Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

CADENA DE CUSTODIA DIGITAL DE LAS EVIDENCIAS PARA LA REALIZACIÓN DE UN PERITAJE

Carlos Romeo García Dahinten

Asesorado por el Ing. Bayron Waldemar Duarte Illescas

Guatemala, febrero de 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

CADENA DE CUSTODIA DIGITAL DE LAS EVIDENCIAS PARA LA REALIZACIÓN DE UN PERITAJE

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

CARLOS ROMEO GARCÍA DAHINTEN
ASESORADO POR EL ING. BAYRON WALDEMAR DUARTE ILLESCAS

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, FEBRERO DE 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Sergio Alejandro Donis Soto
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Marlon Antonio Pérez Türk
EXAMINADORA	Inga. Floriza Felipa Ávila Pesquera
EXAMINADORA	Inga. Sonia Yolanda Castañeda Ramírez
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

CADENA DE CUSTODIA DIGITAL DE LAS EVIDENCIAS PARA LA REALIZACIÓN DE UN PERITAJE

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha octubre de 2013.

Carlos Romeo García Dahinten

Guatemala, 12 de Noviembre del 2013

Ingeniero
Carlos Azurdia
Coordinador del Área de Privados y Asesor de Tesis
Facultad de Ingeniería
USAC

Ingeniero Azurdia:

Por este medio le informo que el estudiante **CARLOS ROMEO GARCIA DAHINTEN**, carné **9420196**, ha finalizado todos los capítulos del trabajo de investigación titulado "CADENA DE CUSTODIA DIGITAL DE LAS EVIDENCIAS PARA LA REALIZACIÓN DE UN PERITAJE", el cual he tenido la oportunidad de revisar y doy mi aprobación del mismo.

Atentamente,

Ing. Bayron Waldemar Duarte Illescas
Colegiado No. 5161

Bayron Waldemar Duarte Illescas
Ingeniero en Ciencias de la Computación
Colegiado No. 5161

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 29 de Enero de 2014

Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **CARLOS ROMEO GARCIA DAHINTEN,** con carné **94-20196,** titulado: **"CADENA DE CUSTODIA DIGITAL DE LAS EVIDENCIAS PARA LA REALIZACIÓN DE UN PERITAJE",** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"CADENA DE CUSTODIA DIGITAL DE LAS EVIDENCIAS PARA LA REALIZACIÓN DE UN PERITAJE"****, realizado por el estudiante CARLOS ROMEO GARCÍA DAHINTEN, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Marlon Antonio Pérez Türk
Director, Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 21 de febrero 2014

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 079.2014

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **CADENA DE CUSTODIA DIGITAL DE LAS EVIDENCIAS PARA LA REALIZACIÓN DE UN PERITAJE,** presentado por el estudiante universitario: **Carlos Romeo García Dahinten,** autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

Guatemala, 24 de febrero de 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

/gdech

ACTO QUE DEDICO A:

Dios	Por ser mi guía en este camino llamado vida, por haberme dado la virtud, paciencia y sabiduría para finalizar una etapa más en mi vida, a Él todos mis logros dedicados con el corazón.
Mis padres	Romeo García y Ruth de García, por siempre haberme apoyado en los buenos momentos y en los difíciles, porque siempre me guiaron con sus sabios consejos y me alentaron a seguir adelante sin desfallecer.
Mis tíos	Sebastián Paredes y Elsa Irma de Paredes, por haber sido una importante influencia en mi carrera y aunque ya no estén entre nosotros a ustedes con cariño.
Mis abuelos	Por el cariño, la enseñanza y los valores que me inculcaron, un tributo terrenal hasta su morada eterna.
Mis hermanos y primos	Por estar ahí cuando los necesitaba y ser parte importante en mi vida.

AGRADECIMIENTOS A:

La tricentenaria Universidad de San Carlos de Guatemala	Viviré eternamente orgulloso de ser sancarlista.
Facultad de Ingeniería	Por abrirme las puertas al conocimiento, librándome de la ignorancia, formándome y desarrollando mis habilidades profesionales.
Mis compañeros	Por las palabras de aliento y la camaradería que me brindaron.
Ing. Waldemar Duarte	Por ser una importante influencia en mi carrera, su asesoría, tiempo y apoyo durante la elaboración de este trabajo de graduación.
Catedráticos	Por el saber y la enseñanza que me impartieron eternamente agradecido.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Core	Núcleo o parte central de un programa informático
DEFR	Digital Evidence First Responder, es la primera persona en procesar la evidencia digital
DES	Digital Evidence Specialist, es la persona encargada del análisis especializado de la evidencia digital
Framework	Marco de trabajo, es la una colección de métodos y procedimientos para realizar un trabajo
NAS	Network Attached Storage, se trata de una solución de almacenamiento en redes de computadoras.
SAN	Storage Area Network, es una red dedicada al almacenamiento.

RESUMEN

En Guatemala la cadena de custodia de las evidencias es un proceso informal que carece de regulaciones estrictas, y se sirve de prácticas parcialmente aceptadas por los entes respectivos que la utilizan.

Esto implica varios problemas en instituciones de alto desempeño y función pública: la carencia de directivas, normas y formalidades. Impactando la credibilidad del trabajo de análisis, asimismo, en la veracidad de las evidencias recolectadas y convirtiéndolas en sujetos de interpretaciones parcializadas.

El presente trabajo muestra un marco de investigación para la cadena de custodia de las evidencias digitales, tomando de referencia el núcleo del Framework de Seguridad Computacional del Gobierno de los Estados Unidos de América, con el objeto de utilizar las mejores prácticas para asegurar la autenticidad e integridad de las evidencias recolectadas y resguardadas por la cadena de custodia.

OBJETIVOS

General

Definir las acciones a seguir para garantizar el seguimiento de la cadena de custodia en evidencias digitales asegurando la integridad y autenticidad de la información recopilada.

Específicos

1. Proveer un marco de trabajo a seguir cuando se encuentren dispositivos digitales relacionados a una investigación.

2. Hacer ver la necesidad de que las evidencias digitales también son importantes.

3. Presentar una guía moderna para la cadena de custodia basada en el marco de trabajo de seguridad computacional.

INTRODUCCIÓN

Los delincuentes de hoy en día están utilizando la tecnología para facilitar el cometer afrentas a la ley y eludir a las autoridades. Este hecho ha creado la necesidad de que tanto la Policía, el Ministerio Público, Fiscalía y el Organismo Judicial deban especializarse y capacitarse en estas nuevas áreas, en donde las Tecnologías de Información y Comunicaciones se conviertan en herramientas necesarias en auxilio de la justicia y la persecución del delito y el delincuente.

La obtención de información (elementos de convicción) se constituye en una de las facetas útiles dentro del éxito en una investigación criminal, aspecto que demanda de los investigadores encargados una labor eficaz en cuanto a la recolección, preservación, análisis y presentación de las evidencias digitales, que garantice la autenticidad e integridad de dichas evidencias a fin de ser utilizadas posteriormente ante el tribunal correspondiente.

Este documento puede ser utilizado por instituciones públicas y privadas de alto desempeño, como guía o marco de trabajo para la recolección, preservación y presentación de evidencia digital, un área que aún no está enmarcada en la ley y regulada formalmente en Guatemala.

1. CADENA DE CUSTODIA

1.1. Concepto

El concepto primordial de una cadena es una serie de eslabones entrelazados, al integrar el término custodia se da a entender que es algo que requiere cuidado y resguardo, por lo tanto al hablar de la cadena de custodia se dice que es un procedimiento controlado que se utiliza sobre algo que necesita resguardo.

La cadena de custodia se basa e implica los siguientes aspectos: identificación, recolección, adquisición y preservación; donde la recolección está ligada al indicio del hecho u objeto, la adquisición es acorde al lugar donde se encontraba (en términos generales una fotografía de donde se encontró lo que se recolectó) y la preservación es acorde al procedimiento de resguardo.

