Escuela Politécnica del Ejército

"ELABORACIÓN DEL PROTOCOLO DE PRIMERA RESPUESTA A DELITOS INFORMÁTICOS"

Karla Villacreses

Pablo Reyes

Objetivo General

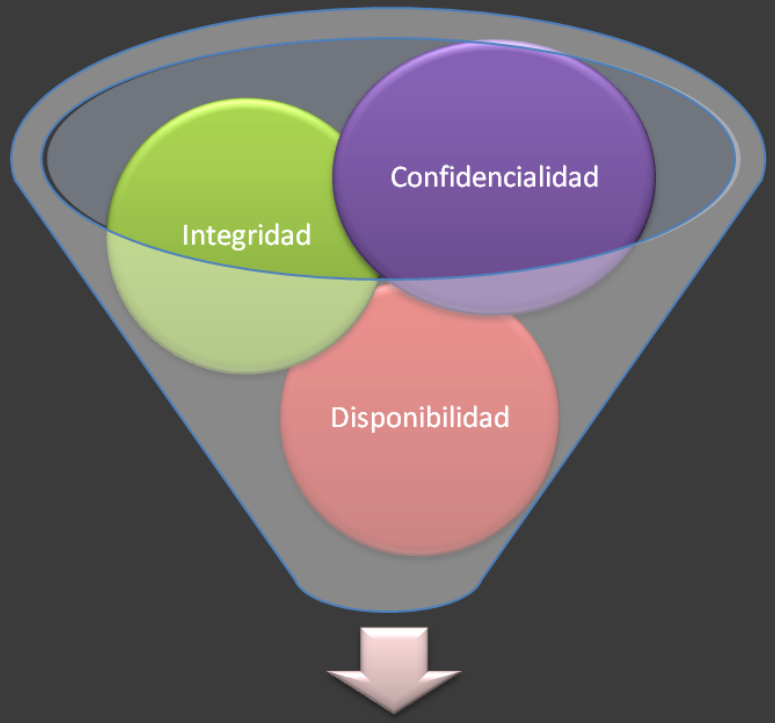
- Elaborar un protocolo genérico de primera respuesta a delitos informáticos, que permita: **identificar, manejar, preservar, analizar y presentar información**; que pueda ser utilizada como evidencia dentro de un proceso legal en el Ecuador.

Planteamiento del Problema

Transacciones actuales se realizan con ayuda de tecnología

Gran crecimiento tecnológico → mayor seguridad

Incidentes informáticos



Seguridad

Tipos de incidentes informáticos

Criminalidad

- Ataques informáticos
- Si estas acciones se encuentran tipificadas en el Código Penal, estas se clasifican como delitos informáticos.

