IFCT0109. SEGURIDAD INFORMÁTICA

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

UD06

UNIDAD 06. ANÁLISIS FORENSE INFORMÁTICO

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. **INTRODUCCIÓN**
2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE
3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD
4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS
5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS
6. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

1. INTRODUCCIÓN

LA INFORMACIÓN DE LAS EMPRESAS Y ORGANIZACIONES **SE HA CONVERTIDO** EN **UN** ASPECTO **ATRACTIVO PARA ATACANTES** QUE SE DEDICAN A GENERAR INTRUSIONES Y USOS INDEBIDOS CON FINES DE LO MÁS VARIADO.

1. INTRODUCCIÓN

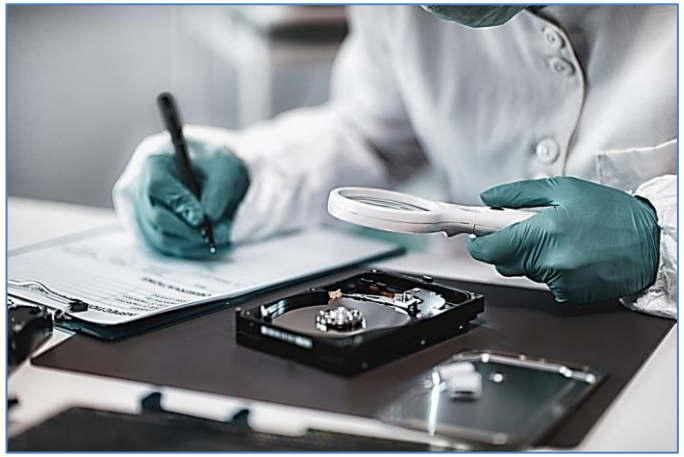
AUNQUE LA CANTIDAD DE HERRAMIENTAS Y SISTEMAS DE PROTECCIÓN SEA LA ADECUADA, **SIEMPRE ES POSIBLE QUE OCURRA CUALQUIER INCIDENTE.**

POR ELLO **ES NECESARIO DETECTAR AL RESPONSABLE PARA PODER RECLAMARLE EXIGENCIAS LEGALES Y ECONÓMICAS** SI PROCEDE.

1. INTRODUCCIÓN

UNA DE LAS PRINCIPALES HERRAMIENTAS PARA CONSEGUIR DETECTAR A ESTOS RESPONSABLES ES EL **ANÁLISIS FORENSE INFORMÁTICO.**

ES UNA CIENCIA QUE SE DEDICA A ***OBTENER HUELLAS*** **EN LOS INCIDENTES SUCEDIDOS** PARA LOGRAR ENCONTRAR A UN CULPABLE DE UN MODO RAZONABLE Y CORRECTAMENTE JUSTIFICADO.



1. INTRODUCCIÓN

SE DESARROLLA EL **CONCEPTO DE INFORMÁTICA FORENSE**, SUS **PROCESOS Y** LAS MEJORES **HERRAMIENTAS** PARA OBTENER UNOS RESULTADOS MÁS EFECTIVOS.

CONTENIDOS

1. INTRODUCCIÓN
2. **CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE**
3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD
4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS
5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS
6. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

EL **ANÁLISIS FORENSE** ES UNA DISCIPLINA DENTRO DE LA SEGURIDAD INFORMÁTICA CUYA **FUNCIÓN ES ANALIZAR LOS INCIDENTES DE SEGURIDAD A POSTERIORI CON LA FINALIDAD DE RECONSTRUIR LOS HECHOS** PARA RESPONDER PREGUNTAS COMO:

- ¿QUIÉN HA SIDO EL ATACANTE?
- ¿CÓMO SE HA PRODUCIDO EL INCIDENTE DE SEGURIDAD?
- ¿CUÁLES HAN SIDO LAS VULNERABILIDADES EXPLOTADAS?
- ¿CUÁLES FUERON LAS ACCIONES DEL INTRUSO CUANDO CONSIGUIÓ ACCEDER AL SISTEMA?

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

OBJETIVOS Y USOS DE LA INFORMÁTICA FORENSE

EL ANÁLISIS FORENSE INFORMÁTICO CONSISTE EN ***CAPTURAR, PROCESAR E INVESTIGAR LA INFORMACIÓN DE LOS SISTEMAS INFORMÁTICOS EN BÚSQUEDA DE EVIDENCIAS UTILIZANDO LA METODOLOGÍA APROPIADA PARA QUE LA INVESTIGACIÓN PUEDA UTILIZARSE CON FINES LEGALES***.

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

OBJETIVOS Y USOS DE LA INFORMÁTICA FORENSE

EL **OBJETIVO PRINCIPAL** DE ESTA METODOLOGÍA **ES RECOGER LAS EVIDENCIAS DIGITALES PRESENTES EN CUALQUIER TIPO DE INCIDENCIA Y DELITO INFORMÁTICO**.

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

OBJETIVOS Y USOS DE LA INFORMÁTICA FORENSE

ADEMÁS DE ESTE OBJETIVO PRINCIPAL HAY QUE DESTACAR OTROS **OBJETIVOS SECUNDARIOS**:

- COMPENSAR LOS DAÑOS CAUSADOS POR LOS INTRUSOS
- PERSEGUIR Y APLICAR MEDIDAS JUDICIALES A LOS ATACANTES
- CREAR E IMPLANTAR MEDIDAS PARA PREVENIR INCIDENTES FUTUROS SIMILARES

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

OBJETIVOS Y USOS DE LA INFORMÁTICA FORENSE

LOS **USOS DE LA INFORMÁTICA FORENSE** PUEDEN SER:

- **PERSECUCIÓN CRIMINAL**
- **LITIGACIÓN CIVIL**
- **INVESTIGACIÓN DE SEGUROS**
- **MANTENIMIENTO DE LA LEY**
- **USUARIO FINAL**
- **ORGANIZACIONES Y TEMAS CORPORATIVOS**

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

OBJETIVOS Y USOS DE LA INFORMÁTICA FORENSE

PERSECUCIÓN CRIMINAL

LA INFORMÁTICA FORENSE PERMITE **OBTENER EVIDENCIAS QUE INCRIMINEN A LOS CULPABLES DE MUCHOS TIPOS DE DELITOS** COMO, POR EJEMPLO, FRAUDES FINANCIEROS, TRÁFICO DE DROGAS, PORNOGRAFÍA INFANTIL, EVASIÓN DE IMPUESTOS, ETC.

LITIGACIÓN CIVIL

ESTA DISCIPLINA **PERMITE APORTAR PRUEBAS QUE AYUDEN A LA RESOLUCIÓN DE CONFLICTOS DE TIPO CIVIL** COMO DIVORCIOS, FRAUDES, PROBLEMAS DE DISCRIMINACIÓN, ETC.

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

OBJETIVOS Y USOS DE LA INFORMÁTICA FORENSE

INVESTIGACIÓN DE SEGUROS

LOS DELITOS RELACIONADOS CON FRAUDES A COMPAÑÍAS DE SEGUROS (ROBOS FALSOS, SOBRE TODO). LA INFORMÁTICA FORENSE **PERMITE LA RECOLECCIÓN DE EVIDENCIAS QUE AYUDEN A LAS COMPAÑÍAS DE SEGUROS A DETECTAR CASOS DE FRAUDE** Y DISMINUIR ASÍ SUS COSTES.

MANTENIMIENTO DE LA LEY

LA INFORMÁTICA FORENSE PUEDE UTILIZARSE TAMBIÉN PARA **LLEVAR A CABO BÚSQUEDAS INICIALES EN INVESTIGACIONES CON ÓRDENES JUDICIALES**. CON LOS RESULTADOS OBTENIDOS SE PUEDE AMPLIAR LA ORDEN JUDICIAL Y PODER REALIZAR BÚSQUEDAS MÁS EXHAUSTIVAS DE EVIDENCIAS.

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

OBJETIVOS Y USOS DE LA INFORMÁTICA FORENSE

USUARIO FINAL

CADA VEZ ES MÁS FRECUENTE QUE LOS USUARIOS FINALES UTILICEN **HERRAMIENTAS DE INFORMÁTICA FORENSE PARA LA RECUPERACIÓN DE ARCHIVOS ELIMINADOS, LA ENCRIPTACIÓN DE ARCHIVOS Y DATOS Y PARA RASTREAR CORREOS ELECTRÓNICOS**, ENTRE OTROS.

ORGANIZACIONES Y TEMAS CORPORATIVOS

PARA **OBTENER EVIDENCIAS Y PERSEGUIR DELITOS RELACIONADOS CON EL USO MALINTENCIONADO O LA APROPIACIÓN DE INFORMACIÓN CONFIDENCIAL** DE ORGANIZACIONES. TAMBIÉN SIRVEN DE APOYO PARA LA RESOLUCIÓN DE DELITOS RELACIONADOS CON EL ESPIONAJE INDUSTRIAL.

