, en el caso particular del delito del Empleado Infiel.

Tal como se expresó en el marco teórico, este delito perjudica el patrimonio ajeno por medio de un abuso de confianza, con la conducta de perjudicar los intereses confiados.

El delito del empleado infiel encuentra su encuadre legal en el Código Penal de la Nación Argentina en su Art. 173, Inc. 7 y 16. En este último, además se tiene en cuenta la presencia de una estafa informática, en la que se establece que la defraudación pasa por el uso de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático.

El desarrollo del trabajo ha permitido, mediante procesos de auditoría en el entorno de trabajo del empleado, reunir toda la información de interés, organizada en tres fases principales y dentro de cada una de ellas, la secuencia de pasos necesarios para completar la guía. El seguimiento de la misma, garantiza que los principios de integridad, validez y disponibilidad, se cumplan. Consiguiendo de esta forma que la información preservada sea válida más adelante, en caso que prospere la acusación y se requiera para la pericia en un juicio.

Se mencionaron técnicas de la informática forense para trabajar en la preservación de la información mediante la copia forense relacionada al puesto de trabajo (la computadora que usa el empleado), el sistema que utiliza y la base de datos a la que accede.

Las buenas prácticas por parte del profesional en informática forense, en cada una de estas etapas garantizará el éxito del proceso en general.

Es importante tener en cuenta que, usando este trabajo como punto de partida, se podría a futuro ampliar los alcances, para lograr obtener una guía que abarque no sólo el ámbito de trabajo del usuario y el sistema informático que usa en su lugar de trabajo, sino que también se tenga en cuenta:

- Historiales de búsqueda en navegadores
- Archivos personales que se encuentren en el equipo del usuario
- Acceso a los archivos de un servidor.
- Análisis de las aplicaciones instaladas
- Reglas y configuraciones configuradas en las puertas de enlace.
- Análisis de caso cuando el usuario realiza teletrabajo.

En este trabajo se sintetizaron temas relacionados con las materias: Auditoría y Seguridad Informática, Recuperación de Datos y Derecho informático.

Para finalizar, como conclusión final del autor, se quiere resaltar la importancia de haber realizado la especialización, siendo un nuevo enfoque para la profesión, que permite abrir nuevos horizontes de trabajo.

La realización de este trabajo final es el corolario de todo el proceso de aprendizaje, desde un enfoque relacionado a su ámbito laboral.

BIBLIOGRAFÍA

- D'Iorio, A. et al. (2017). *El rastro digital del delito*. Universidad FASTA.
- Cook, I. (2020). *The Components of the IT Audit Report*. (ISACA JOURNAL VOL 1). ISACA.
- Fernández Grajales, N. (2005). *"Importancia de la auditoría informática en las organizaciones "*. Revista Internet, Cómputo y Telecomunicaciones de la Universidad Nacional Autónoma de México-Año 4, Número 43.
- Domínguez Chávez, J. (2021). *Fundamentos de Auditoría Informática*. IEASS, Editores.
- Piattini, M. y Del Peso, E. (1997). *Auditoría informática, un enfoque práctico.* Alfaomega RA-MA.
- López Rivera, R. (2012). *Peritaje informático y tecnológico. Un enfoque teórico-práctico.*
- Nessi, A. (2017). *Manual de Evidencia Digital.* ABA ROLI
- Aceto, J., Di Iorio, A., Greco, F. (2010). *La necesidad de una perspectiva interdisciplinaria en la investigación de delitos económicos.* 39 JAIIO - SID 2010 Ciudad Autónoma de Buenos Aires.
- Presman, G. (4 de junio de 2014). *ISO/IEC 27037 Normalizando la Práctica Forense Informática.* DOCPLAYER. https://docplayer.es/5605332-Iso-iec-27037-normalizando-la-practica-forense-informatica.html
- EBS (6 de mayo de 2011). *Instructivo para la Reunión de Apertura de la Auditoría.* SLIDESHARE. https://es.slideshare.net/costosyauditorias/instructivo-reunion-de-apertura-7974476
- Figari, R. (26 de septiembre de 2016). *Pormenores de la administración fraudulenta.* Derecho Penal. http://www.rubenfigari.com.ar/pormenores-de-la-administracion-fraudulenta -art-173-inc-7o-c-p/
- Butlow, R. (25 de julio de 2017). *Arquitectura Laboral Empleado Infiel.* Arquitectura legal según Butlow. https://arquilegal.com.ar/arquitectura-laboral-empleado-infiel/
- De la Torre R. (s.f.). *La pericial informática como prueba en el proceso judicial.* Indalics. https://indalics.com/blog-peritaje-informatico/pericial-informatica-prueba-proceso-judicial
- Castillero Mimenza, O. (12 de mayo de 2018). *¿Cuál es la diferencia entre indicio, prueba y evidencia?* Información Relevante en Materia Forense. https://www.sijufor.org/informacioacuten-relevante-en-materia-forense/cual-es-la-diferencia-entre-indicio-prueba-y-evidencia
- UNIR. (24 de junio de 2021). *Informática forense: en qué consiste.* UNIR https://www.unir.net/ingenieria/revista/informatica-forense/
- Rodríguez, P. *Estafa y otras Defraudaciones.* [Archivo PDF]. Pensamiento Penal. https://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37767.pdf

- Rodríguez, P. *Casos especiales de Defraudación.* [Archivo PDF]. Pensamiento Penal. https://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37768.pdf
- Acurio Del Pino, S. *Manual de Manejo de Evidencias Digitales y Entornos Informáticos.* [Archivo PDF]. OAS. https://www.oas.org/juridico/english/cyb_pan_manual.pdf
- Facultad de Ciencias Exactas, Ingeniería y Agrimensura, UNR. (s.f.). *Herramientas y Técnicas para la Auditoría Informática.* [Archivo PDF]. FECEIA. https://www.fceia.unr.edu.ar/asist/intro-aa-t.pdf
- Arocena, G. *Administración Fraudulenta.* [Archivo PDF]. CIIDPE. http://www.ciidpe.com.ar/area2/administracion%20fraudulenta.pdf