SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

3.3.1.MF0488_3. Capítulo 3
Parte 1
Análisis forense informático

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Ante cualquier incidente es necesario detectar al responsable para poder reclamarle exigencias legales y económicas si procede.

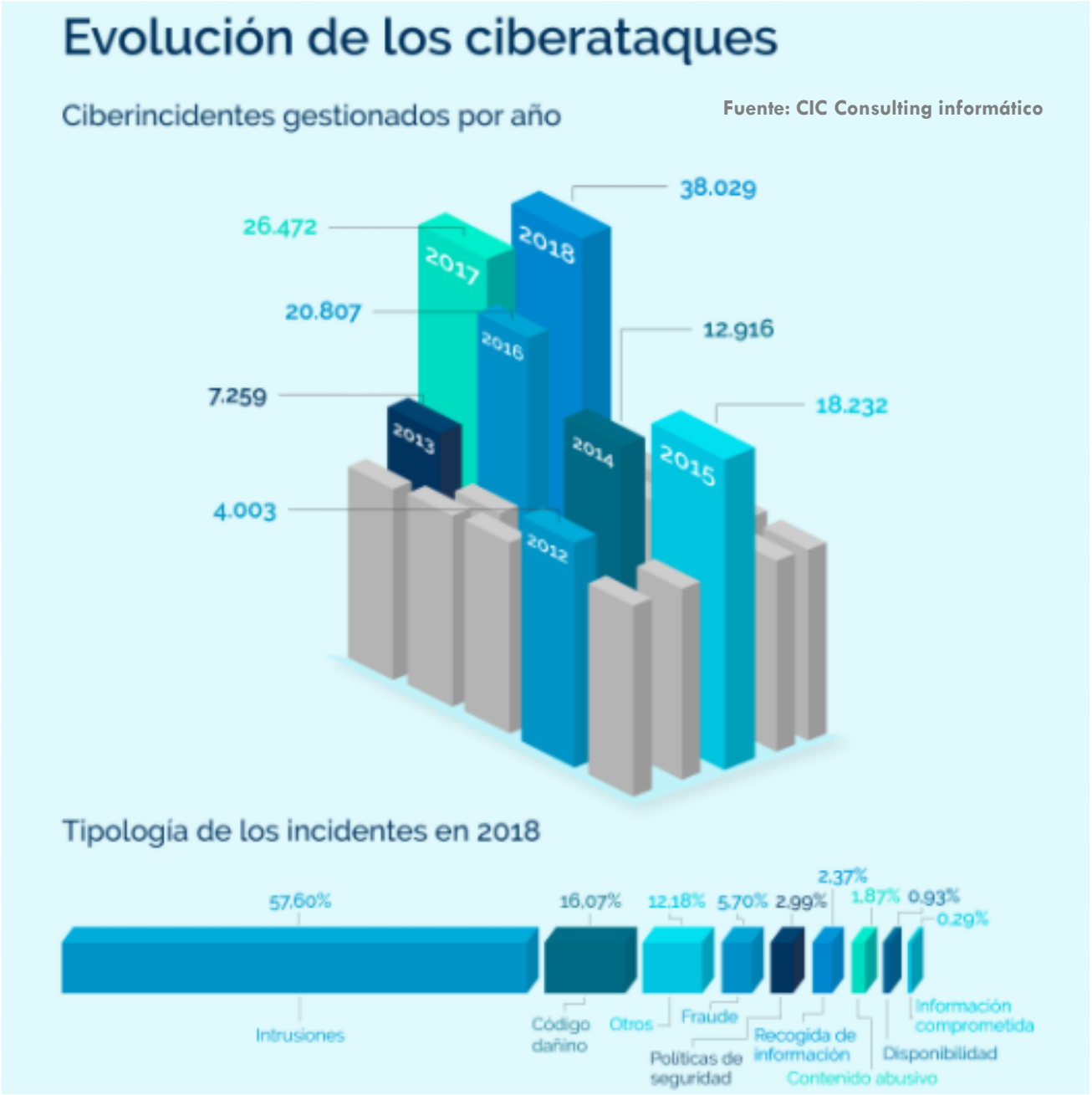
Una de las principales herramientas para conseguir detectar a estos responsables es el análisis forense informático, una ciencia que se dedica a obtener "huellas" en los incidentes sucedidos para lograr encontrar a un culpable de un modo razonable y correctamente justificado.