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

METODOLOGÍA DEL ANÁLISIS FORENSE INFORMÁTICO

EL **ANÁLISIS FORENSE INFORMÁTICO** *ES UNA* ***PARTE FUNDAMENTAL DENTRO DEL PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD***. CON ESTOS ANÁLISIS **SE CONSIGUE AVERIGUAR CÓMO, QUIÉN Y QUÉ DAÑOS HA CAUSADO CUALQUIER TIPO DE INTRUSIÓN O ATAQUE**.

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

METODOLOGÍA DEL ANÁLISIS FORENSE INFORMÁTICO

LAS **TÉCNICAS DE ANÁLISIS FORENSE** SE LLEVAN A CABO DENTRO DE LAS FASES DE ***ANÁLISIS PRELIMINAR*** **E** ***INVESTIGACIÓN*** DEL PROCESO DE ***GESTIÓN DE INCIDENTES.***

PESE A FORMAR PARTE DEL PROCESO DE GESTIÓN DE INCIDENTES, SUS UTILIDADES SON DE LO MÁS VARIADAS, POR LO QUE RESULTA IMPRESCINDIBLE CONOCER MÁS EN PROFUNDIDAD SU PROCEDIMIENTO CONCRETO.

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

METODOLOGÍA DEL ANÁLISIS FORENSE INFORMÁTICO

EL ANÁLISIS FORENSE INFORMÁTICO SE LLEVA A CABO EN VARIAS **FASES**:

- **FASE 1: ESTUDIO PRELIMINAR**
- **FASE 2: ADQUISICIÓN DE DATOS Y RECOPILACIÓN DE EVIDENCIAS**
- **FASE 3: ANÁLISIS E INVESTIGACIÓN DE LAS EVIDENCIAS**
- **FASE 4: CONFIRMACIÓN DE LAS PRUEBAS REALIZADAS Y REALIZACIÓN DEL INFORME**

EN CASO DE DELITO DIGITAL, ESTE INFORME **SE PODRÁ INCORPORAR A LA DENUNCIA** QUE SE FORMULE A LAS AUTORIDADES COMPETENTES.

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

METODOLOGÍA DEL ANÁLISIS FORENSE INFORMÁTICO

FASE 1: ESTUDIO PRELIMINAR

SE LLEVA A CABO UN **ESTUDIO INICIAL** EN EL QUE SE REALIZAN **ENTREVISTAS** Y SE **REVISA LA DOCUMENTACIÓN INICIAL** OBTENIDA DEL INCIDENTE PARA **IDENTIFICAR LAS FUENTES DISPONIBLES** QUE PUEDEN RESULTAR ÚTILES PARA LA INVESTIGACIÓN.

FASE 2: ADQUISICIÓN DE DATOS Y RECOPILACIÓN DE EVIDENCIAS

LA FINALIDAD ES LA **RECOLECCIÓN Y OBTENCIÓN DE LOS DISTINTOS TIPOS DE EVIDENCIAS E INFORMACIONES** PARA LA INVESTIGACIÓN. SE RECOMIENDA **REALIZAR COPIAS DE LOS DISPOSITIVOS** QUE HAN ESTADO IMPLICADOS PARA QUE PUEDAN SER **ANALIZADOS POSTERIORMENTE**.

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

METODOLOGÍA DEL ANÁLISIS FORENSE INFORMÁTICO

FASE 3: ANÁLISIS E INVESTIGACIÓN DE LAS EVIDENCIAS

CON LOS DATOS OBTENIDOS EN LA SEGUNDA FASE SE LLEVA A CABO UN **ANÁLISIS MÁS EXHAUSTIVO PARA RECONSTRUIR EL TIMELINE** DEL ATAQUE Y LLEGAR AL INICIO DEL MISMO PARA DETECTAR AL ATACANTE.

FASE 4: CONFIRMACIÓN DE LAS PRUEBAS REALIZADAS Y REALIZACIÓN DEL INFORME

UNA VEZ ANALIZADAS LAS EVIDENCIAS Y OBTENIDOS LOS RESULTADOS **DEBE PLASMARSE TODO EL PROCEDIMIENTO EN UN INFORME** QUE SE REMITIRÁ A LA DIRECCIÓN O A LOS RESPONSABLES DE SEGURIDAD DE LA ORGANIZACIÓN.

CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE
3. **EXPOSICIÓN DEL PRINCIPIO DE LOCARD**
4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS
5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS
6. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

LA **CIENCIA FORENSE** FUNDAMENTA **LOS PRINCIPIOS Y TÉCNICAS QUE SE PUEDEN Y DEBEN UTILIZAR PARA INVESTIGAR CUALQUIER DELITO CRIMINAL**.

ESTA CIENCIA INCLUYE LOS PRINCIPIOS Y TÉCNICAS QUE SE UTILIZARÁN PARA IDENTIFICAR, RECUPERAR, RECONSTRUIR Y ANALIZAR LAS EVIDENCIAS QUE FORMAN PARTE DE UN DELITO.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EN CUANTO A LOS **PRINCIPIOS**, **TODO PROCEDIMIENTO** DE RECOLECCIÓN Y ANÁLISIS DE EVIDENCIAS **DEBE TENER EN CUENTA** LOS SIGUIENTES **ASPECTOS**:

- RECOGIDA Y EXAMEN DE LAS HUELLAS DACTILARES Y ADN.
- RECUPERACIÓN DE LOS DOCUMENTOS DE LOS DISPOSITIVOS DAÑADOS.
- REALIZACIÓN DE COPIAS EXACTAS DE LAS EVIDENCIAS DIGITALES DETECTADAS.
- GENERACIÓN DE UNA HUELLA DIGITAL DE LOS TEXTOS Y EVIDENCIAS PARA ASEGURARSE QUE NO SE MODIFICAN.
- UTILIZACIÓN DE LA FIRMA DIGITAL PARA CONFIRMAR LA AUTENTICIDAD DE LOS DOCUMENTOS Y MANTENER LA CADENA DE CUSTODIA DE EVIDENCIAS.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

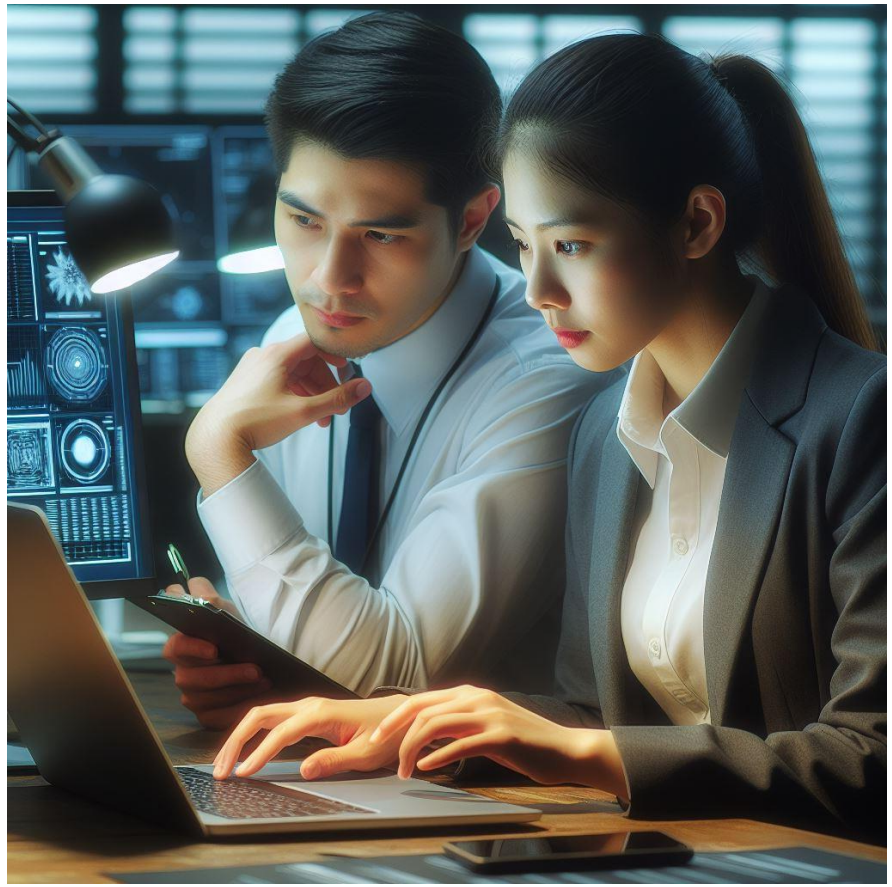
LOS **FORENSES INFORMÁTICOS** SE ENCARGAN DE **APLICAR SU CONOCIMIENTO PARA** AYUDAR A LOS INVESTIGADORES A **ENCONTRAR EVIDENCIAS Y PISTAS** Y ASÍ PODER **RECONSTRUIR EL CRIMEN.**

UTILIZANDO **UN MÉTODO CIENTÍFICO** ***CREAN HIPÓTESIS*** *SOBRE LO QUE HA SUCEDIDO MEDIANTE EL* ***ANÁLISIS DE LAS EVIDENCIAS, PRUEBAS ADICIONALES Y*** *UNA SERIE DE* ***CONTROLES*** *QUE CONFIRMEN O INVALIDEN LAS HIPÓTESIS FORMULADAS*.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

LOS FORENSES INFORMÁTICOS NO PUEDEN CONOCER TODO **EL PASADO**,.