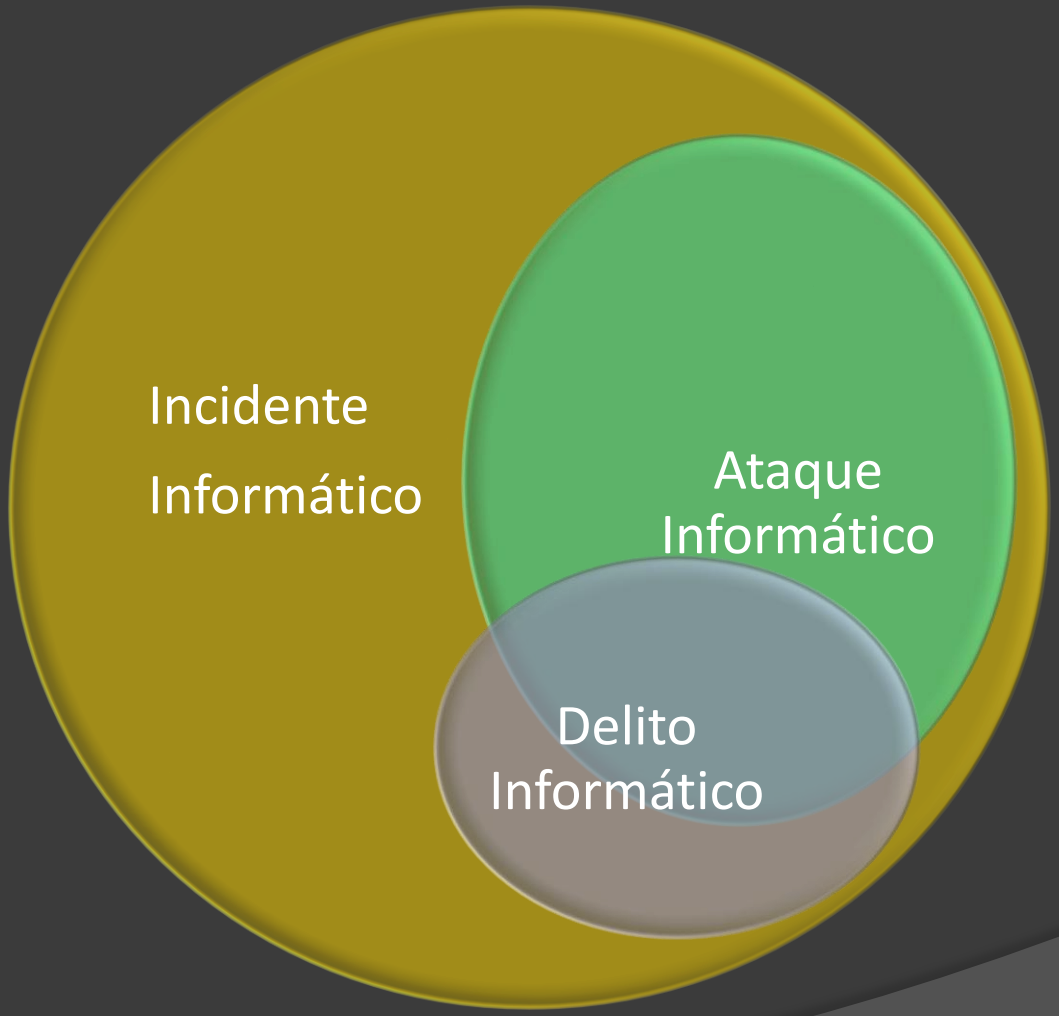
Sucesos de origen físico

- Eventos naturales y técnicos
- Pueden o no contar con intervención humana
- No entran en las categorías de ataque o delito informático
- Califican como error humano.

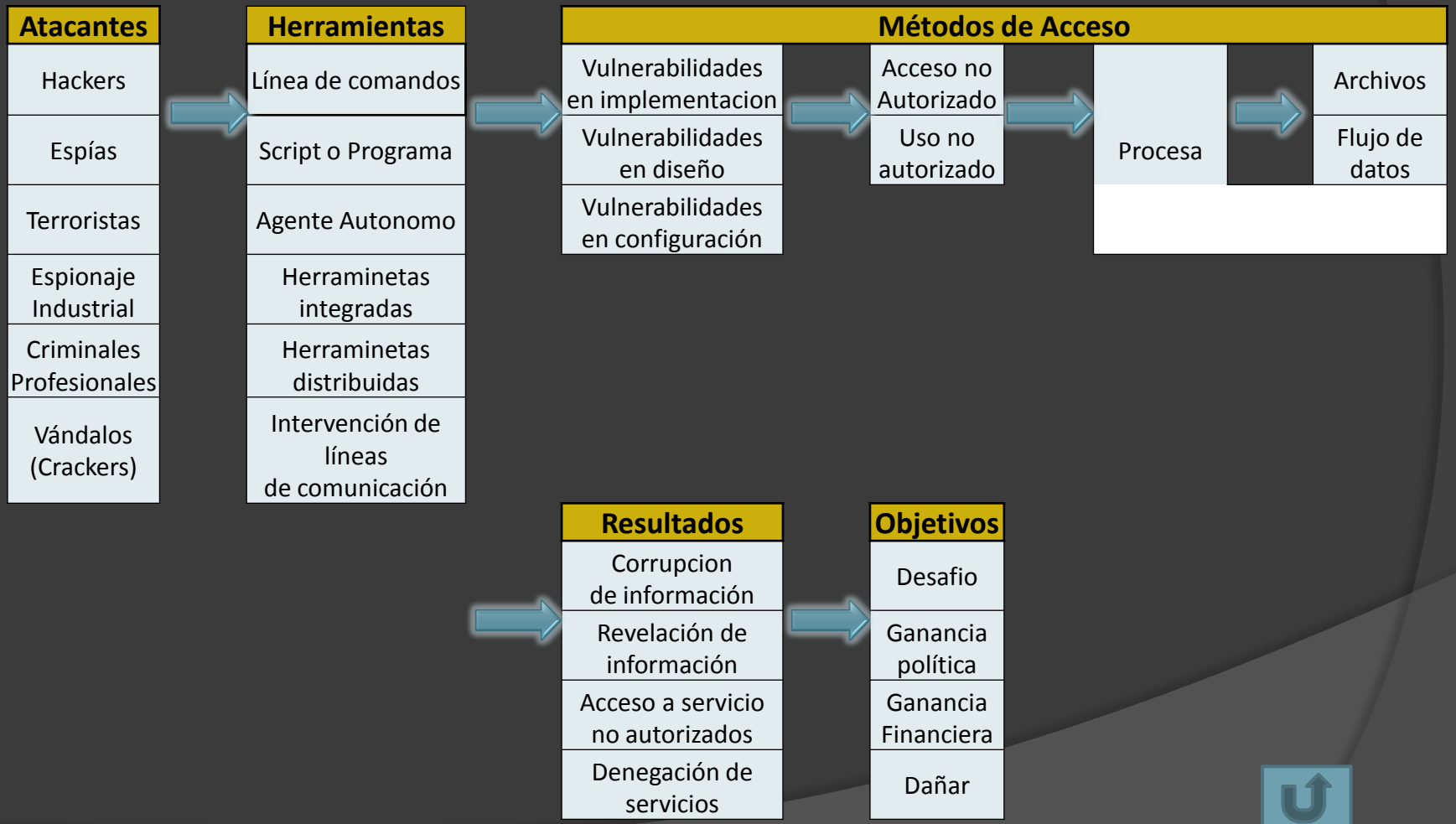
Negligencia y decisiones institucionales

- Acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema.
- Amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

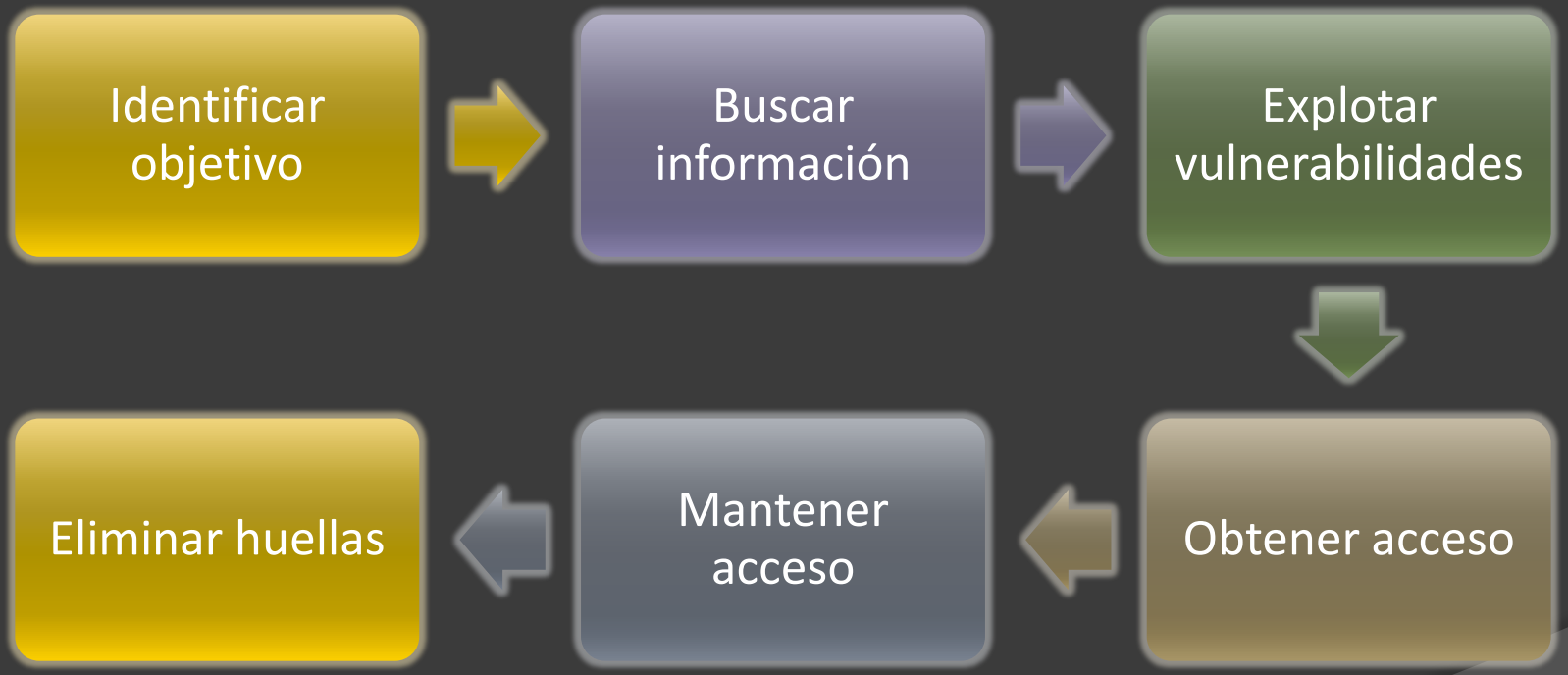
Tipos de incidentes informáticos



Ataques Informáticos



Fases de un ataque informático



Debilidades de Seguridad

- Ingeniería social
- Factor Insiders
- Códigos maliciosos
- Contraseñas inseguras
- Configuraciones predeterminadas