1.2. Principios

La cadena de custodia de la evidencia se caracteriza por una serie de principios, que aseguran su funcionalidad y confiabilidad en instancias de juicio fundamentándose en los siguientes principios legales:

- Principio de aseguramiento de la prueba: surge de la necesidad de protección de los medios probatorios, del tiempo y del interés de las partes afectadas.

- Principio de la licitud de la prueba : se refiere a que los canales y medios de obtención de pruebas sean legales y estén debidamente establecidos

- Principio de la veracidad de la prueba: se basa en la obtención y preservación de una prueba libre de vicio y artimaña.

- Principio de la necesidad de la prueba: la prueba acredita el hecho, es decir que la prueba sea útil a la investigación probando un hecho.

- Principio de la obtención coactiva de la prueba: el estado emplea la coerción para garantizar la recaudación de la prueba.

1.3. Características

La caracterización de la cadena de custodia se da por una serie de rasgos distintivos que proveen una certificación del uso adecuado del proceso, entre las características distintivas de la cadena de custodia se encuentran:

- Esta formada por personas que tienen bajo su responsabilidad los elementos de prueba, por lo tanto toda persona que entre en contacto con estos, forma parte de la cadena de custodia.

- La cadena de custodia inicia desde la recolección de las pruebas y desde el conocimiento del delito, y finaliza con el juez y los funcionarios.

- La cadena de custodia es un proceso por escrito en toda su vida útil.

- La custodia se aplica a todo elemento probatorio físico. Extendiendo la misma a la documentación que acompañe al material.

- Los participantes son responsables de los procedimientos generales y específicos de la cadena de custodia.

- Los participantes son responsables del control y registro de su actuación directa en el proceso.

- Describe completamente los elementos de prueba, incluyendo detalles de lugar y persona que recolecto.

- Toda muestra o elemento probatorio tendrá el registro de cadena de custodia: fecha, hora, nombre y firma de quien recibe y de quien entrega.

Toda muestra o elemento probatorio y contra muestra o remanente de esta, deben llegar debidamente embalados y rotulados, de acuerdo con lo establecido en los manuales de los diferentes laboratorios criminalísticos y del Instituto de Medicina Legal y Ciencias Forenses.

Todo funcionario perito que analiza muestras o elementos de prueba dejará en el dictamen pericial constancia escrita de la descripción detallada de los mismos, de las técnicas y procedimientos de análisis utilizados, así como de las modificaciones realizadas sobre los elementos de prueba, mencionando si estos se agotaron en los análisis o si quedaron remanentes; este aspecto es muy importante cuando se analizan estupefacientes.

La cadena de custodia implica que tanto los elementos de prueba como los documentos que los acompañan, se deben mantener siempre en lugar seguro.

Los laboratorios criminalísticos o el Instituto Nacional de Medicina Legal y Ciencias Forenses podrán abstenerse de analizar elementos de prueba enviados por las autoridades competentes, cuando se compruebe que no ha existido cadena de custodia o que esta se ha interrumpido.

En el formato de cadena de custodia aparecerán las firmas de quien recibe y entrega en forma legible (nombres y apellidos claros), no rúbrica, tanto en el original como en la copia.

En el formato de cadena de custodia no se admiten tachones, borrones, enmendaduras, espacios y líneas en blanco, tintas de diferente color o interlineaciones (palabras o signos entre líneas), ni adiciones en la copia al carbón.

El formato de cadena de custodia se diligenciará completamente, teniendo en cuenta lo siguiente:

- Si existen o quedan espacios en blanco se anularán en cada renglón a continuación de la última palabra del texto con X y/o rayas.

- Cuando existan referencias a cantidades, valores o cifras, se expresarán en letras seguidas con el número correspondiente entre paréntesis.

- En caso de que se requiera mayor espacio para escribir del preestablecido en el formato de cadena de custodia, se deberá hacer mención de la continuidad con el siguiente texto “continúa al respaldo” y reiniciar con la palabra “continuación”. Seguidamente se consigna el texto faltante sin dejar espacios en blanco (véase primer viñeta), concluyendo con la firma y la fecha.

El control y el diligenciamiento del registro de cadena de custodia, continúa e inicia internamente en los laboratorios criminalísticos y forenses, en la oficina de correspondencia respectiva.

El registro de cadena de custodia se diligencia por todos y cada uno de los funcionarios por cuyas manos pase el material de prueba y los documentos que lo acompañan.

El funcionario de correspondencia o internamente en cada área, sección o laboratorio, responsable por la cadena de custodia, debe almacenar adecuadamente y en sitio seguro los oficios, petitorios, elementos de prueba y documentos anexos, que se reciben de las autoridades, garantizando la integridad y preservación de los mismos.

Si se presentan inconvenientes o inconsistencias en la revisión de cadena de custodia por parte de los jefes o responsables, se informará en forma inmediata al jefe directo, dejando la constancia de la anomalía detectada, por escrito.

Para evitar que se rompa un eslabón de la cadena de custodia en los laboratorios criminalísticos y forenses, se cumplirán normas de seguridad personal, industrial e instrumental.

Internamente, en los laboratorios se llevará un control, con la información suficiente de casos o respuestas pendientes.

1.4. Control

Para garantizar el control en la cadena de custodia se debe tomar en cuenta que la cadena de custodia es una herramienta que facilita la creación de controles en las siguientes áreas:

- Rutas: las rutas se refiere al camino que ha seguido la evidencia.

- Personal: se trata de las personas que en algún momento han estado en contacto con la cadena de custodia y su debido registro en la misma.

- Sistemas de seguridad: se trata de los sistemas de seguridad utilizados para resguardar las pruebas.

- Tiempos: los tiempos que han estado involucrados cada vez que hay un contacto con la cadena de custodia.

- Procedimientos de transferencia: papelería referente a los involucrados, y los procedimientos realizados para entrega y recepción de pruebas.

- Cambio de custodia: esto se refiere al cambio de la seguridad inherente a las pruebas.

- Observaciones: para registrar estado de la prueba e inconsistencias entre lo solicitado y lo recibido.

La creación de estos controles en cada área facilitará la auditoria. Uno de los controles que se debe observar de sobremanera es la seguridad referente a los registros de la cadena de custodia.

1.5. Objetivo

El objetivo de la cadena de custodia es el control de la integridad de la evidencia o prueba, al hablar de integridad se implica la protección contra el daño, contaminación, destrucción, alteración y sustitución.

Mediante de la cadena de custodia se garantiza la autenticidad de los elementos de prueba o evidencias, desde su identificación y recolección hasta la conclusión del proceso, identificando a las personas involucradas en la manipulación y análisis de la evidencia o pruebas.

1.6. Importancia

La importancia de la cadena de custodia radica en asegurar la integridad de las pruebas recolectadas identificando certeramente a las personas involucradas en la cadena, es decir todos las personas que tuvieron algún contacto con las evidencias, por mínimo e insignificante que este contacto fuera, también establecer la relación de la evidencia con el hecho, el sitio o lugar del hecho, asimismo los involucrados, víctima y victimario.

2. LA EVIDENCIA

La evidencia es una certeza clara y manifiesta de la que no se puede dudar. Las características fundamentales que la evidencia debe poseer son:

- Relevancia: una evidencia se considera relevante acorde al contexto del proceso.

- Confiabilidad: la confiabilidad de la evidencia es conforme a los pasos usados para obtenerla y la certeza que esta no ha sido alterada en ningún caso, desde su identificación, recolección, almacenaje y análisis hasta su presentación en el proceso que la requirió.

- Suficiencia: la evidencia debe ser suficiente para probar y justificar el hecho por el cual se recolecto.

2.1. Evidencia física

Al hablar de evidencia física se busca obtener elementos que permitirán conseguir información objetiva e imparcial que demostrará si el testigo dice la verdad o miente y se enmarca a los elementos físicos tangibles que se encuentran en una escena, tales como:

- Computador de escritorio.
- Computador portátil.
- Estación de trabajo.
- Hardware de red.