SIMPLEMENTE **PUEDEN FORMULAR HIPÓTESIS Y TEORÍAS DE QUÉ HA PODIDO OCURRIR** EN FUNCIÓN DE LA INFORMACIÓN LIMITADA DE LA QUE SE DISPONE.



3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

UNO DE LOS PRINCIPIOS MÁS RELEVANTES Y UTILIZADOS EN LA CIENCIA FORENSE ES EL **PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD**.

EDMOND LOCARD (FRANCIA, 1877-1966), CRIMINALISTA FRANCÉS, FUE UNO DE LOS PIONEROS EN CRIMINOLOGÍA Y FUNDÓ EL INSTITUTO DE CRIMINALÍSTICA DE LA UNIVERSIDAD DE LYON.

ES CONOCIDO POR ENUNCIAR EL FAMOSO ***PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD.***

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

ESTE PRINCIPIO **SE UTILIZA** MUY FRECUENTEMENTE **PARA RELACIONAR AL CRIMINAL CON EL CRIMEN** QUE HA COMETIDO Y, EN TÉRMINOS GENERALES, **DICE QUE**:

CUALQUIERA O CUALQUIER OBJETO QUE FORMA PARTE DE LA ESCENA DEL CRIMEN DEJA UN RASTRO EN LA ESCENA O EN LA VÍCTIMA Y VICEVERSA, EL OBJETO O CRIMINAL SE LLEVARÁ CONSIGO ALGO DE LA ESCENA DEL CRIMEN.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

CONCRETAMENTE, EL PRINCIPIO DE LOCARD SE DEFINE COMO:

CADA CONTACTO DEJA UN RASTRO

SIEMPRE QUE DOS OBJETOS ENTRAN EN CONTACTO HAY UNA TRANSFERENCIA DE PARTE DE ALGÚN MATERIAL DE UN OBJETO AL OTRO.

CUANDO UN CRIMINAL ENTRA EN UNA ESCENA DEL CRIMEN O ENTRA EN CONTACTO CON UNA VÍCTIMA, *LA VÍCTIMA SE QUEDA CON ALGO DEL CRIMINAL, PERO ESTE TAMBIÉN SE LLEVA ALGO A CAMBIO*.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

EN OTRAS PALABRAS, **CUANDO UN CONTACTO ENTRA EN LA ESCENA DEL CRIMEN DEJA SIEMPRE ALGUNA HUELLA** (PELO, SUDOR, HUELLAS DACTILARES, ETC.) **PERO TAMBIÉN SE LLEVA ALGO CONSIGO CUANDO ABANDONE LA ESCENA** (BARRO, OLORES, FIBRAS, ETC.).

CON LA **DETECCIÓN Y ANÁLISIS DE** ESTAS **EVIDENCIAS** SE PODRÁ **DEMOSTRAR** CON ALTAS **PROBABILIDADES LA PRESENCIA DE ALGO O ALGUIEN** EN LA ESCENA DEL CRIMEN.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

EN LA CIENCIA FORENSE TRADICIONAL SE DISTINGUEN LOS **TIPOS DE EVIDENCIAS FÍSICAS**:

- **EVIDENCIAS TRANSITORIAS**
- **EVIDENCIAS CURSO O PATRONES**
- **EVIDENCIAS CONDICIONALES**
- **EVIDENCIAS TRANSFERIDAS**

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

TIPOS DE EVIDENCIAS FÍSICAS:

EVIDENCIAS TRANSITORIAS

SON EVIDENCIAS TEMPORALES QUE ***SOLO PERMANECEN EN LA ESCENA DEL CRIMEN EN UN PERÍODO DE TIEMPO GENERALMENTE CORTO***. POR EJEMPLO, TEMPERATURA, OLOR, ETC.

EVIDENCIAS CURSO O PATRONES

EVIDENCIAS QUE ***SE HAN PRODUCIDO POR EFECTOS DE CONTACTO***, *HAN TENIDO QUE SER TOCADAS POR EL ATACANTE O POR LA VÍCTIMA*. SON EJEMPLOS LOS MUEBLES CAMBIADOS DE SITIO, LA TRAYECTORIA DE UNA BALA, ETC.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

TIPOS DE EVIDENCIAS FÍSICAS:

EVIDENCIAS CONDICIONALES

EVIDENCIAS *QUE* ***SE HAN ORIGINADO POR ALGUNA ACCIÓN O EVENTO SUCEDIDOS EN LA ESCENA DEL CRIMEN***. POR EJEMPLO, LOCALIZACIÓN DE EVIDENCIAS SEGÚN LA UBICACIÓN DEL CUERPO (VÍCTIMA), VENTANAS ABIERTAS O CERRADAS, TELEVISIÓN ENCENDIDA/APAGADA, ETC.

EVIDENCIAS TRANSFERIDAS

SON LAS EVIDENCIAS QUE ***SE ORIGINAN POR EL CONTACTO ENTRE VARIAS PERSONAS, ENTRE VARIOS OBJETOS O ENTRE PERSONAS Y OBJETOS***. EN ESTAS EVIDENCIAS ENTRA EN JUEGO EL CONCEPTO DE RELACIÓN ENTRE PERSONAS, OBJETOS O AMBOS.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

EN RESUMEN, EL PRINCIPIO DE INTERCAMBIO DE LOCARD SE COMPONE DE **TRES ELEMENTOS**:

1. **EL SOSPECHOSO SE LLEVARÁ CON ÉL ALGÚN RASTRO** O HUELLA **DE LA ESCENA Y DE LA VÍCTIMA.**
2. **EL SOSPECHOSO DEJARÁ RASTROS EN LA VÍCTIMA Y LA VÍCTIMA PUEDE DEJAR ALGÚN RASTRO SOBRE EL SOSPECHOSO**.
3. **EL SOSPECHOSO DEJARÁ** TAMBIÉN **ALGÚN RASTRO EN LA ESCENA DEL CRIMEN.**

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

EL **OBJETIVO PRINCIPAL** DE ESTE PRINCIPIO ES ***ESTABLECER RELACIONES ENTRE LOS DISTINTOS ELEMENTOS QUE FORMAN PARTE DEL CRIMEN***:

- **LA VÍCTIMA**
- **EL SOSPECHOSO**
- **LA EVIDENCIA**
- **LA ESCENA DEL CRIMEN**

EL CONCEPTO DE RELACIÓN ENTRE ESTOS ELEMENTOS ES FUNDAMENTAL PARA UNA CORRECTA RESOLUCIÓN DEL CRIMEN: SI NO HAY RELACIÓN ALGUNA NO SE PODRÁ ACUSAR DIRECTAMENTE A UN CRIMINAL AL NO HABER PRUEBAS QUE LO INCRIMINEN.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

EN CUANTO A **LAS EVIDENCIAS** SEGÚN LOCARD, ESTAS **PUEDEN SER TRANSFERIDAS DE DOS MODOS** DIFERENTES:

TRANSFERENCIA DIRECTA

CUANDO LA EVIDENCIA SE TRANSFIERE DE ORIGEN A DESTINO DIRECTAMENTE, SIN INTERMEDIARIOS.

TRANSFERENCIA INDIRECTA

CUANDO LA EVIDENCIA ES TRANSFERIDA A UNA LOCALIZACIÓN Y, POSTERIORMENTE, SE TRANSFIERE DE NUEVO A OTRA LOCALIZACIÓN.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

PRINCIPIO DE INTERCAMBIO DE LOCARD	
CADA CONTACTO DEJA UN RASTRO	LA VÍCTIMA DEJA RASTRO EN LA ESCENA DEL CRIMEN Y EN EL SOSPECHOSO.
	EL SOSPECHOSO DEJA RASTRO EN LA VÍCTIMA Y EN LA ESCENA DEL CRIMEN.
	TANTO LA VÍCTIMA COMO EL SOSPECHOSO TENDRÁN ALGÚN RASTRO DE LA ESCENA DEL CRIMEN.
TIPOS DE EVIDENCIAS FÍSICAS	EVIDENCIAS TRANSITORIAS.
	EVIDENCIAS CURSO O PATRONES.
	EVIDENCIAS CONDICIONALES.
	EVIDENCIAS TRANSFERIDAS.
MÉTODOS DE TRANSFERENCIA DE EVIDENCIAS	TRANSFERENCIA DIRECTA.
	TRANSFERENCIA INDIRECTA.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

APLICACIÓN DEL PRINCIPIO DE LOCARD AL ANÁLISIS FORENSE DIGITAL

LOS CONCEPTOS DEL **PRINCIPIO DE INTERCAMBIO DE LOCARD** SON PERFECTAMENTE **TRASLADABLES AL ANÁLISIS FORENSE INFORMÁTICO** O DIGITAL Y TIENE PLENA VALIDEZ EN LAS EVIDENCIAS ELECTRÓNICAS.