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



2.1. 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.

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.

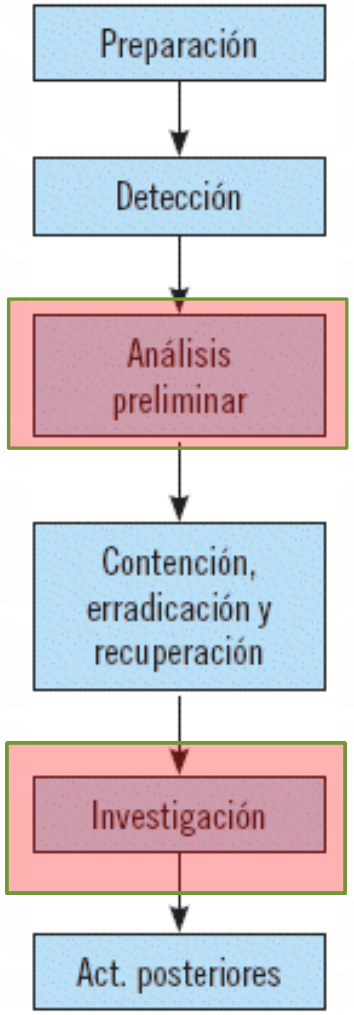
2.1. OBJETIVOS Y USOS DE LA INFORMÁTICA FORENSE

Los usos de la informática forense pueden ser de lo más variado. A continuación se describen los más importantes:

- Persecución criminal.
- Litigación civil.
- Investigación de seguros.
- Mantenimiento de la ley.
- Usuario final.
- Organizaciones y temas corporativos.

2.2. METODOLOGÍA DEL ANÁLISIS FORENSE INFORMÁTICO

Procedimiento de gestión de incidentes



2.2. METODOLOGÍA DEL ANÁLISIS FORENSE INFORMÁTICO

Fases del análisis forense informático

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

Edmond Locard (Francia, 1877-1966), criminalista francés, fue uno de los pioneros en criminología y fundó el Instituto de Crimininalística de la Universidad de Lyon.

Es conocido por enunciar el famoso principio de intercambio o transferencia de Locard.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

Todo procedimiento de recolección y análisis de evidencias debe tener en cuenta y llevar a cabo 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.

3.1. EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

El principio de Locard se define como:

“Cada contacto deja un rastro”