- Servidor.
- Teléfono celular.
- Teléfono Inteligente – misma funcionalidad de que el anterior con una amplia gama de servicios y aplicaciones con enfoque en acceso a internet y redes sociales.
- Teléfono inalámbrico.
- Aparato para identificar llamadas.
- Localizador - *beeper.*
- GPS – aparato que utiliza tecnología satélite capaz de ubicar geográficamente a la persona o vehículo que lo opera.
- Cámaras, videos.
- Sistemas de seguridad.
- Memoria flash – dispositivo que tiene capacidad almacenar información de diferentes formas y tamaños.
- Palm – asistente personal electrónico que almacena datos y posiblemente tiene conectividad inalámbrica con el Internet.
- Tablet – es una versión moderna del anterior, es propiamente un hibrido intermedio entre teléfono inteligente y computador personal portátil que tiene conectividad inalámbrica con el Internet.
- Juegos electrónicos – en su unidad de datos se puede guardar, incluso, una memoria de otro aparato.
- Sistemas en vehículos –computadoras obvias y computadoras del sistema operativo del vehículo que registra cambios en el ambiente y el mismo vehículo.
- Impresora.
- Copiadora.
- Grabadora.
- Videograbadora, DVD.

- Duplicadora de discos.
- Discos, disquetes, cintas magnéticas.
- Aparatos ilícitos – tales como los aparatos que capturan el número celular de teléfonos cercanos para después copiarlo en otros teléfonos, o los llamados analizadores de paquetes, decodificadores.

2.2. Evidencia digital

Es una denominación usada de manera amplia para describir cualquier registro generado o almacenado en un sistema computacional, que puede ser utilizado como prueba en un proceso legal y se refiere a la información contenida dentro de un elemento físico electrónico.

2.3. Información y elementos sujetos a investigación

Los crímenes y la evidencia potencial primaria asociada a la investigación se detalla en los elementos que pueden ser sujetos a la misma dentro del marco digital, los mismos no son exclusivos, es decir, una investigación de un tipo de crimen, puede obtener evidencia digital que demuestre otro. Por ejemplo, un crimen de homicidio puede proveer evidencia de otro de fraude.

2.3.1. Investigaciones de fraudes

Es cualquier acto ilegal caracterizado por el engaño, el ocultamiento o la violación de la confianza. Los fraudes son perpetrados por individuos y organizaciones, con el fin de obtener dinero, propiedades o servicios, evitar pagos o pérdida de servicios, asegurar una ventaja personal o del negocio.

Los elementos más comunes en una investigación digital de este tipo son:

- Datos de cuentas de subastas en línea
- Software de contabilidad y archivos
- Libretas de direcciones
- Calendario
- Registros de conversaciones
- Información de cliente
- Datos de tarjetas de crédito
- Bases de datos
- Software de cámara digital
- Correo electrónico, notas y cartas
- Registros financieros y de activos

2.3.2. Investigaciones de abuso infantil y pornografía

Las investigaciones de abuso infantil y pornografía en el campo digital, se extienden a elementos físicos que pueden contener evidencias digitales que prueben de manera contundente estos hechos, y se deben centrar en:

- Registros de conversaciones.
- Software de la cámara digital.
- Correo electrónico, notas y cartas.
- Juegos.
- Software de edición y visualización gráfica.
- Imágenes y películas.
- Registros de actividad de internet.
- Nombres de archivos y directorios que clasifican imágenes.

2.3.3. Investigaciones de intrusión en redes

Las intrusiones en las redes son uno de los problemas más frecuentes que afectan a miles de usuarios y empresas, estas intrusiones pueden incluso llevar a la quiebra por venta de información privilegiada a la competencia. Al investigar las intrusiones en el área digital es importante verificar los siguientes elementos:

- Libretas de direcciones.
- Archivos de configuración.
- Correos electrónicos, notas y cartas.
- Programas ejecutables.
- Registros de actividad de internet.
- Direcciones de protocolos de internet y nombres de usuarios.
- Registros de conversaciones por internet vía mensajes instantáneos.
- Código fuente.
- Archivos de texto y documentos con nombres de usuarios y contraseñas.

2.3.4. Investigaciones de homicidios

Este tipo de investigaciones involucran como resultado el privar de libertad al culpable de los hechos, por lo tanto se hace necesario seguir los procedimientos adecuados para obtener resultados confiables. Estas investigaciones en el área digital deben tener en cuenta:

- Libretas de direcciones
- Correos electrónicos, notas y cartas
- Registros de activos financieros
- Registros de actividad de internet

- Documentos legales y testamentos
- Registros médicos
- Registros telefónicos
- Diarios
- Mapas
- Fotos de víctima / sospechoso
- Fotos de trofeos

2.3.5. Investigaciones de violencia doméstica

Es todo patrón de conducta asociado a una situación de ejercicio desigual de poder, que se manifiesta en el uso de la violencia física, psicológica, patrimonial y/o económica o sexual. Para las investigaciones de violencia doméstica en el campo digital se deben tener en cuenta:

- Libretas de direcciones
- Diarios
- Correos electrónicos, notas y cartas
- Registros de activos financieros
- Registros telefónicos

2.3.6. Investigaciones de fraude financiero y falsificaciones

Estos se cometen en un entorno profesional o comercial con el objetivo de ganar dinero. Estos delitos no son violentos, pero ocasionan pérdidas a compañías, inversores y empleados.

En el campo digital las áreas de investigación son las siguientes:

- Libretas de direcciones
- Calendario
- Imágenes de cheques y órdenes de pago
- Imágenes de monedas
- Información de clientes
- Bases de datos
- Correos electrónicos, notas y cartas
- Identificaciones falsas
- Registros de activos financieros
- Imágenes de firmas
- Registros de actividad de internet
- Software bancario en línea
- Imágenes de falsificación de moneda
- Registros bancarios
- Números de tarjetas de crédito

2.3.7. Investigaciones de amenazas por correo electrónico, acoso y acecho

En este caso es el uso de información electrónica y medios de comunicación; tales como correo electrónico, redes sociales, boletines públicos, mensajería instantánea, mensajes de texto, teléfonos móviles y sitios web difamatorios para acosar a un individuo o grupo, mediante ataques personales u otros medios. Los principales elementos de prueba digital se pueden obtener investigando:

- Libretas de direcciones
- Diarios
- Correos electrónicos, notas y cartas
- Registros de activos financieros
- Imágenes
- Registros de actividad de internet
- Documentos legales
- Registros telefónicos
- Investigación de antecedentes de la víctima
- Mapas y ubicaciones de la víctima

2.3.8. Investigaciones de narcóticos

Los narcóticos comprenden gran variedad de drogas con efectos psicoactivos, aunque terapéuticamente no se usan para promover cambios en el humor, como los psicotrópicos, sino por otras propiedades farmacológicas, y en los peores casos son mal utilizados por sus efectos secundarios. Las investigaciones digitales en estos casos deben abarcar:

- Libretas de direcciones
- Calendario
- Bases de datos
- Recetas de drogas
- Correos electrónicos, notas y cartas
- Identificaciones falsas
- Registros de activos financieros
- Registros de actividad de internet
- Imágenes de recetas médicas

2.3.9. Investigaciones de piratería de software

La propiedad intelectual es un factor crucial para innovación tecnológica y la competitividad económica, es fundamental en el negocio de software y un incentivo para que los innovadores inviertan en investigación y desarrollo de productos que beneficiaran a sus clientes y a los consumidores en general. Al investigar esto, las áreas de interés principales en un entorno digital son:

- Registros de conversaciones
- Correos electrónicos, notas y cartas.
- Archivos de imágenes de certificados de software
- Registros de actividad de internet
- Números de serie de software
- Utilidades de software para ingeniería inversa
- Directorios de usuario y nombres de archivos que clasifican el software con derechos de autor