CUALQUIER ATACANTE DEJA SIEMPRE ALGÚN TIPO DE HUELLA DIGITAL EN EL SITIO ATACADO ADEMÁS DE LLEVARSE ALGO CON ÉL.

CON ***EL ANÁLISIS DE LAS HUELLAS DIGITALES Y DE LAS EVIDENCIAS SE PODRÁ RECONSTRUIR QUÉ HA OCURRIDO PARA RELACIONAR AL ATACANTE CON LA VÍCTIMA Y,*** *A SU VEZ,* ***CON LA ESCENA DEL CRIMEN*** (EN ESTE CASO LOS EQUIPOS O DISPOSITIVOS AFECTADOS).

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

APLICACIÓN DEL PRINCIPIO DE LOCARD AL ANÁLISIS FORENSE DIGITAL

A TRAVÉS DE LA DETERMINACIÓN DE ¿CÓMO HA SUCEDIDO?, ¿DÓNDE HA SUCEDIDO? Y ¿QUÉ SE HA AFECTADO? SE PODRÁN DETECTAR LAS EVIDENCIAS DIGITALES Y RELACIONARLAS ENTRE ELLAS PARA RESOLVER EL CRIMEN.

POR EJEMPLO, CON LA DETECCIÓN DE QUIÉN FUE LA ÚLTIMA PERSONA QUE ESCRIBIÓ EN UN ARCHIVO RELACIONADO CON UNA INTRUSIÓN SE PUEDEN LOCALIZAR SOSPECHOSOS DE LA MISMA.

PARA FINALIZAR, NO SE PUEDE RELACIONAR EL PRINCIPIO DE LOCARD AL MUNDO DIGITAL SI NO SE CONOCE EL CONCEPTO DE **EVIDENCIA DIGITAL**.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

APLICACIÓN DEL PRINCIPIO DE LOCARD AL ANÁLISIS FORENSE DIGITAL

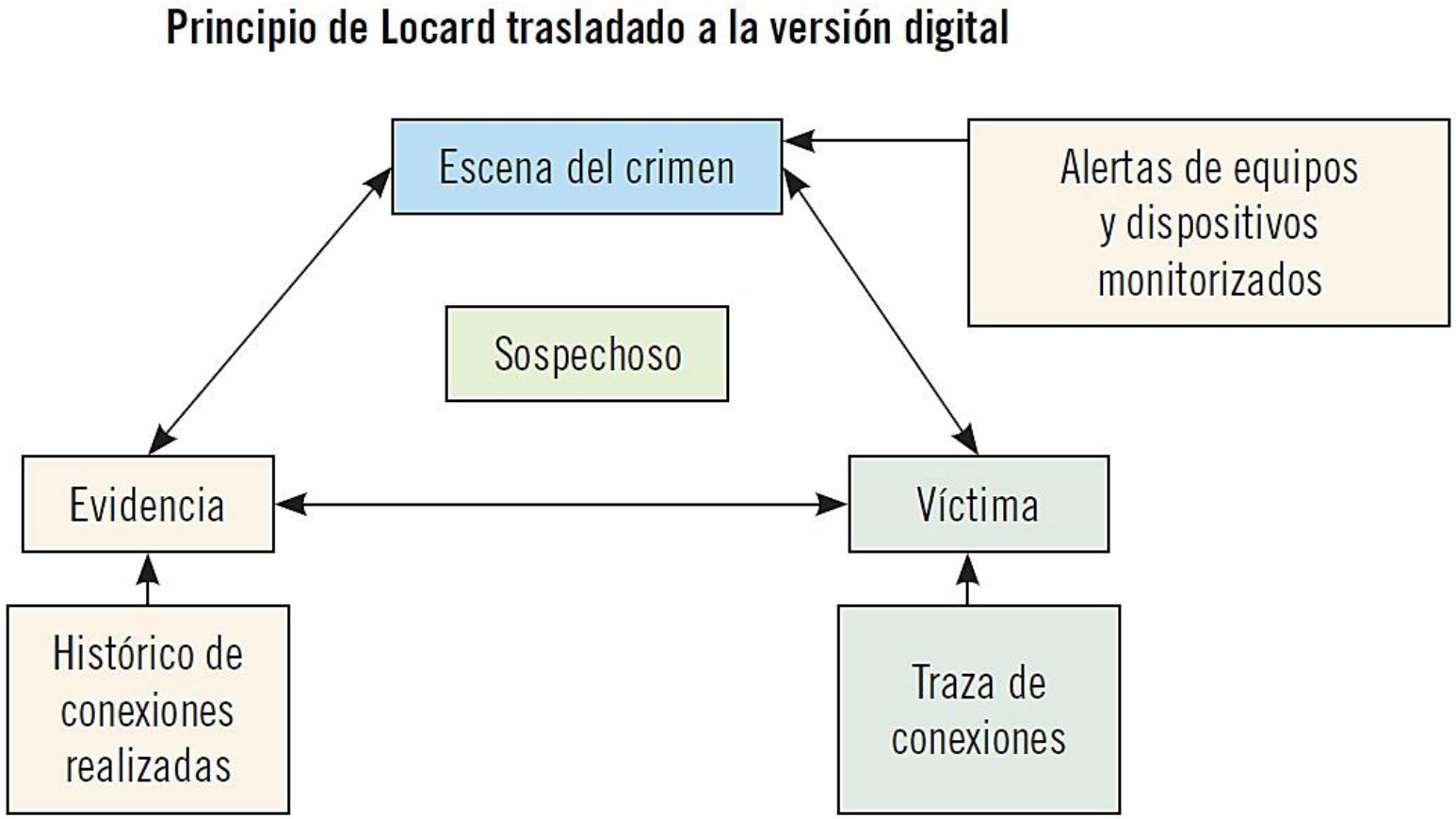
UNA **EVIDENCIA DIGITAL**, A DIFERENCIA DE LAS EVIDENCIAS FÍSICAS, ***ES CUALQUIER DOCUMENTO, FICHERO, REGISTRO, ETC. QUE ESTÁ CONTENIDO EN UN SOPORTE INFORMÁTICO O DIGITAL Y QUE ES SUSCEPTIBLE DE TRATAMIENTO*.**

SON EJEMPLOS DE EVIDENCIAS DIGITALES CUALQUIER DOCUMENTO DE OFIMÁTICA (ARCHIVOS EXCEL, WORD, ETC.), IMAGEN, BASE DE DATOS, REGISTRO DE ACTIVIDAD, COMUNICACIÓN DIGITAL (CORREO ELECTRÓNICO, ETC.), ETC.

LAS EVIDENCIAS DIGITALES SON **UNO DE LOS PILARES MÁS IMPORTANTES DE LA INFORMÁTICA FORENSE,** YA QUE SUMINISTRAN UN GRAN VALOR EN LAS INVESTIGACIONES Y SE APORTAN EN PROCESOS JUDICIALES.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

APLICACIÓN DEL PRINCIPIO DE LOCARD AL ANÁLISIS FORENSE DIGITAL



EN EL GRÁFICO SE MUESTRAN RASTROS DE LOS DISTINTOS ELEMENTOS:

- EN LA ESCENA DEL CRIMEN SE PUEDE ENCONTRAR ALGÚN RESTO DEL CRIMEN CON EL ANÁLISIS DE LAS ALERTAS EMITIDAS POR LOS DISPOSITIVOS Y EQUIPOS QUE HAN SIDO MONITORIZADOS PREVIAMENTE.
- EN CUANTO AL SOSPECHOSO, ESTE HA PODIDO DEJAR ALGÚN RASTRO EN LA ESCENA DEL CRIMEN. SE PODRÁ ENCONTRAR ALGÚN RASTRO OBSERVANDO EL HISTÓRICO DE LAS CONEXIONES REALIZADAS PARA ENCONTRAR A POSIBLES SOSPECHOSOS.
- ANALIZANDO A LA VÍCTIMA (EN ESTE CASO, LOS EQUIPOS AFECTADOS) SE PUEDE OBTENER UN TRAZADO DE RUTA DE LAS CONEXIONES REALIZADAS QUE PERMITA OBTENER EL CAMINO PASO A PASO DE UN PAQUETE DE DATOS DESDE SU ORIGEN HASTA SU DESTINO Y ASÍ ENCONTRAR A LOS ATACANTES DESDE SU ORIGEN.
- ADEMÁS, SE PRODUCE TAMBIÉN UNA RELACIÓN ENTRE EL ATACANTE SOSPECHOSO Y EL EQUIPO VÍCTIMA, YA QUE GENERALMENTE HAY ALGÚN ARCHIVO QUE HAYA SIDO UTILIZADO Y/O MODIFICADO POR AMBOS.

CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE
3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD
4. **GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS**
5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS
6. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

LA **RECOPILACIÓN DE EVIDENCIAS ELECTRÓNICAS** ES UNA DE LAS **FASES MÁS CRÍTICAS Y VITALES DEL ANÁLISIS FORENSE DIGITAL**.

SI LA RECOPILACIÓN NO SE REALIZA BIEN PUEDE INVALIDARSE TODO EL ANÁLISIS POSTERIOR Y LOS RESULTADOS PUEDEN SER ERRÓNEOS.

LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS **DEBE SER UN PROCESO METICULOSO** EN EL QUE DEBE TRATARSE DE NO REALIZAR NINGÚN CAMBIO SOBRE LAS MISMAS PARA TENER ERRORES DE ANÁLISIS.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

CUANDO HAY QUE RECOGER EVIDENCIAS ELECTRÓNICAS HAY QUE TENER EN CUENTA UNA SERIE DE **CONCEPTOS IMPRESCINDIBLES**:

- **EVIDENCIAS VOLÁTILES Y NO VOLÁTILES**
- **ETIQUETADO DE EVIDENCIAS**
- **CADENA DE CUSTODIA**
- **FICHEROS Y DIRECTORIOS OCULTOS**
- **RECUPERACIÓN DE FICHEROS BORRADOS**

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

EVIDENCIAS VOLÁTILES Y NO VOLÁTILES

LAS EVIDENCIAS DIGITALES SE CLASIFICAN EN:

EVIDENCIAS VOLÁTILES

SON AQUELLAS QUE **SE PIERDEN CUANDO SE APAGA EL EQUIPO** (ESTADO DE LA MEMORIA, PROCESOS EN EJECUCIÓN, ETC.).

EVIDENCIAS NO VOLÁTILES

SE ALMACENAN EN EL SISTEMA DE FICHEROS Y NO SE PIERDEN AL APAGAR EL EQUIPO (APLICACIONES, CONFIGURACIONES, ETC.).

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

EVIDENCIAS VOLÁTILES Y NO VOLÁTILES

LA **PRIMERA DECISIÓN** A TOMAR **ES SI APAGAR EL EQUIPO O NO APAGARLO**.

ESTA DECISIÓN PUEDE SER CRUCIAL, YA QUE **AL APAGAR EL EQUIPO PUEDEN PERDERSE EVIDENCIAS VOLÁTILES IMPORTANTES** COMO USUARIOS CONECTADOS, CONEXIONES EXISTENTES EN ESE MOMENTO, ETC.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

EVIDENCIAS VOLÁTILES Y NO VOLÁTILES

DEBIDO A LA RELEVANCIA DE LAS EVIDENCIAS VOLÁTILES **SE RECOMIENDA PRESERVAR LA EVIDENCIA MÁS VOLÁTIL EN EL MOMENTO INICIAL** DEL ANÁLISIS FORENSE DIGITAL.

SE DEBE **ATENDER LAS EVIDENCIAS DIGITALES EN EL ORDEN** (RELACIONADO CON SU GRADO DE VOLATILIDAD) DE LA TABLA SIGUIENTE:

Orden de preservación de las evidencias digitales:
Registros, memoria caché, memoria de periféricos
Memoria física
Estado de las conexiones de red
Ficheros temporales del sistema
Procesos que se están ejecutando en ese momento
Discos duros, rígidos
Archivos de backups
Registros y datos de monitorización remotos relevantes
Configuración física y topología de la red
CD-ROM, impresiones

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

ETIQUETADO DE EVIDENCIAS

PARA QUE LAS EVIDENCIAS SE PUEDAN ADMITIR COMO TAL DEBEN CUMPLIR CON UNA SERIE DE **REQUISITOS**:

- DEBEN **CONSERVARSE EN UN ESTADO LO MÁS PARECIDO POSIBLE AL ESTADO EN EL QUE SE ENCONTRARON**.
- EN LA MEDIDA DE LO POSIBLE, **DEBE REALIZARSE UNA COPIA EXACTA DE LA EVIDENCIA ORIGINAL** PARA REALIZAR LOS TRABAJOS DE INVESTIGACIÓN SOBRE LA MISMA Y NO DAÑAR LOS DATOS ORIGINALES.
- **LAS COPIAS** REALIZADAS **DEBERÁN REALIZARSE EN MEDIOS ESTÉRILES**, ES DECIR, EN MEDIOS QUE NO HAYAN CONTENIDO NINGÚN DATO ANTERIORMENTE.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

ETIQUETADO DE EVIDENCIAS

- **LAS EVIDENCIAS DEBERÁN ETIQUETARSE Y DOCUMENTARSE** DEBIDAMENTE EN LA CADENA DE CUSTODIA. ADEMÁS, CADA ACCIÓN REALIZADA SOBRE LA EVIDENCIA O SOBRE SU COPIA DEBERÁ SER TAMBIÉN DOCUMENTADA CON DETALLE.
- LAS EVIDENCIAS DIGITALES DEBERÁN DOCUMENTARSE **CON FIRMAS DIGITALES DEL INVESTIGADOR** PARA GARANTIZAR QUE NADIE MÁS REALIZA NINGUNA ACCIÓN SOBRE ELLAS.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

ETIQUETADO DE EVIDENCIAS

EN EL MOMENTO DE ETIQUETAR LAS EVIDENCIAS DIGITALES HAY QUE TENER EN CUENTA QUE SE CLASIFICAN EN VARIAS **CATEGORÍAS:**

- **REGISTROS GENERADOS POR ORDENADOR**
- **REGISTROS ALMACENADOS POR ORDENADORES**
- **REGISTROS HÍBRIDOS**
- **REGISTROS DE CADA SERVIDOR**
- **REGISTROS DE TRÁFICO DE RED**
- **REGISTROS DE APLICACIÓN**

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

ETIQUETADO DE EVIDENCIAS

CATEGORÍAS

REGISTROS GENERADOS POR ORDENADOR

SE GENERAN POR LA PROGRAMACIÓN DE UN EQUIPO Y SON INALTERABLES POR UN USUARIO. ESTOS REGISTROS SON LOS LLAMADOS **REGISTROS DE EVENTOS DE SEGURIDAD O LOGS** Y SE UTILIZAN COMO MEDIO PROBATORIO PARA DEMOSTRAR EL CORRECTO O INCORRECTO FUNCIONAMIENTO DEL SISTEMA CUANDO SE GENERÓ EL REGISTRO.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

ETIQUETADO DE EVIDENCIAS

CATEGORÍAS

REGISTROS ALMACENADOS POR ORDENADORES

ESTOS REGISTROS NO SON GENERADOS POR UN EQUIPO, **LOS GENERA UNA PERSONA Y POSTERIORMENTE SON ALMACENADOS** EN UN EQUIPO (POR EJEMPLO, UN DOCUMENTO DE WORD).

DE ESTOS REGISTROS SE PUEDE DEDUCIR LA IDENTIDAD DEL USUARIO QUE LOS GENERÓ Y PROBAR HECHOS QUE ESTÉN CONTENIDOS EN ESTE.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

ETIQUETADO DE EVIDENCIAS

CATEGORÍAS

REGISTROS HÍBRIDOS

SON REGISTROS QUE COMBINAN ACCIONES REALIZADAS POR PERSONAS Y ACCIONES REALIZADAS POR EL EQUIPO.

REGISTROS DE CADA SERVIDOR

SON LOS REGISTROS DEL SISTEMA Y DE LOS PROGRAMAS EN EJECUCIÓN.

REGISTROS DE TRÁFICO DE RED

REGISTROS QUE INCLUYEN LA ACTIVIDAD DE RED GENERADA EN EL EQUIPO.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

ETIQUETADO DE EVIDENCIAS

CATEGORÍAS

REGISTROS DE APLICACIÓN

ESTOS REGISTROS SON ALMACENADOS POR CADA APLICACIÓN E INCLUYEN DATOS SOBRE EL ACCESO DE USUARIOS, LOS ERRORES OCURRIDOS E INFORMACIÓN SOBRE LAS ACCIONES QUE HA REALIZADO CADA USUARIO.