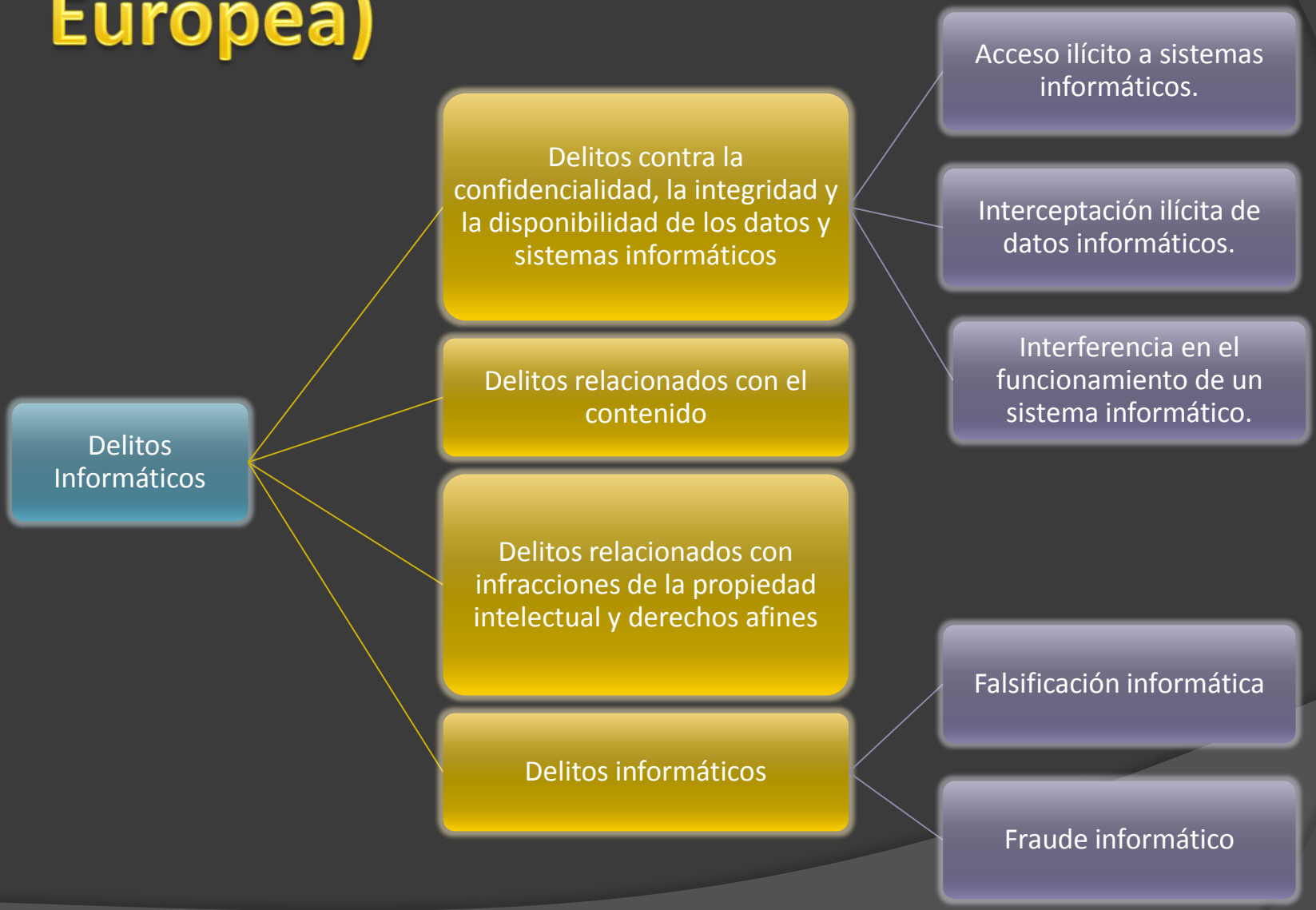
Delitos Informáticos

- Un delito informático puede definirse como cualquier conducta o **comportamiento ilícito, antijurídico, doloso** en los cuales se usa un computador para manipular datos o procesos.