2.3.10. Investigaciones de fraude de telecomunicaciones

Este tipo de investigación se puede centrar en demostrar el uso indebido y no autorizado de los servicios de telecomunicaciones, siendo las principales áreas de investigación en un entorno digital las siguientes:

- Software de clonación
- Registros de la base de clientes
- Números de serie electrónicos, números de identificación móvil
- Correos electrónicos, notas y cartas
- Registros de activos financieros
- Registros de actividad de internet

2.3.11. Investigaciones de robo de identidad

El robo de identidad o usurpación de identidad es la apropiación de la identidad de una persona para hacerse pasar por ella, asumir su identidad ante otras personas en público o en privado y, en general, para acceder a ciertos recursos o la obtención de créditos y otros beneficios en nombre de esa persona. Las investigaciones en el área digital deben considerar:

- Hardware y herramientas de software
  - Telones
  - Lector / grabador de tarjetas de crédito
  - Software de la cámara digital
  - Software del escáner
- Plantillas de identificación
  - Actas de nacimiento
  - Tarjetas de cobro de cheques
  - Fotos digitales
  - Licencias de conducir
  - Firma electrónica
  - Matrículas de vehículos falsas
  - Falsificación de seguros
  - Tarjetas de seguro social
- Actividad de Internet relacionados con robo de identidad
  - Correo electrónico y grupos de noticias publicaciones
  - Documentos eliminados
  - Pedidos en línea
  - Información sobre la negociación en línea
  - Registros de actividad en internet

- Instrumentos negociables
    - Cheques de negocios
    - Cheques de caja
    - Números de tarjetas de crédito
    - Falsificación de documentos judiciales
    - Certificados de regalo falsificados
    - Falsificación de documentos de préstamo
    - Recibos de venta falsificados
    - Órdenes de pago
    - Cheques personales

3. PRINCIPIOS DEL PERITAJE

3.1. Objetividad

El perito debe ser objetivo, con independencia de la propia manera de pensar o de sentir, observando el código de ética profesional y favoreciendo a la neutralidad e imparcialidad dejando de lado la subjetividad.

3.2. Autenticidad

Durante toda la investigación debe conservar la autenticidad e integridad de los medios probatorios, es decir, todos los elementos deben estar debidamente identificados para su posterior acreditación de autenticidad.

3.3. Legalidad

El perito debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de su actividad pericial y cumplir con los requisitos establecidos por ella.

3.4. Idoneidad

Los medios probatorios deben ser auténticos, relevantes y suficientes para el caso, con lo cual reúnen las condiciones necesarias que permitirán que estos desempeñen su función.

3.5. Inalterabilidad

En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios de prueba no han sido modificados, alterados o cambiados durante la investigación.

3.6. Documentación

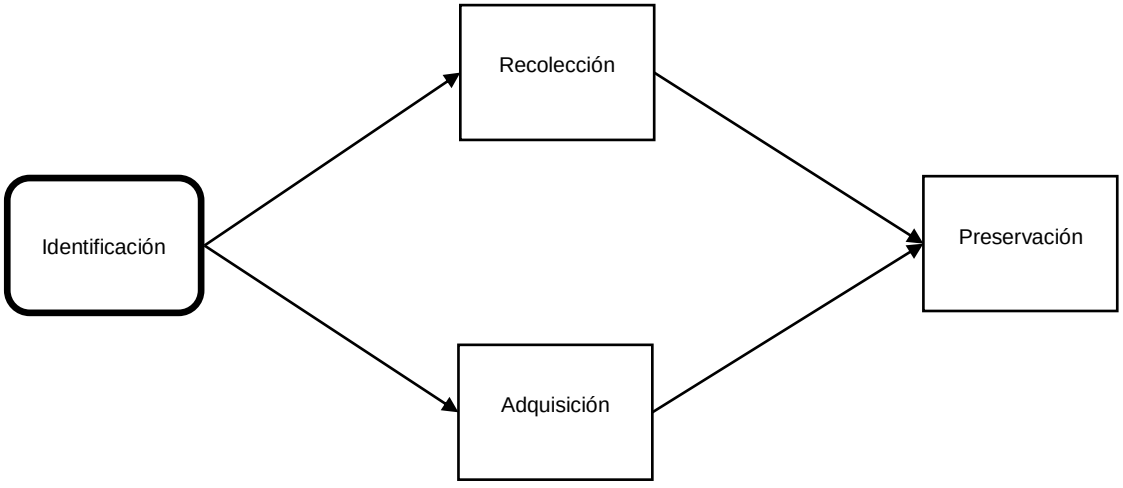
Se deberá establecer por escrito los pasos dados en el procedimiento de investigación, también los pasos llevados a cabo para el procesamiento de la información con la finalidad de informar los hechos.

4. ISO 27037 : DIRECTRICES PARA LA IDENTIFICACIÓN, RECOPILACIÓN, CONSOLIDACIÓN Y PRESERVACIÓN DE EVIDENCIA DIGITAL

La Normativa busca crear una línea base para la normalización internacional de prácticas digitales forenses, su objetivo es facilitar la usabilidad de la evidencia en distintas jurisdicciones, por procesos legales.

La Norma ISO 27037 solo cubre el proceso inicial del trabajo forense digital: identificación, obtención y preservación de la evidencia digital potencial.

Figura 1. **Proceso de manejo de evidencias acorde Norma ISO 27037**



Fuente: *Cloud Security Alliance, https://downloads.cloudsecurityallience.org/initiatives/imf/ Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf*.Consulta: 30 de septiembre de 2013.

4.1. Identificar

El proceso de análisis forense comienza con la identificación de los elementos que pueden ser o contener evidencia digital potencial. Formalmente, la identificación es el proceso que implica la búsqueda, el reconocimiento y la documentación de potencial evidencia digital.

Aunque la identificación de potencial evidencia digital suena simple en principio, existen complejidades sutiles. Por ejemplo, la evidencia digital tiene tanto una representación física y una virtual. Un disco duro con potencial de almacenar evidencia digital, la ubicación física de los datos es el disco duro, pero la propia evidencia viene de los datos contenidos en la unidad. Por otra parte, también puede no ser en absoluto obvia donde se aloja la potencial evidencia digital. Un servidor puede tener muy pocos discos conectados directamente y tienen una parte significativa de su almacenamiento dentro de un SAN o NAS (Storage Area Network o Network Attached Storage).

4.2. Recolectar y adquirir

Una vez identificada la potencial evidencia digital, debe ser o bien recogida u adquirida para su procesamiento, para el efecto hay que tener en cuenta las diferencias entre los conceptos:

- Colección: proceso de recopilación de artículos, que contengan potencial evidencia digital.

- Adquisición: proceso de creación de una copia de los datos en un conjunto definido.

Colección es más o menos equivalente a la práctica de aplicación de la ley estándar de aprovechar los elementos que contengan potencial evidencia digital bajo la autoridad de un orden jurídico (es decir, una orden de registro) y el envío de ellos a un laboratorio forense u otro centro para el procesamiento y análisis. La adquisición es más común en el sector privado debido a la necesidad de minimizar el impacto, de una investigación en curso, en el negocio.

Cabe señalar que la copia creada durante la adquisición puede variar desde la creación de una imagen forense de una unidad de disco duro, a una copia de los contenidos de la memoria de un servidor, hasta los contenidos lógicos de casilla de correo electrónico de un usuario individual, dependiendo del propósito y alcance de la investigación.

En todos los casos, los requisitos para la copia son muy similares: debe hacerse mediante un proceso bien conocido, defendible y bien documentado. Además, el proceso debe incluir medidas de integridad para asegurar que la copia no se ha modificado desde la adquisición. La amplia variedad de la potencial evidencia digital a copiar, y los requisitos del proceso de copia, hacen de la adquisición un proceso más complejo y difícil que el de colección.

4.3. Preservar

Una vez que la potencial evidencia digital ha sido recolectada o adquirida, que debe ser preservada. La Normativa ISO 27037 define la conservación como el proceso de mantener y salvaguardar la integridad y / o el estado original del potencial de la evidencia digital.