TENIENDO EN CUENTA ESTAS CATEGORÍAS, LA EVIDENCIA DIGITAL DEBERÁ CONSIDERAR UNA SERIE DE **CRITERIOS** PARA DECIDIR SU ADMISIBILIDAD REFLEJADOS EN LA TABLA SIGUIENTE:

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

ETIQUETADO DE EVIDENCIAS

CRITERIOS DE ADMISIBILIDAD DE EVIDENCIAS ELECTRÓNICAS

AUTENTICIDAD	LA EVIDENCIA DEBE HABER SIDO GENERADA Y REGISTRADA EN LA ESCENA DEL CRIMEN Y DEBE MOSTRAR QUE LOS MEDIOS UTILIZADOS NO SE HAN MODIFICADO
CONFIABILIDAD	LAS EVIDENCIAS SERÁN CONFIABLES SI EL SISTEMA QUE LAS PRODUJO NO HA SIDO VIOLADO Y ESTABA FUNCIONANDO CORRECTAMENTE CUANDO SE RECIBIÓ, ALMACENÓ O GENERÓ LA PRUEBA.
COMPLETITUD O SUFICIENCIA	LA EVIDENCIA DEBE ESTAR COMPLETA, TIENE QUE HABERSE MANTENIDO SU INTEGRIDAD.
RESPETO POR LAS LEYES	LAS TÉCNICAS DE RECOLECCIÓN Y TRATAMIENTO DE LA EVIDENCIA DEBEN CUMPLIR LAS NORMATIVAS LEGALES VIGENTES EN EL ORDENAMIENTO JURÍDICO.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

CADENA DE CUSTODIA

LA **CADENA DE CUSTODIA** ESTÁ **FORMADA POR *UNA SERIE DE PROCEDIMIENTOS Y DOCUMENTOS*** *RELACIONADOS CON LA* ***RECOLECCIÓN, COPIA, TRASLADO, TRATAMIENTO, VERIFICACIÓN Y ANÁLISIS DE LAS EVIDENCIAS ENCARGADOS DE SU PRESERVACIÓN*** *PARA EVITAR QUE LA MANIPULACIÓN DE ESTAS PUEDA LLEVAR A ERROR EN LOS RESULTADOS DEL ANÁLISIS.*

LA CADENA DE CUSTODIA **DEBE REALIZARSE EN TODAS LAS FASES DEL ANÁLISIS FORENSE DIGITAL**, DESDE EL MOMENTO DE LA RECOLECCIÓN HASTA LA EMISIÓN DEL INFORME FINAL.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

CADENA DE CUSTODIA

EN UN PRIMER MOMENTO DEBERÁN UTILIZARSE **MÉTODOS ADECUADOS** PARA **LA IDENTIFICACIÓN, DOCUMENTACIÓN, ETIQUETADO Y ALMACENAMIENTO DE LAS EVIDENCIAS AÑADIENDO FIRMAS TEMPORALES** QUE PERMITAN TEMPORALIZAR CADA ACCIÓN REALIZADA SOBRE LAS MISMAS.

EN SU TRATAMIENTO, **LAS EVIDENCIAS DEBERÁN PROTEGERSE DE FACTORES AMBIENTALES** (LLUVIA, CAMPOS MAGNÉTICOS, ETC.) QUE PUEDAN PROVOCAR PÉRDIDAS DE DATOS. SE RECOMIENDA MANTENER LOS SOPORTES INFORMÁTICOS DONDE SE REGISTRAN LAS EVIDENCIAS EN BOLSAS DE PLÁSTICO ANTIESTÁTICAS QUE LOS PROTEJAN.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

CADENA DE CUSTODIA

PARA UNA CORRECTA PRESERVACIÓN DE LA CADENA DE CUSTODIA ES NECESARIO QUE **LAS EVIDENCIAS** SEAN **TRATADAS POR PROFESIONALES CON CONOCIMIENTOS ESPECIALIZADOS** Y CORRECTAMENTE IDENTIFICADOS.

EN **LA DOCUMENTACIÓN DE LA EVIDENCIA DEBE PLASMARSE QUIÉN REALIZÓ CADA ACCIÓN, CUÁNDO LA REALIZÓ Y DÓNDE LA REALIZÓ** PARA EVITAR PROBLEMAS DE FALTA DE INTEGRIDAD EN LOS DATOS DE LA EVIDENCIA.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

CADENA DE CUSTODIA

EN CONCRETO, **LA CADENA DE CUSTODIA DEBE:**

- REDUCIR TODO LO POSIBLE LA CANTIDAD DE AGENTES QUE TRATEN LAS EVIDENCIAS.
- MANTENER LA IDENTIDAD DE LAS PERSONAS IMPLICADAS EN TODO EL PROCESO DE GESTIÓN DE LA EVIDENCIA.
- ASEGURAR LA FIRMEZA DE LAS EVIDENCIAS CUANDO ESTÉN ALMACENADAS PARA ASEGURAR SU PROTECCIÓN.
- REGISTRAR LOS TIEMPOS FIRMADOS POR CADA AGENTE EN LOS INTERCAMBIOS DE EVIDENCIAS ENTRE ELLOS PARA DETECTAR AL RESPONSABLE DE SU TRATAMIENTO EN CADA MOMENTO.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

FICHEROS Y DIRECTORIOS OCULTOS

EN EL MOMENTO DE REALIZAR LA RECOLECCIÓN DE EVIDENCIAS **HAY QUE TENER EN CUENTA QUE PUEDE HABER EVIDENCIAS ESCONDIDAS EN FICHEROS O DIRECTORIOS OCULTOS.**

ES MÁS, LOS ATACANTES SUELEN ESCONDERSE EN ARCHIVOS OCULTOS, POR LO QUE ES FUNDAMENTAL AVERIGUAR SU LOCALIZACIÓN Y DE QUÉ TIPO SON PARA CONSIDERAR SI PUEDEN SER EVIDENCIAS OCULTAS O SI DEBEN DESCARTARSE POR SER ARCHIVOS INOFENSIVOS.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

INFORMACIÓN OCULTA DEL SISTEMA

NO SOLO HAY QUE LOCALIZAR LOS ARCHIVOS Y DIRECTORIOS OCULTOS EN EL SISTEMA, TAMBIÉN DEBEN ENCONTRARSE LOS DISTINTOS PARÁMETROS E INFORMACIONES DEL SISTEMA QUE SE HAN MANTENIDO OCULTOS PARA PROTEGERLOS DE ATACANTES PARA COMPROBAR SI HAN SIDO ALTERADOS.

DE ESTAS ALTERACIONES**, CON HERRAMIENTAS DE ANÁLISIS ADECUADAS, SE PODRÁN ENCONTRAR EVIDENCIAS ELECTRÓNICAS** Y PRUEBAS QUE PODRÁN UTILIZARSE PARA INCRIMINAR AL ATACANTE.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

INFORMACIÓN OCULTA DEL SISTEMA

HAY QUE TENER EN CUENTA QUE **LA INFORMACIÓN OCULTA DEL SISTEMA CONTIENE DETALLES IMPORTANTES SOBRE LA UTILIZACIÓN DEL EQUIPO** COMO PUEDE SER EL HISTORIAL DE PÁGINAS WEB VISITADAS, CORREOS ELECTRÓNICOS ENVIADOS Y RECIBIDOS, DOCUMENTOS CREADOS, MODIFICADOS Y ELIMINADOS, ETC.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

RECUPERACIÓN DE FICHEROS BORRADOS

EN GENERAL, CUANDO UN ARCHIVO SE ELIMINA NO ES BORRADO DEFINITIVAMENTE, SINO QUE SE MANTIENE EN LA PAPELERA DE RECICLAJE DURANTE UN PERÍODO DETERMINADO.

ES MÁS, CUANDO ESTE ARCHIVO SE BORRA DE LA PAPELERA DE RECICLAJE QUEDA MARCADO COMO BORRADO, PERO SIGUE FÍSICAMENTE EN EL DISCO DURO A PESAR DE ESTAR OCULTO PARA LOS USUARIOS.