3.1. EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

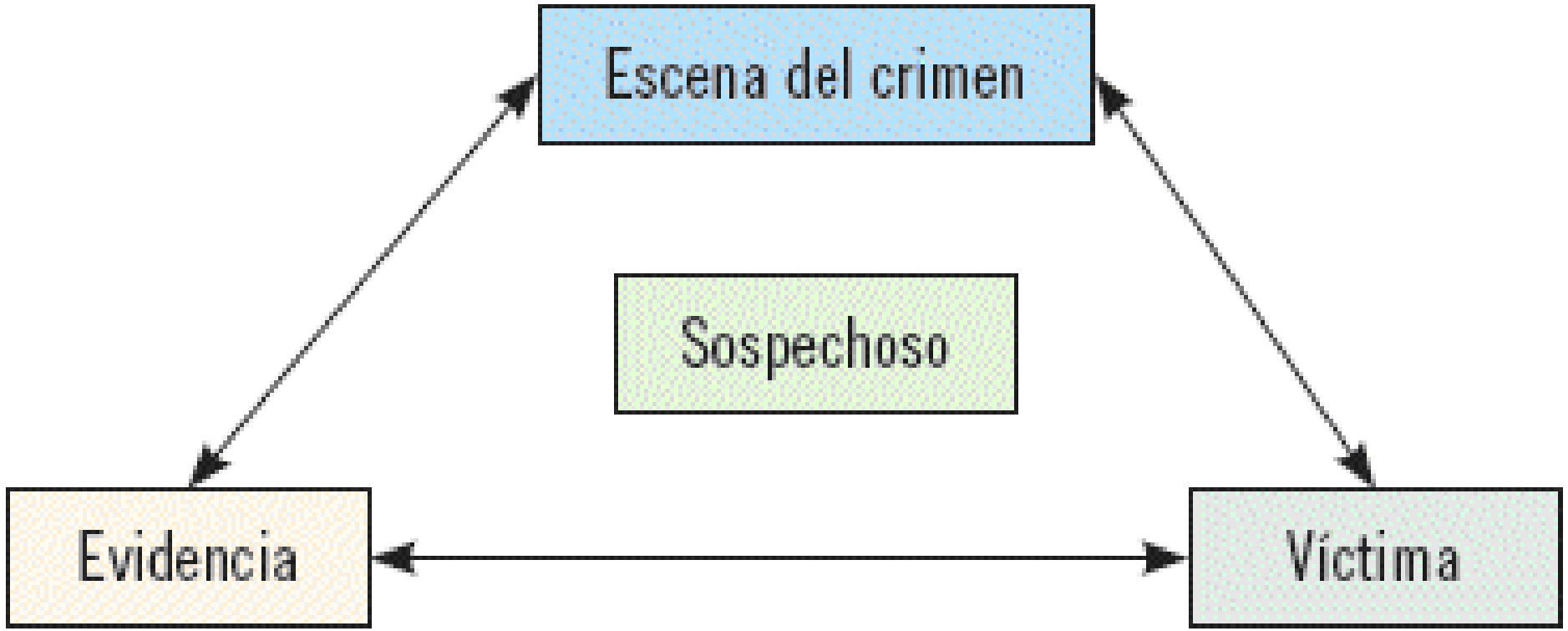
Evidencias transitorias.

Evidencias curso o patrones.

Evidencias condicionales.

Evidencias transferidas.