La preservación del potencial de evidencia digital es un proceso complejo e importante. Ayuda a asegurar la preservación de pruebas admisibles ante un

tribunal de justicia. Sin embargo, la evidencia digital es notoriamente frágil y se cambia o se destruye fácilmente.

Teniendo en cuenta que el trabajo del laboratorio forense digital oscila entre seis meses a un año (y que los retrasos en el sistema legal podrían crear nuevos retrasos), el potencial de la evidencia digital puede pasar un período de tiempo significativo en almacenamiento antes de que se analice o se utilice de forma legal.

Este almacenamiento requiere estrictos controles de acceso para proteger los artículos de la modificación accidental o deliberada, así como los controles de entorno apropiados.

4.4. Requerimientos generales

Los requerimientos generales para la Normativa ISO 27037, se llenan al cumplir con los principios de auditabilidad, repetibilidad, reproducibilidad y justificabilidad definidos por la misma.

4.4.1. Auditable

Debería ser posible que un evaluador independiente o de otras partes interesadas acreditadas para evaluar las actividades realizadas por un DEFR[1] y DES[2]. Esto requiere la documentación apropiada en relación con las medidas adoptadas, por qué y cómo.

[1] DEFR es una acrónimo en inglés que significa Digital Evidence First Responder
[2] DES es un acrónimo en inglés que significa Digital Evidence Specialist

4.4.2. Repetible

La repetibilidad se establece cuando los mismos resultados de la prueba, se reproducen bajo las siguientes condiciones definidas por la Normativa ISO 27037:

- Usando el mismo procedimiento de medición y método
- Utilizando los mismos instrumentos y en las mismas condiciones
- Se puede repetir en cualquier momento después de la prueba inicial

4.4.3. Reproducible

La reproducibilidad se establece cuando los mismos resultados de la prueba se producen bajo las siguientes condiciones definidas por la Normativa ISO 27037:

- Utilizando el mismo método de medición
- El uso de diferentes instrumentos y bajo diferentes condiciones
- Puede ser reproducido en cualquier momento después de la prueba inicial

4.4.4. Justificable

El DEFR debe ser capaz de justificar todas las acciones y los métodos utilizados, por lo cual la Normativa ISO 27037 provee las herramientas necesarias para el efecto.

4.5. Manejo de la evidencia digital

La falta de preparación y conocimiento de los procedimientos para manejar la evidencia digital, lleva muchas veces a privilegiar la continuidad de las operaciones del negocio, sin averiguar de donde provino el ataque o cual fue el grado de impacto y afectación.

4.5.1. General

La evidencia digital potencial se suele obtener en el campo o en un área, que por lo general se encuentra fuera de nuestro control, por lo tanto la misma debe ser tratada de acuerdo con los siguientes principios:

- Minimizar el manejo.
- Registro de cambios y acciones que se han tomado.
- Cumplir con las normas locales para las pruebas.
- No tomar acciones más allá de la propia competencia.

4.5.2. Identificación

La búsqueda, el reconocimiento y la documentación del potencial de la evidencia digital, deben llevarse a cabo de acuerdo con los siguientes principios:

- Dar prioridad a la recopilación de pruebas sobre la base de volatilidad.
- Reduzca al mínimo el daño a la potencial evidencia digital.
- Identificarla evidencia digital oculta.

4.5.3. Colección

La colección es un proceso en el proceso de manejo de la evidencia digital en donde los dispositivos que pueden contener pruebas digitales se envían de su ubicación original a un laboratorio u otro ambiente controlado para su posterior adquisición y análisis

4.5.4. Adquisición

El proceso de crear una copia de un elemento de potencial evidencia digital, por lo general la adquisición se da en sistemas donde interrumpir el flujo de información del negocio puede provocar pérdidas monetarias o humanas.

4.5.5. Preservación

La preservación es la protección de la integridad de la potencial evidencia digital. La potencial evidencia digital y dispositivos digitales, deben ser salvaguardados y protegidos de la manipulación o de expoliación.

5. LA CADENA DE CUSTODIA EN EL MARCO DE TRABAJO DE SEGURIDAD COMPUTACIONAL

Las necesidades de seguridad de las instituciones varían conforme a sus requerimientos y presupuestos, por lo cual se hace necesario de un marco de trabajo flexible y adaptable. El núcleo del marco de trabajo de Seguridad Computacional presenta las características requeridas para el caso.

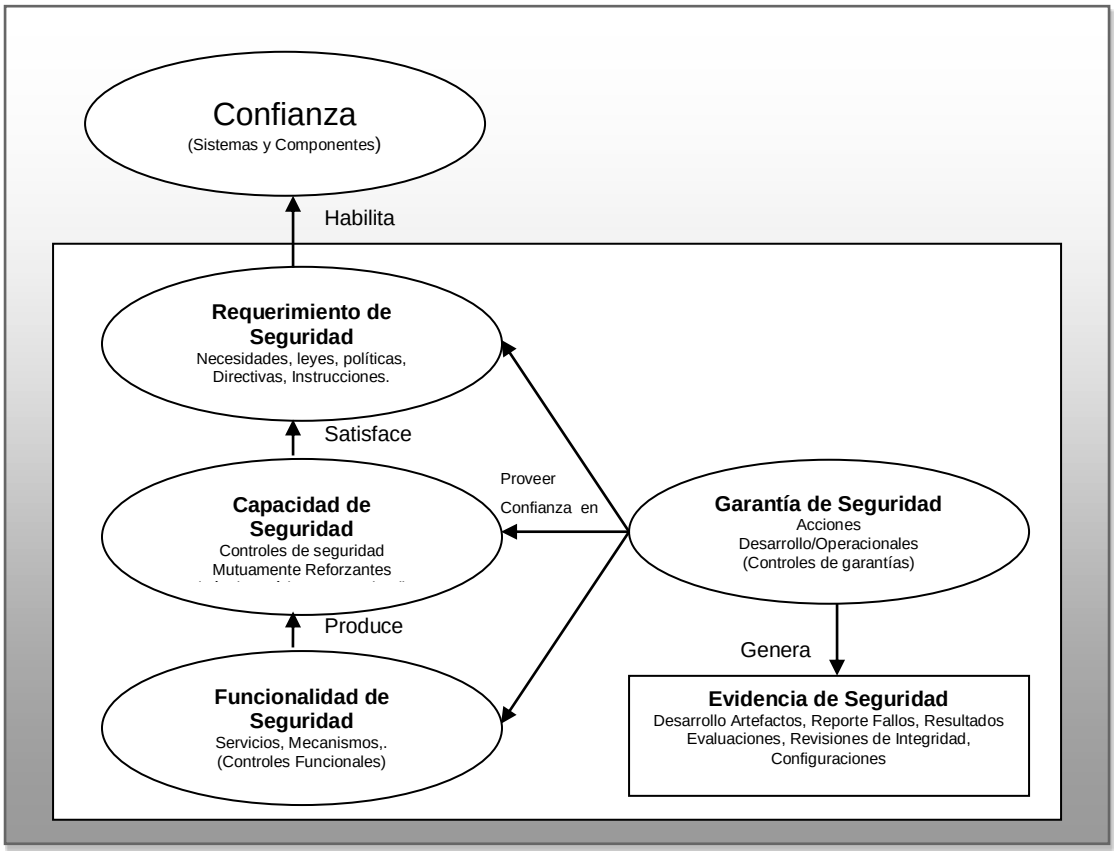
Tabla I. **Estructura del núcleo del marco de trabajo de seguridad computacional**

Framework Core			
Funciones	**Categorias**	**Subcategorias**	**Referencias**
Identificar			
Proteger			
Detectar			
Responder			
Recuperar			

Fuente: *National Institute of Standards, Discussion Draft of the Preliminary Cybersecurity Framework. p.4.*

Teniendo en cuenta que lo más importante dentro de la cadena de custodia es la integridad, la confiabilidad es de suma importancia tal y como se muestra a continuación:

Figura 2. **Modelo de confianza**



Fuente: *National Institute of Standards, Security and Privacy Controls for Federal Information Systems and Organizations*.p.24.