EN CUANTO AL ANÁLISIS FORENSE **SE RECOMIENDA LOCALIZAR ESTOS ARCHIVOS ELIMINADOS QUE NO HAN DESAPARECIDO DEFINITIVAMENTE DEL EQUIPO PARA INTENTAR DESCUBRIR ARCHIVOS SOSPECHOSOS Y**, POR LO TANTO, **POSIBLES EVIDENCIAS DIGITALES.**

CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE
3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD
4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS
5. **GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS**
6. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

UNA VEZ RECOPILADAS LAS EVIDENCIAS DIGITALES Y ALMACENADAS ADECUADAMENTE, **EL ANÁLISIS FORENSE DIGITAL DEBE ENCARGARSE DE LA RECONSTRUCCIÓN Y TEMPORALIZACIÓN DE LOS HECHOS OCURRIDOS CON LOS DATOS RECOPILADOS.**

SE DARÁ POR **FINALIZADO CUANDO SE DETECTE QUIÉN** REALIZÓ EL ATAQUE, **CÓMO** SE PRODUJO, **CUÁL FUE** SU **OBJETIVO Y BAJO QUÉ CIRCUNSTANCIAS** SE COMETIÓ.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

EL PROCESO DE ANÁLISIS DE EVIDENCIAS SE DIVIDE EN VARIAS **FASES**:

- **PREPARACIÓN DEL ENTORNO DE TRABAJO PARA EL ANÁLISIS**
- **RECONSTRUCCIÓN DE LA SECUENCIA TEMPORAL DEL ATAQUE**
- **DETERMINACIÓN DE CÓMO SE REALIZÓ EL ATAQUE**
- **IDENTIFICACIÓN DEL ATACANTE O ATACANTES**
- **EVALUACIÓN DEL IMPACTO CAUSADO**
- **DOCUMENTACIÓN DEL ATAQUE**
- **ELABORACIÓN DEL INFORME**

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

PREPARACIÓN DEL ENTORNO DE TRABAJO PARA EL ANÁLISIS

ANTES DE EMPEZAR EL ANÁLISIS DEBERÁ PREPARARSE EL ENTORNO DE TRABAJO PARA QUE SEA ADECUADO PARA LLEVAR A CABO LAS INVESTIGACIONES PREVISTAS.

SE RECOMIENDA NO TOCAR LOS DISPOSITIVOS ORIGINALES Y TRABAJAR CON LAS COPIAS DE LAS EVIDENCIAS.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

PREPARACIÓN DEL ENTORNO DE TRABAJO PARA EL ANÁLISIS

PARA ELLO **SE ACONSEJA PREPARAR DOS ESTACIONES DE TRABAJO**:

- **UNA DE ELLAS DEBERÁ CONTENER DOS DISCOS DUROS:** EN UNO SE INSTALARÁ EL **SISTEMA OPERATIVO** QUE SERVIRÁ DE ANFITRIÓN Y CON EL QUE SE REALIZARÁ EL ANÁLISIS DE LAS EVIDENCIAS Y EN OTRO SE VOLCARÁ **LA IMAGEN DEL DISCO DURO** DEL EQUIPO ATACADO.
- **EN LA OTRA ESTACIÓN DE TRABAJO SE INSTALARÁ UN SISTEMA OPERATIVO CONFIGURADO EXACTAMENTE IGUAL QUE EL EQUIPO ATACADO**.

DE ESTE MODO SE PODRÁN ANALIZAR LOS CAMBIOS PRODUCIDOS EN AMBOS EQUIPOS, DETECTANDO LOS EFECTOS OCASIONADOS POR LOS ATAQUES SUFRIDOS EN EL EQUIPO.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

RECONSTRUCCIÓN DE LA SECUENCIA TEMPORAL DEL ATAQUE

UNA VEZ PREPARADO EL ENTORNO DE TRABAJO PARA UN ANÁLISIS FORENSE ADECUADO, EL SIGUIENTE PASO A REALIZAR SERÁ LA **CREACIÓN DE UNA SECUENCIA TEMPORAL** DE LOS SUCESOS QUE SE PRODUJERON DURANTE EL ATAQUE.

PARA ELLO SE RECOPILA Y ANALIZA INFORMACIÓN DE LOS FICHEROS:

- TAMAÑO Y TIPO DE FICHERO
- USUARIOS Y GRUPOS A LOS QUE PERTENECE EL FICHERO
- PERMISOS DE ACCESO
- DETECCIÓN SOBRE SI EL FICHERO FUE BORRADO O NO
- TRAZADO DE RUTA COMPLETO
- MARCAS DE TIEMPO: CREACIÓN, MODIFICACIÓN, BORRADO Y ACCESO

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

RECONSTRUCCIÓN DE LA SECUENCIA TEMPORAL DEL ATAQUE

SE PRETENDE ENCONTRAR FICHEROS Y DIRECTORIOS (TANTO VISIBLES COMO OCULTOS) **QUE HAN SIDO CREADOS, MODIFICADOS O ELIMINADOS RECIENTEMENTE** QUE SE ENCUENTREN EN RUTAS POCO COMUNES.

HAY QUE VIGILAR CON DETALLE LOS ARCHIVOS OCULTOS Y ELIMINADOS, YA QUE EN ELLOS SUELEN ESCONDERSE LAS HUELLAS DE LOS ATACANTES (INTENTAR RECUPERAR LOS ARCHIVOS ELIMINADOS, ADEMÁS DE ANALIZAR LOS ARCHIVOS OCULTOS Y LA INFORMACIÓN OCULTA DEL SISTEMA).

LOS ATACANTES EN GENERAL INSTALARÁN SUS HERRAMIENTAS Y CREARÁN ARCHIVOS Y DIRECTORIOS EN RUTAS POCO COMUNES QUE NO SE VISUALICEN CON FRECUENCIA POR LOS USUARIOS HABITUALES.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

DETERMINACIÓN DE CÓMO SE REALIZÓ EL ATAQUE

DEBERÁ REALIZARSE UN ANÁLISIS PARA **DETECTAR CÓMO SE ACCEDIÓ AL SISTEMA**, INVESTIGANDO LAS VULNERABILIDADES DE LAS QUE SE HAYA PODIDO APROVECHAR EL ATACANTE PARA ACCEDER A ESTE.

TAMBIÉN SE DEBERÁ INVESTIGAR **CUÁLES FUERON LAS HERRAMIENTAS UTILIZADAS** POR EL ATACANTE QUE LE PERMITIERON APROVECHARSE DE LA VULNERABILIDAD O FALLO DE ADMINISTRACIÓN Y ACCEDER AL SISTEMA.

PARA ELLO SE REALIZARÁN CONSULTAS Y SE ANALIZARÁN ARCHIVOS DE LOGS, REGISTROS, CUENTAS DE USUARIOS, ETC.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

IDENTIFICACIÓN DEL ATACANTE O ATACANTES

ES FUNDAMENTAL, SOBRE TODO CUANDO LA ORGANIZACIÓN QUIERE TOMAR ACCIONES LEGALES CONTRA LOS RESPONSABLES.

DEBERÁ INTENTAR AVERIGUARSE INICIALMENTE LA DIRECCIÓN IP DEL ATACANTE MEDIANTE LA REVISIÓN DE LOS REGISTROS DE LAS CONEXIONES DE RED.

LA IDENTIFICACIÓN SERÁ POSIBLE SOBRE TODO CON EL ANÁLISIS DE LAS EVIDENCIAS VOLÁTILES, YA QUE SON LOS QUE CONTIENEN INFORMACIÓN SOBRE CONEXIONES FALLIDAS, ARCHIVOS TEMPORALES, ARCHIVOS ELIMINADOS, INFORMACIÓN SOBRE CORREOS ELECTRÓNICOS, ETC.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

EVALUACIÓN DEL IMPACTO CAUSADO

ES FUNDAMENTAL **ANALIZAR EL IMPACTO CAUSADO POR EL ATACANTE EN EL SISTEMA**, QUÉ HAN HECHO LOS ATACANTES UNA VEZ HAN ACCEDIDO AL SISTEMA Y SI HA PODIDO COMPROMETER LA INFORMACIÓN DE LOS EQUIPOS. SE DISTINGUIRÁN DOS **TIPOS DE ATAQUES**:

- **ACTIVOS**
- **PASIVOS**

TAMBIÉN DEBERÁ INTENTAR DEDUCIRSE EL IMPACTO POTENCIAL DEL ATAQUE (EL IMPACTO QUE HUBIERA TENIDO SI NO SE HUBIERAN TOMADO MEDIDAS A TIEMPO) PARA AYUDAR A DEFINIR MEDIDAS DE PREVENCIÓN DE ATAQUES FUTURAS.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

DOCUMENTACIÓN DEL ATAQUE

DEBE LLEVARSE A CABO LA DOCUMENTACIÓN DE TODAS LAS ACCIONES REALIZADAS EN LA RECOLECCIÓN Y ANÁLISIS DE LAS EVIDENCIAS.

ES IMPRESCINDIBLE DEJAR ANOTADAS TODAS LAS ACTIVIDADES EJECUTADAS PARA AUMENTAR LA EFICIENCIA DEL ANÁLISIS FORENSE Y DISMINUIR LAS POSIBILIDADES DE ERROR EN LA OBTENCIÓN DE RESULTADOS.