Características de un delito informático

- El **delito es un acto humano**, (acción u omisión).
- Dicho acto humano ha de **ser antijurídico**, debe lesionar o **poner en peligro un interés jurídicamente protegido**.
- Debe **corresponder a un tipo legal** (figura de delito), definido por la ley, ha de ser un acto típico.
- Ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.
- La ejecución u omisión del acto **debe estar sancionada por una pena.**

Tipos de delitos informáticos (Unión Europea)



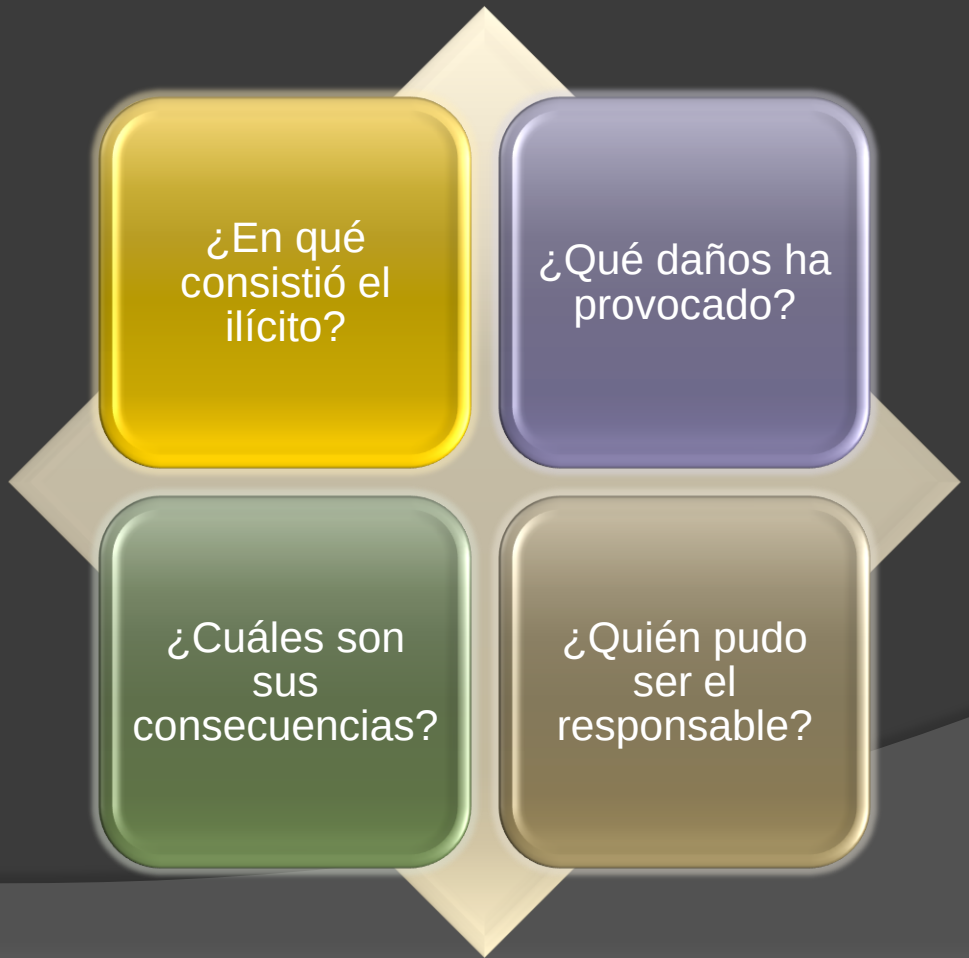
Tipos de Delitos (legislación ecuatoriana)

A partir del año 2002, se reconocen en el Código Penal los siguientes delitos:

- Delitos contra la Información Protegida: Destrucción o supresión de documentos o programas
- Delitos contra la Información Protegida: Violación de claves o sistemas de seguridad
- Falsificación Electrónica
- Fraude Informático
- Daños informáticos
- Violaciones al Derecho a la Intimidad (Contravención)
- Pornografía Infantil

Evidencia Digital

Toda información que podrá ser **capturada y** posteriormente **analizada para interpretar de la forma más exacta posible el incidente de seguridad,** debe responder preguntas como:

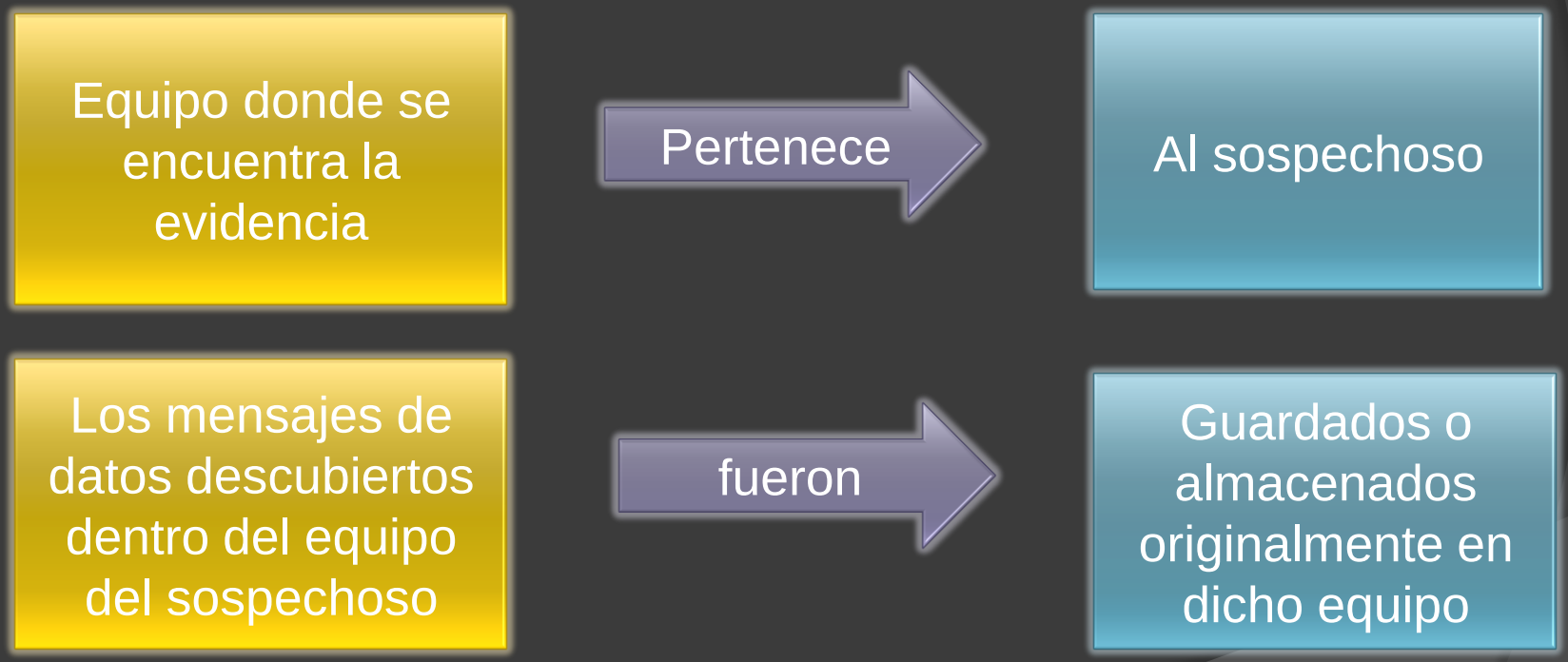


Características de la evidencia

Admisible	Autentica	Completa	Fiable	Creíble
• La evidencia debe ser **capaz de utilizarse en una corte o juzgado.**	• Debe demostrarse que las **pruebas se refieren al incidente y a la escena del crimen** en investigación.	• Recolectar la **suficiente evidencia** que muestre la perspectiva del incidente y permita poder **incriminar a un atacante o también inculpar** a alguien si así fuese el caso.	• La evidencia **no debe causar duda de su veracidad y autenticidad**.	• La evidencia debe ser **clara y entendible** de acuerdo al nivel profesional

Normas de recolección de evidencia

- El Estado a través del órgano de persecución penal que es la Fiscalía General del Estado debe establecer:



Legislación sobre validez de la evidencia digital en Ecuador

Con el fin de que la evidencia recolectada pueda ser usada en Ecuador, es necesario tener en cuenta los principios y normas legales que están en relación con la evidencia de cualquier tipo

- Principio de equivalencia funcional (mensaje de datos mismo valor jurídico que los documentos escritos).
- Validez de las actuaciones procesales por medio de las tecnologías de la información y comunicación.
- Mensajes de datos (firmas electrónicas, documentos electrónicos y certificados electrónicos) como medio de prueba.