5.1. Identificar

Al identificar los elementos que pueden contener potencial evidencia digital, se debe tomar en consideración la administración de activos, la gobernanza, las evaluaciones de riesgos y la estrategia a seguir para la administración del riesgo.

5.1.1. Administración de activos

Identificar y administrar al personal que tiene contacto con la escena, y a las personas accesibles que pueden ser objeto de recolección. Se debe identificar todo lo que puede ser sujeto a proceso o análisis, incluso lo que pasa durante la recolección.

- Inventario y rastreo de dispositivos físicos y sistemas.
- Inventario de plataformas de software y aplicaciones.
- Identificar redes y conexiones.
- Identificar sistemas externos de servicio, procesamiento y almacena-miento.

5.1.2. Gobernanza

Identificar requerimientos legales y regulatorios que den garantía y soporte a lo recolectado bajo la categoría de administración de activos, con lo cual se provee la base legal para la cadena de custodia.

- Identificando políticas de seguridad de la información.
- Identificando roles de seguridad, responsabilidad y coordinación.
- Identificando requerimientos legales regulatorios.

5.1.3. Evaluación del riesgo

Consisten en evaluar el riesgo constantemente en las operaciones de la cadena de custodia digital, este es un proceso delicado que puede involucrar directamente a la prueba y su veracidad para lo cual hay que:

- Identificar las amenazas a la información digital.
- Identificar las amenazas a los activos de la información tanto externas como internas.
- Identificar el impacto potencial.

5.1.4. Estrategia de administración del riesgo

Identificar los supuestos específicos, limitaciones, tolerancia al riesgo y las prioridades/compensaciones utilizados dentro de la organización para apoyar las decisiones de riesgo operacional.

- Identificar y establecer procesos de administración del riesgo.
- Determinar los umbrales de alerta de incidentes.

5.2. Proteger

La protección de los elementos de prueba es indispensable, ya que una alteración, modificación, manipulación o extracción indebida puede llevar a término una investigación digital o en el peor de los casos a una condena inadecuada.

5.2.1. Control de acceso

Limitar el acceso de los usuarios autorizados a la información o los dispositivos (incluyendo otros sistemas de información) y los tipos de operaciones y funciones que los usuarios autorizados se les permite ejercer.

- Administración de credenciales de usuarios y dispositivos
- Reforzar controles de acceso físico a la evidencia
- Evitar accesos remotos y restringir dispositivos móviles
- Implementar controles de acceso basados en roles y atributos

5.2.2. Entrenamiento y concientización

El personal está adecuadamente capacitado para llevar a cabo su función, informando, asignado deberes y responsabilidades relacionadas con la seguridad a través de actividades de sensibilización y formación.

5.2.3. Seguridad de los datos

Proteger la información y registros (datos) de los peligros naturales y de origen humano para lograrla confidencialidad, integridad, y los requisitos de la cadena de custodia.

- Proteger la evidencia digital en el almacenamiento.
- Proteger la evidencia digital en el transporte.

5.2.4. Procesos de protección de la información y procedimientos

Asegurar la protección adecuada a través de la política de planificación de la seguridad (que se ocupa del propósito, el alcance, las funciones, las responsabilidades, compromiso de la dirección, la coordinación entre las entidades de la organización) y los procedimientos para facilitar su aplicación.

Proteger la información mediante la realización de copias de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información de copia de seguridad, almacenamiento correcto de la información con copia de seguridad y las pruebas periódicas para asegurar la recuperabilidad de los datos y la eficacia de los procesos.

5.2.5. Tecnologías de protección

Implementar soluciones técnicas de seguridad alineando las decisiones de riesgo con el marco de trabajo de seguridad computacional.

Determinar, documentare implementar la auditoria física y lógica del sistema y los registros de sucesos de conformidad con la política de auditoría.

5.3. Detectar

Esta función se centra en la detección de anomalías y eventos que conlleva un monitoreo continuo, y una revisión que puede incluir actualizaciones en los procesos de detección.

5.3.1. Anomalías y eventos

Detectar actividad anómala y determinar el posible impacto de los acontecimientos acorde a los objetivos de la organización, tal como se establezca en la función de protección.

5.3.2. Monitoreo continuo de seguridad

Seguimiento, control y gestión de los aspectos de seguridad computacional de desarrollo y operación (por ejemplo, productos, servicios, manufactura, procesos de negocio y tecnología de la información) para identificar los eventos de seguridad cibernética.

5.3.3. Procesos de detección

Garantizar el nivel de sensibilidad adecuado y oportuno de los acontecimientos anómalos a través de los procesos y procedimientos de detección implementados.

5.4. Responder

La respuesta va en función de la detección e incluye una planificación de la respuesta, establecer los canales de comunicación pertinentes, analizar el incidente, mitigar los efectos y mejorar el nivel de respuesta a eventos.

5.4.1. Planificar la respuesta

Asegurar la protección adecuada a través de las políticas, los procedimientos, las prácticas y la coordinación, para implementar las acciones organizativamente acordadas después de la detección (o anticipación) de los eventos de seguridad.

5.4.2. Comunicar

Coordinar la respuesta con las partes interesadas internas y externas, según corresponda, para incluir el apoyo externo en los eventos de aplicación de la ley.

5.4.3. Analizar

Llevar a cabo actividades de análisis en curso, en relación con la función de responder, para garantizar las actividades de recuperación y apoyo a la respuesta adecuada.

- Clasificación de incidente
- Alcances del incidente
- Análisis forense
- Anomalías
- Impacto

5.4.4. Mitigar

Esta función se centra en llevar a cabo las actividades para prevenir un evento, mitigar o minimizar sus efectos y erradicar el incidente para regresar de una pronta manera a la normalidad del sistema.

- Contener
- Reforzar controles

5.4.5. Mejorar

Mejorar la respuesta de la organización al incorporar las lecciones aprendidas a partir de la detección y las actividades de respuestas actuales y anteriores.

- Actualizar estrategias de respuesta
- Incorporar cosas aprendidas

5.5. Recuperar

La recuperación tiene su base en la protección y acorde al nivel de protección alcanzado, es el nivel de recuperación obtenido. A partir de esto se debe considerar el planificar la recuperación, incluso la adición de posibles mejoras.

5.5.1. Planificar recuperación

Ejecutarlas actividades del plan de recuperación para lograr la restauración de los servicios o funciones, que retornen el sistema a un estado anterior a un evento.

5.5.2. Mejoras

Mejorar la planificación y los procesos de recuperación mediante la incorporación de las lecciones aprendidas en los procesos de identificación, protección, detección y respuesta en las actividades futuras.

6. GUÍA PARA LA CADENA DE CUSTODIA DIGITAL

La siguiente tabla está basada en los conceptos anteriormente expuestos, se propone un perfil basado en el criterio de necesidad de recuperación e información detallada.

Tabla II. **Perfil de cadena de custodia digital**

	Recolectar	Adquirir	Preservar	Examinar	Analizar	Reportar	Documentar
Identificar	B	I	A	A	A	I	B
Proteger	B	I	B	B	B	A	B
Detectar	B	B	B	B	A	B	B
Responder	I	A	B	A	I	I	B
Recuperar	B	B	B	B	B	B	B

Fuente: elaboración propia.

Leyenda

- B (básico)
- I (intermedio)
- A (avanzado)

6.1. Ejemplo de un flujo de una cadena de custodia digital

En una cadena de custodia digital el flujo de trabajo siempre está enmarcado en una base temporal, en la evidencia y en el funcionario que tiene potestad de la misma en ese marco temporal.

6.1.1. Tiempo

El tiempo es uno de los elementos primordiales de una cadena de custodia y debe ser el primer elemento que se registra dentro de la misma como parte de su control y seguimiento.