PARA QUE LA DOCUMENTACIÓN SEA CORRECTA Y EFECTIVA SE RECOMIENDA LA **UTILIZACIÓN DE FORMULARIOS** QUE DEBERÁN SER RELLENADOS POR LOS RESPONSABLES DE LA GESTIÓN DEL ATAQUE Y DE LAS EVIDENCIAS.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

DOCUMENTACIÓN DEL ATAQUE

EN CONCRETO DEBERÍAN ELABORARSE **FORMULARIOS** COMO MÍNIMO DE LOS SIGUIENTES ASPECTOS:

- CADENA DE CUSTODIA DE LA EVIDENCIA.
- IDENTIFICACIÓN DE LOS EQUIPOS, COMPONENTES Y DISPOSITIVOS.
- ATAQUES TIPIFICADOS.
- RECOLECCIÓN Y ALMACENAMIENTO DE LAS EVIDENCIAS.
- DISCOS DUROS DE LA ORGANIZACIÓN.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

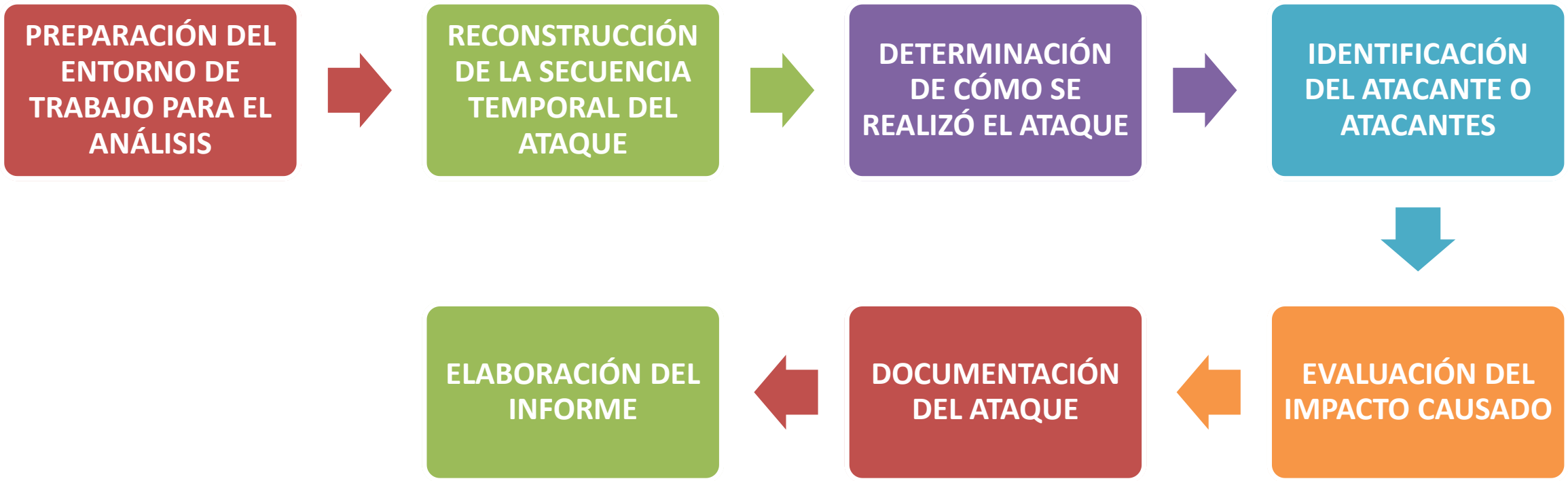
ELABORACIÓN DEL INFORME

EL **INFORME** DESCRIBIRÁ LAS HERRAMIENTAS, METODOLOGÍA, TÉCNICAS UTILIZADAS Y LOS HALLAZGOS OBTENIDOS. **DEBERÁ CONTENER**:

- ANTECEDENTES DEL ATAQUE
- RECOLECCIÓN PREVIA DE DATOS Y EVIDENCIAS
- DESCRIPCIÓN DE LA EVIDENCIA
- HERRAMIENTAS UTILIZADAS EN EL ANÁLISIS
- ANÁLISIS DE LA EVIDENCIA
- DESCRIPCIÓN DE LOS HALLAZGOS ENCONTRADOS
- CRONOLOGÍA DEL ATAQUE
- CONCLUSIONES
- RECOMENDACIONES

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

FASES DEL ANÁLISIS DE EVIDENCIAS



NO HAY QUE OLVIDAR LA IMPORTANCIA DE LA PRESERVACIÓN DE LA CADENA DE CUSTODIA EN TODAS LAS FASES DEL ANÁLISIS DE LAS EVIDENCIAS

CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE
3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD
4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS
5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS
6. **GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE**

5. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

LOS ATACANTES CADA VEZ UTILIZAN TÉCNICAS MÁS SOFISTICADAS PARA LLEVAR A CABO SUS ATAQUES .

LA **DETECCIÓN DE EVIDENCIAS Y EL POSTERIOR ANÁLISIS DE LAS MISMAS** PUEDE SER UNA **TAREA BASTANTE TEDIOSA** PARA LOS INVESTIGADORES SI NO UTILIZAN **HERRAMIENTAS ESPECÍFICAS** QUE COMPLETEN Y AÑADAN EFICACIA A LA INVESTIGACIÓN.

LA ELECCIÓN DE LA HERRAMIENTA ADECUADA DEPENDERÁ DEL SISTEMA OPERATIVO UTILIZADO Y DE LA PREFERENCIA ENTRE SOFTWARE COMERCIAL Y SOFTWARE LIBRE.

5. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

LAS HERRAMIENTAS MÁS UTILIZADAS PARA EL ANÁLISIS FORENSE SON LAS QUE SE LISTAN A CONTINUACIÓN:

AUTOPSY, ENCRYPTED DISK DETECTOR, WIRESHARK, MAGNET RAM CAPTURE, NETWORK MINER, NMAP, RAM CAPTURER, FORENSIC INVESTIGATOR, FAW, HASHMYFILES, CROWD RESPONSE, NFI DEFRASER, EXIFTOOL, TOOLSLEY, SIFT, DUMPZILLA, BROWSER HISTORY, FORENSICUSERINFO, KALI LINUX, PALADIN, SLEUTH KIT, CAINE, FTK IMAGER

CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE
3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD
4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS
5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS
6. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

RESUMEN

DEBIDO A LA PRESENCIA CRECIENTE DE INCIDENTES DE SEGURIDAD SURGIERON LAS **HERRAMIENTAS DE ANÁLISIS FORENSE DIGITAL**.

SE TRATA DE UNA DISCIPLINA DENTRO DE LA SEGURIDAD INFORMÁTICA QUE *SE ENCARGA DE ANALIZAR LOS INCIDENTES DE SEGURIDAD Y LOS DELITOS DIGITALES A POSTERIORI PARA RECONSTRUIR LOS HECHOS Y CONSEGUIR DETECTAR AL ATACANTE Y AVERIGUAR CÓMO HA ACCEDIDO A LOS EQUIPOS*.

LOS USOS Y OBJETIVOS DE ESTOS ANÁLISIS SON DE LO MÁS VARIADOS Y PUEDEN UTILIZARSE TANTO PARA APORTAR PRUEBAS PARA INVESTIGAR DELITOS DE FRAUDE CON COMPAÑÍAS DE SEGUROS, COMO PARA REALIZAR INVESTIGACIONES CON ÓRDENES JUDICIALES, ENTRE OTROS.

RESUMEN

PARA DESARROLLAR LAS TÉCNICAS DE ANÁLISIS FORENSE DIGITAL DEBE SEGUIRSE UNA METODOLOGÍA CON UNAS **FASES** PERFECTAMENTE DEFINIDAS**: ESTUDIO PRELIMINAR, RECOPILACIÓN DE EVIDENCIAS, ANÁLISIS DE EVIDENCIAS Y ELABORACIÓN DE INFORMES CON LOS RESULTADOS.**

CON LA CORRECTA APLICACIÓN DE ESTAS FASES Y UN MANTENIMIENTO ADECUADO DE LA CADENA DE **CUSTODIA DE LAS EVIDENCIAS** (QUE IMPIDA QUE LA INFORMACIÓN RECOPILADA SE MODIFIQUE Y PUEDA LLEVAR A RESULTADOS ERRÓNEOS) SE PUEDE LLEGAR A DESCUBRIR EL ORIGEN DEL ATAQUE, LOCALIZAR AL ATACANTE E, INCLUSO, TOMAR MEDIDAS LEGALES CONTRA ESTE PARA EXIGIRLE RESPONSABILIDAD POR LOS DAÑOS CAUSADOS.

RESUMEN

POR ESTE MOTIVO, LOS DISTINTOS ATACANTES CADA VEZ UTILIZAN TÉCNICAS MÁS SOFISTICADAS PARA OCULTAR SUS HUELLAS Y EVITAR SER DESCUBIERTOS.

AUN ASÍ, SE PUEDEN ENCONTRAR EN EL MERCADO VARIAS HERRAMIENTAS (TANTO DE PAGO, COMO GRATUITAS Y PARA VARIOS SISTEMAS OPERATIVOS) QUE CONSIGUEN RECOGER EVIDENCIAS Y DETECTAR AL CULPABLE CON BASTANTE PROBABILIDAD.

ESTO ES TODO