First Responder

- Un First Responder es el primer agente que responde a la aplicación de la ley u otro funcionario de seguridad pública, o proveedor de servicios que llega al lugar antes de la llegada del investigador a cargo. Debe ser el primero en notificar y responder a un incidente de seguridad, su deber es manejar el incidente y determinar sus posibles y principales motivos.

- De acuerdo a la legislación de Ecuador, la investigación de los delitos informáticos, deberá llevarse a cabo por un fiscal.

Consideraciones sobre los investigadores de delitos informáticos en Ecuador

- El funcionario de la Fiscalía o de la Policía Judicial nunca debe acudir sólo al lugar de los hechos, **mínimo por dos funcionarios**.
- Ninguna acción debe tomarse por parte de la Policía Judicial, la Fiscalía o por sus agentes y funcionarios que cambie o altere la información almacenada dentro de un sistema informático o medios magnéticos.
- En circunstancias excepcionales una persona competente puede tener acceso a la información.
- Se debe llevar una bitácora de todos los procesos adelantados en relación a la evidencia digital.
- El Fiscal del Caso y/o el oficial a cargo de la investigación son responsables de garantizar el cumplimiento de la ley y del apego a estos principios, los cuales se aplican a la posesión y el acceso a la información almacenada en el sistema informático.

Legislación Procesal sobre búsqueda y recolección de evidencia en Ecuador

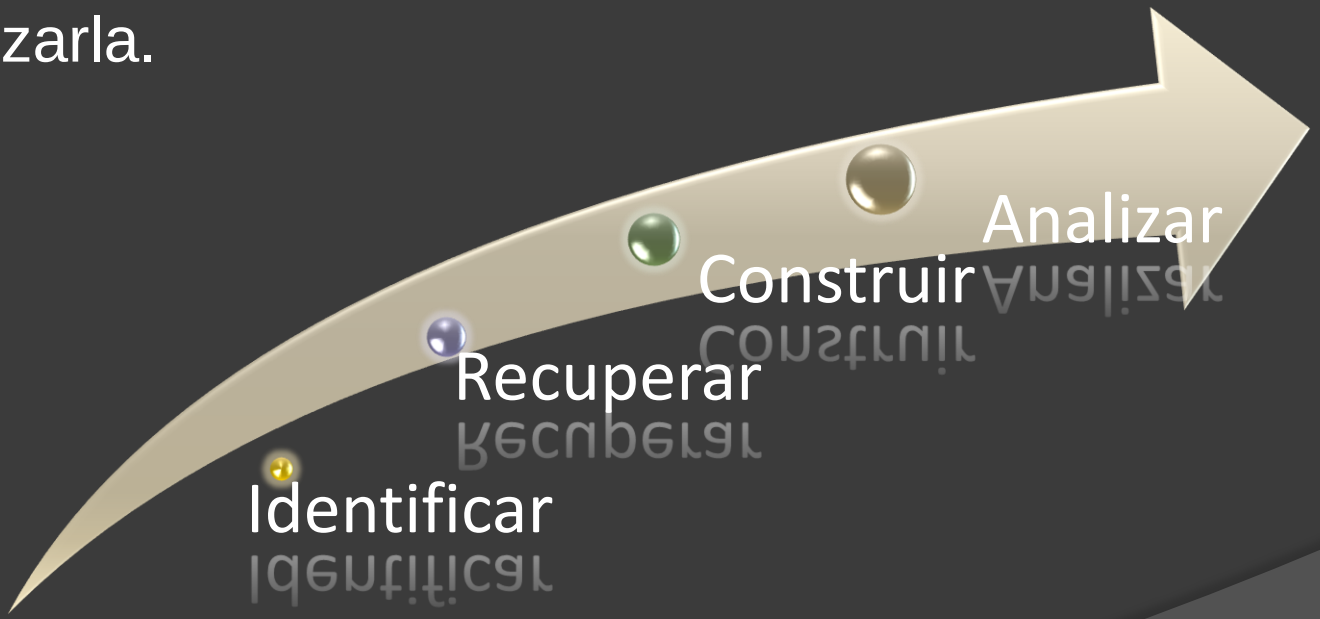
Tanto el First responder como todos los involucrados en el proceso de recolección de datos e investigación deben responder al Código Penal.

ACTIVIDAD PROCESAL

- Incautación
- Petición de Información
- Apertura de correspondencia
- Interceptación de Comunicaciones
- Reconocimiento de la evidencia

Principio de la Ciencia forense

La ciencia forense suministra los principios y técnicas que norman la investigación del delito criminal con el fin de estandarizarla, facilitarla y agilizarla.