- Recibido (entregas a y de bodega)
- Apertura (fecha inicio)
- Finalización (fecha fin)
- Horas de trabajo

6.1.2. Identificación

El elemento de identificación es primordial junto al tiempo, ya que ambos enmarcan la potestad de un funcionario o institución, sobre un elemento de prueba digital dentro de la cadena de custodia.

- Persona que solicita el análisis
- Numero de autorización
- Autoridad (entidad que solicita)
- Nombre del caso
- Número de caso
- Prioridad (1 2 3 4 5)
- Clasificación del caso (reservado, urgente, alto impacto, normal)

6.1.3. Descripción general

La descripción general de la cadena de custodia provee las características del examinador de la evidencia, así como las características y las condiciones propiamente dichas de la evidencia.

- Examinador / analista asignado
- Identificación del analista
- Número de evidencia
- Sistema operativo
- Sistema de archivos
- Datos a analizar (tamaño)

6.1.4. Protección

La protección de la evidencia es indispensable dentro del marco de trabajo en una cadena de custodia digital, ya que los métodos para obtener información de la evidencia pueden provocar la pérdida de la misma, con lo cual es importante asegurar su protección e integridad para evitar un posterior repudio.

- Medios externos
- NAS
- Respaldo

6.1.5. Detección

Es parte del proceso de búsqueda de evidencia potencial, que requiere un registro detallado de acciones, ya que este proceso puede llevar a disparar un proceso de borrado, virus o inhabilitación que puede afectar la evidencia de manera parcial o total.

- Registro detallado de las acciones realizadas sobre la evidencia digital
- Marcas de tiempo: creación, modificado, opcional (eliminado)
- Nombre, extensión y permisos (propietarios)
- Características(escondido, del sistema, protegido)

6.1.6. Responder

La respuesta es la parte del flujo de cadena de custodia que se encarga de registrar e informar los hallazgos que se dieron en el transcurso de la misma a la entidad competente, el documento para el efecto debe contener las firmas del investigador, supervisor y sello de la institución..

6.1.7. Recuperar

La recuperación se puede dar en cualquier momento, ya que todos y cada uno de los pasos puede comprometer la evidencia de forma parcial o total, el proceso de recuperación tiene por objetivo, el dejar a disposición la evidencia en el estado original en que se encontró y se registró inicialmente dentro de la cadena de custodia digital.

- Restaurar evidencia comprometida
- Restaurar evidencia destruida por algún efecto programado

CONCLUSIONES

1. El marco de trabajo de seguridad computacional es una herramienta que provee una estructura viable para la cadena de custodia digital, ya que la evidencia digital en el caso de un proceso penal requiere de todas las medidas necesarias para la preservación de la prueba, evitar una invalidación por malos manejos o contaminación, para lo cual, se presenta una recopilación de los métodos, procedimientos y técnicas más comunes.

2. Se aporta un marco de trabajo base que es flexible y extensible, de acuerdo a las necesidades de la cadena de custodia que se extiende hacia el ambiente digital, como medio de protección de documentos o archivos digitales que serán utilizados como medio de prueba.

3. La evidencia digital es un indicio de un hecho, el cual se encuentra dentro de un elemento físico de índole electrónica, que por sus características es necesario aplicar consideraciones adicionales.

4. La cadena de custodia digital, pone en contexto las evidencias digitales y el proceso para su identificación, búsqueda, discriminación, selección, recolección y custodia.

5. La cadena de custodia digital, debe hacerse con una firma de tiempo cronológica de fecha y hora, siendo lo ideal en el momento de la intervención contar con un archivo generado por una autoridad certificadora abierta, que avale al investigador, la fecha, la hora, el proceso y el lugar, lo cual garantiza la integridad del archivo.

RECOMENDACIONES

1. La cadena de custodia de la evidencia digital debe regirse estrictamente en normas y procedimientos confiables que minimicen la manipulación de los dispositivos que la contienen, dada la naturaleza de su volatilidad.

2. Es importante hacer ver que existen dos situaciones de cadena de custodia, el dispositivo con la información y la información en sí, por lo que es necesario tener cuidado en la naturaleza de la evidencia. Si el dispositivo es prueba debe consignarse en la respectiva cadena de custodia, y si un archivo digital es prueba, el análisis de la información debe detallar el procedimiento realizado, dentro de la cadena de custodia de la evidencia digital.

3. Para aplicar los conceptos aquí mencionados hay que tomar en consideración que es una decisión de alto nivel en la que debe estar comprometida toda la institución, desde el nivel ejecutivo hasta el nivel operacional, incluyendo infraestructura, presupuesto, riesgos y cuya realización puede implicar varios meses, incluso años, dependiendo del nivel de trabajo, personal y presupuesto disponibles.

4. Es necesario reconocer y regular la existencia de la evidencia digital y sus implicaciones, para lo cual se requiere que las instituciones estén preparadas, capacitadas y respaldadas por leyes para el efecto.

BIBLIOGRAFÍA

1. International Standards Organization. *ISO 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence*. [en línea]. http://www.iso.org/iso/catalogue_detail?csnumber=44381. 2012 [Consulta: 30 de septiembre de 2013].

2. Real Academia Española. *Diccionario de la Lengua Española*. [en línea] http://rae.es/recursos/diccionarios/drae. [Consulta: 10 de octubre 2013].

3. Cloud Security Alliance, *Mapping the Forensic Standard ISO IEC 27037 to Cloud Computing*. [en línea]. https://downloads.cloud securityallience.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf. [Consulta: 15 de octubre de 2013].

4. MONZÓN SOTO, Blanca Aracely. *La cadena de custodia de evidencias en el proceso penal guatemalteco*. Trabajo de graduación de Lic. en Ciencias Jurídicas y Sociales. Universidad de San Carlos de Guatemala, Facultad de Derecho. 2012. 92 p

5. National Institute of Justice. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* [en línea]. http://www.nij.gov/pubs-sum/199408.htm. [Consulta: 18 de octubre de 2013].

6. U.S. Department of Homeland Security. *Best Practices for Seizing Electronic Evidence v.3: A Pocket Guide for First Responders*. [en línea] https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=239359. [Consulta: 25 de septiembre de 2013].

7. National Institute of Standards. *Discussion Draft of the Preliminary Cybersecurity Framework*. [en línea].http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf [Consulta: 15 de septiembre de 2013].

8. _____. *Security and Privacy Controls for Federal Information Systems and Organizations.* [en línea]. http://dx.doi.org/10.6028/NIST.SP.800-53r4. [Consulta: 30 de septiembre de 2013].

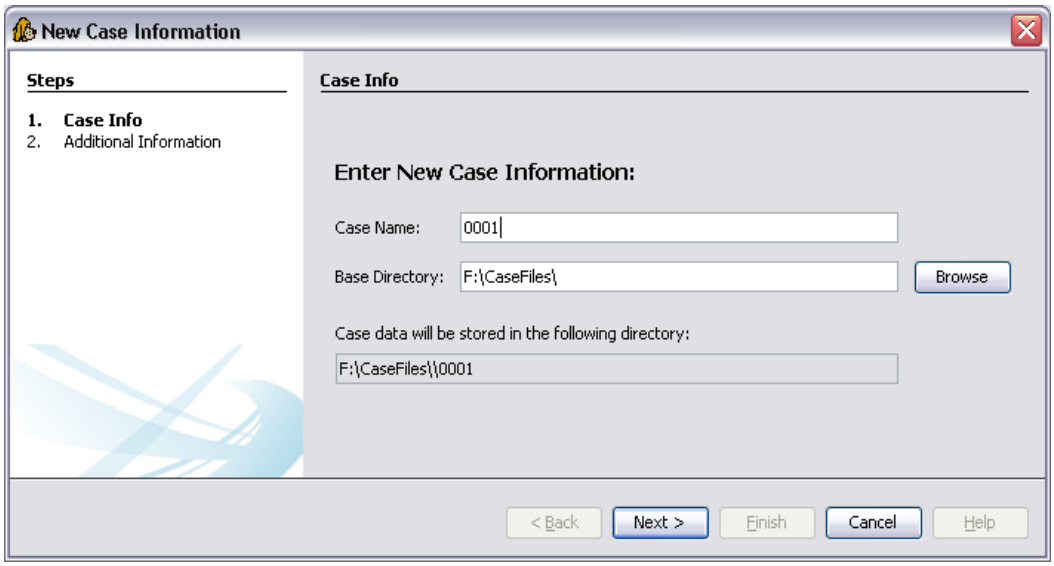
ANEXO

Software de código libre para la cadena de custodia digital

La herramienta con mayor aceptación de código abierto de distribución libre es Autopsy, cuyo marco de trabajo Sleuth Kit, ha recibido el apoyo inicial del *U.S. Army Intelligence Center of Excellence* para aplicar el procesamiento de los casos en la nube para acelerar su procesamiento, es una herramienta enfocada al análisis con capacidad para mantener la cadena de custodia digital.