3.1. EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD



3.1. EL PRINCIPIO DE INTERCAMBIO O TRANSFERENCIA DE LOCARD

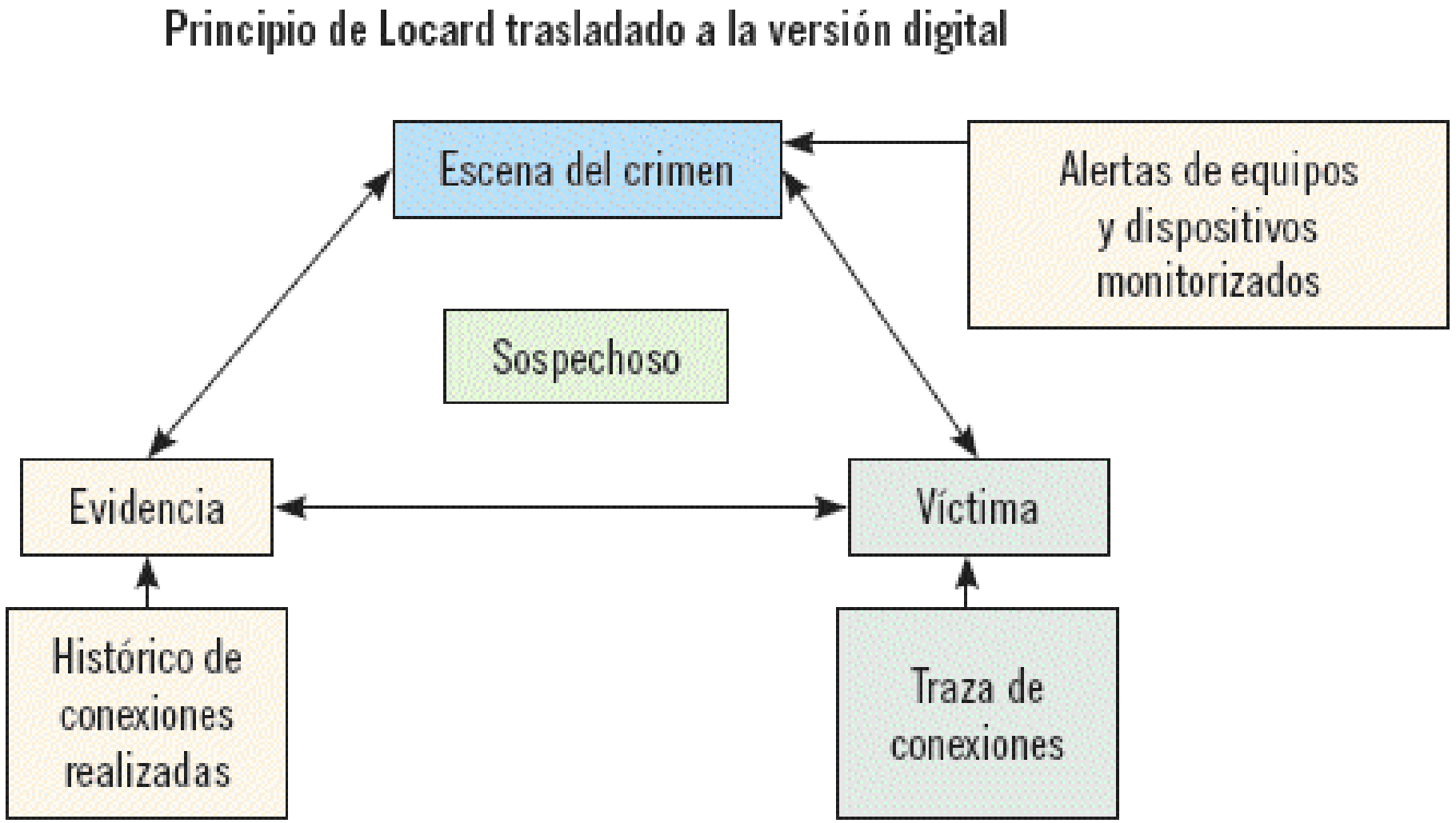
Principio de intercambio de Locard	
"Cada contacto deja un rastro"	La víctima deja rastro en la escena del crimen y en el sospechoso.
	El sospechoso deja rastro en la víctima y en la escena del crimen.
	Tanto la víctima como el sospechoso tendrán algún rastro de la escena del crimen.
Tipos de evidencias físicas	Evidencias transitorias.
	Evidencias curso o patrones.
	Evidencias condicionales.
	Evidencias transferidas.
Métodos de transferencia de evidencias	Transferencia directa.
	Transferencia indirecta.

3.2. APLICACIÓN DEL PRINCIPIO DE LOCARD AL ANÁLISIS FORENSE DIGITAL

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).