- Características:
    - Control del nombre del caso
    - Control del directorio del caso (preferente una ubicación con capacidad de replicación)

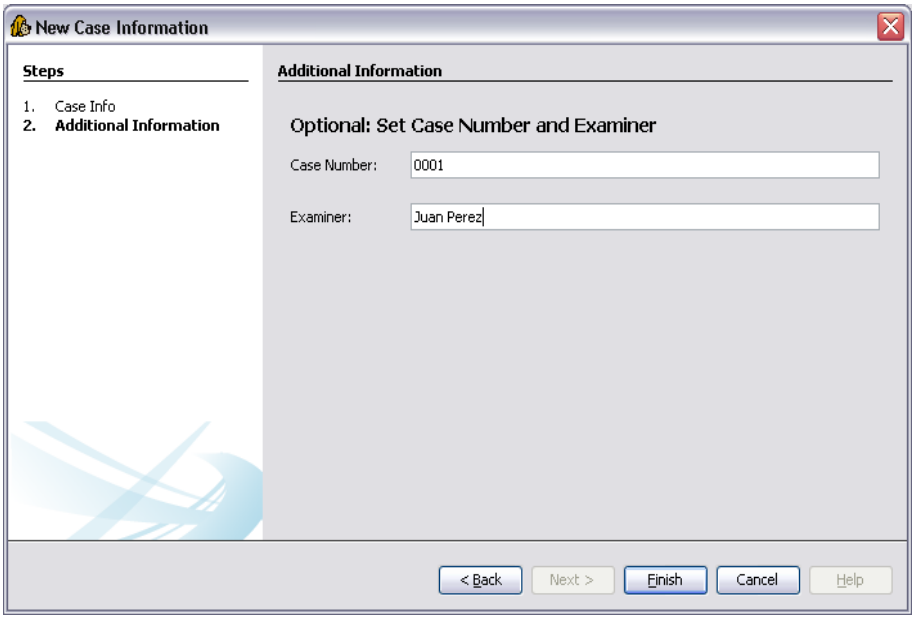
Figura A. **Creación de un caso nuevo**



Fuente: programa de código abierto *Autopsy* [disponible en línea http://www.sleuthkit.org/autopsy/]

- Control del número de caso
- Control del examinador o encargado de la evidencia digital

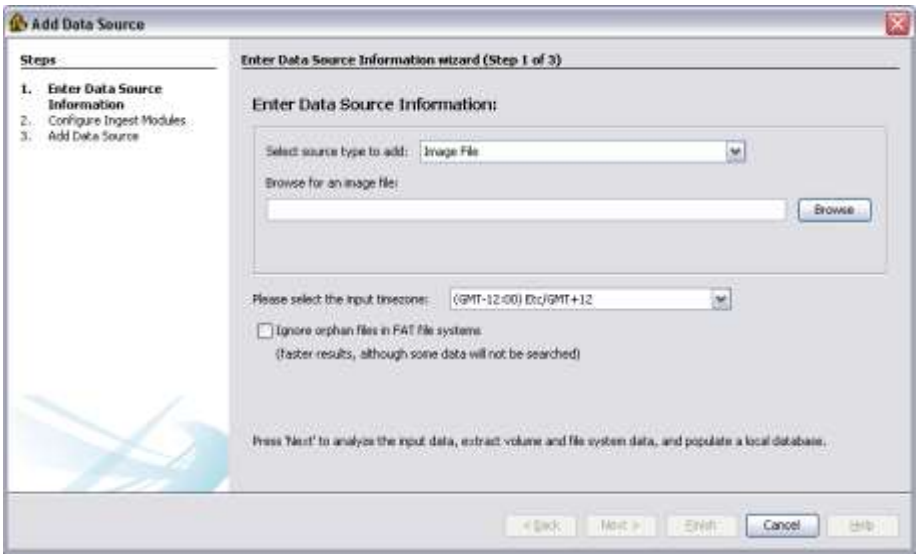
Figura B. **Información del caso**



Fuente: programa de código abierto *Autopsy* [disponible en línea http://www.sleuthkit.org/autopsy/]

- Control de datos a examinar:
  - Imágenes
  - Discos físicos
  - Datos lógicos
- Control de tiempo (fecha y hora con formato GMT)

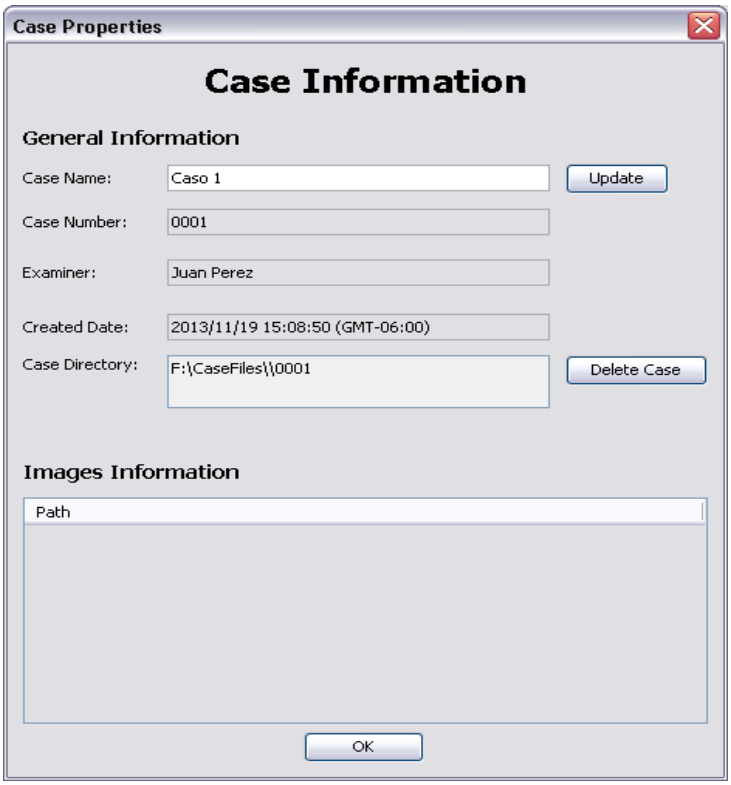
Figura C**. Identificacion de las fuentes de informacion y marcas de tiempo**



Fuente: programa de código abierto *Autopsy*[disponible en línea http://www.sleuthkit.org/autopsy/]

- Resumen de un caso
  - Nombre del caso
  - Número del caso
  - Examinador
  - Marca temporal de creación
  - Directorio del caso
  - Información de imágenes digitales de evidencias relacionadas al caso

Figura D. **Resumen de un caso**



Fuente: programa de código abierto *Autopsy* [disponible en línea http://www.sleuthkit.org/autopsy/]

Esta herramienta llena las necesidades de la cadena de custodia digital, sin embargo, hay que hacer notar que se requiere seguir con la cadena de custodia a nivel físico, es decir, seguir el proceso de registro manual, en el cual se detalla todo lo que el examinador realizó.