3.2. APLICACIÓN DEL PRINCIPIO DE LOCARD AL ANÁLISIS FORENSE DIGITAL



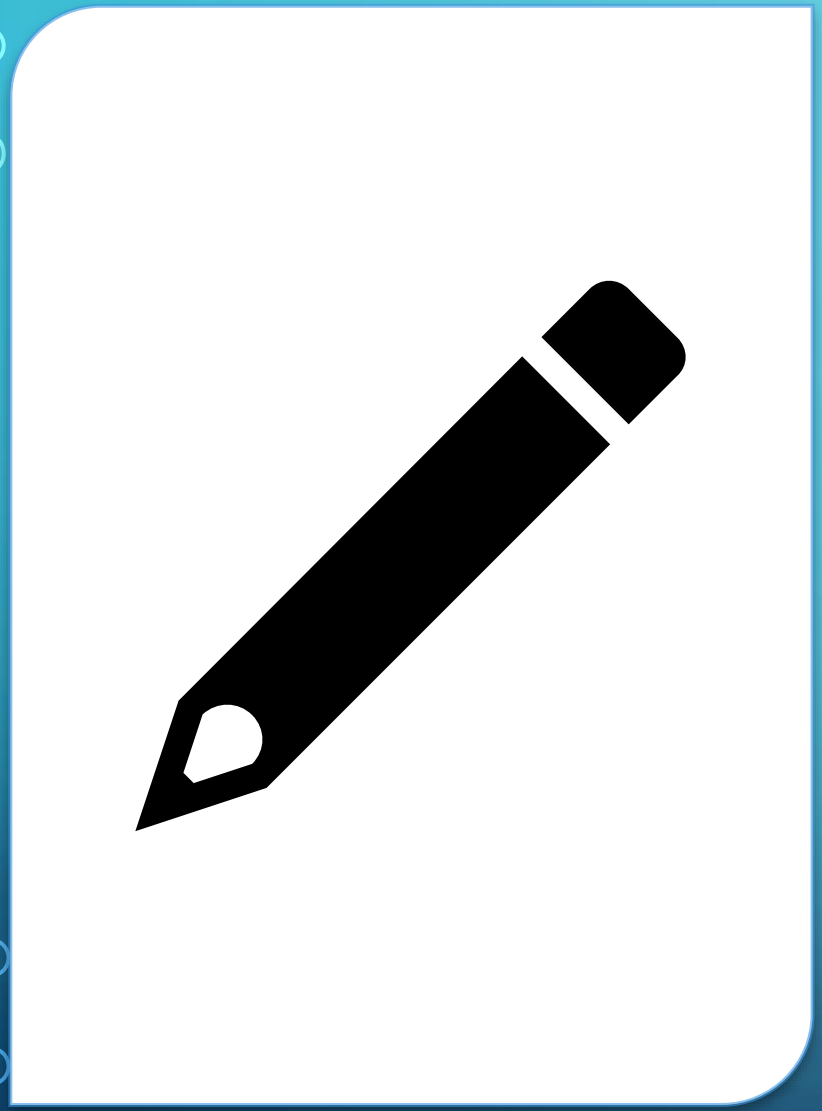
3.2. APLICACIÓN DEL PRINCIPIO DE LOCARD AL ANÁLISIS FORENSE DIGITAL

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.

Ejemplo

ESTABA REALIZANDO UNAS GESTIONES EN SU EQUIPO Y DE REPENTE LE HA SALTADO UNA ALARMA INDICÁNDOLE QUE UN VIRUS HA ACCEDIDO AL ORDENADOR. TENIENDO EN CUENTA EL PRINCIPIO DE INTERCAMBIO DE LOCARD IDENTIFIQUE LOS DISTINTOS ELEMENTOS QUE INTERVIENEN EN EL ATAQUE.



Ejemplo. Solución

SEGÚN EL PRINCIPIO DE INTERCAMBIO DE LOCARD, EN UN ATAQUE SE DETECTAN TRES ELEMENTOS: EL SOSPECHOSO, LA VÍCTIMA Y LA ESCENA DEL CRIMEN.

EN ESTE CASO, EL SOSPECHOSO SERÍA EL VIRUS SOBRE EL QUE HA ALERTADO EL SISTEMA. LA VÍCTIMA SERÍA EL EQUIPO, YA QUE ES EL QUE VA A SUFRIR LOS DAÑOS DEL ATAQUE Y LA ESCENA DEL CRIMEN SERÍA EL SISTEMA OPERATIVO UTILIZADO EN EL EQUIPO Y A TRAVÉS DEL CUAL HA ACCEDIDO EL ATACANTE AL EQUIPO.