Principios fundamentales durante este decisivo proceso

- Juntar al grupo de trabajo; seguridad policial, un manual de incidentes (no informáticos), y abogados
- Recoger y examinar huellas dactilares y ADN.
- Filmar y fotografiar detalles de los sistemas tanto como sea posible.
- Tomar nota de los detalles y acciones realizadas incluyendo fecha y hora exacta.
- Diferenciar la hora en cada detalle, dato o evidencia obtenida, ubicando y especificando el tiempo utilizado.
- Evitar realizar cambios a los datos durante la recolección, evitar actualizar tiempos y estado de archivos o directorios.

Principios fundamentales durante este decisivo proceso

- Disminuir la interacción externa de los equipos para evitar cambio de datos.
- Recolectar primero toda la evidencia para luego analizarla
- Implementar metodologías que garanticen el accionar durante el proceso
- La recolección de evidencias debe ser mediante un análisis de volatilidad
- Se deberá realizar una copia de las evidencia originales y para análisis o pruebas posteriores en laboratorios sacar copias de la copia de los originales no trabajar sobra la copia obtenida de las evidencia
- Firmar digitalmente un documento para poder afirmar que es auténtico y preservar la cadena de evidencias.

Proceso de la Cadena de Custodia de la evidencia

La cadena de custodia sigue los procesos en un orden estricto para no ser alterada contemplando:

- La identificación de la evidencia
- Definir el proceso que se seguirá durante la investigación
- Preservación de la evidencia
- Mantener la evidencia integra
- Utilización de métodos de preservación de información
- Análisis de las evidencias
- Responder preguntas como: ¿Quien?, ¿Qué?, ¿Cómo?, ¿Cuando?
- Identificar las evidencia del caso presente ajustados a los requerimientos del caso
- Presentación de las evidencias
- Realizar un informe adecuado que sea claro preciso y conciso.
- Deberá contener toda la evidencia encontrada y tratada en la escena
- Minimizar la manipulación e interacción con las evidencias originales

Preparación previa a la recolección de la evidencia digital

- Mantener la integridad de la escena del crimen
- Asegurar el área
- Mantener recordatorios
- Determinar responsabilidad y procedimientos
- Interrogar a los involucrados
- Aislar los equipos
- Decidir donde hacer el análisis

Herramientas (toolkit) y equipo para respuesta a incidentes

- Toolkit es un conjunto completo de herramientas y elementos que nos permitan determinar y documentar las evidencias para no perder ningún detalle que nos permita tener una idea clara del delito.

Tarea	Herramienta
Capturar y analizar logs para identificar quien y de donde han tenido accesos a los sistemas.	My Event View
Escanear, mapear y dar reportes de puertos abiertos, conexiones disponibles y accesos al usuario	Currports - WirelessView SniffPass - WireShark AdapterWatch
Respaldar bit a bit de un disco duro	FTK Imager - DD
Realizar una imagen y firmar electrónicamente un disco duro	FTK imager - Winen WFT – MDD
Examinar archivos en un disco duro	FileAnalyzer – WinAdusit
Documentar la Fecha y hora del sistema CMOS	MSI
Crackear contraseñas	Asterix Logger
Recolectar datos o archivos ocultos, dañados o borrados.	Recuva - Autopsy

Instrumentos para documentar

Etiquetas para cables	Cortadora de cables y alambres	Cinta adhesiva
Marcadores permanentes	Bolsas de pruebas	Guantes
Etiquetas adhesivas	Bolsas antiestéticas y plástico de burbujas	Bandas de goma
Herramientas para desmontar los equipos de diferentes tamaños no magnéticos	Suministros para almacenamiento y trasporte de evidencia	Lupa
Desarmadores de punta plana y de estrella	Materiales de embalaje (evitar materiales que puedan producir estática)	Lista de números de asistencia
Hexagonales	Cinta de embalaje	Papel de impresora
Alicate y pinzas pequeñas	Cajas resistentes de diferentes tamaños	Disco de captura de evidencia
Destornilladores especiales	Otros elementos	Pequeña linterna
Playo	Etiquetas de pruebas	Herramientas de documentación

Recolección de la evidencia

Encontrar los datos relevantes.

Crear un orden de volatilidad.

Obtención de información general del sistema

Obtención de datos volátiles

Creación de imagen forense

Preservar evidencia

Análisis Forense

Documentar todo.

Verificar información obtenida

Orden de volatilidad

- Cache de BIOS, cache de memoria, cache de disco, registros de sistema.
- Tablas de enrutamiento.
- Cache ARP
- Tabla de procesos.
- Estadísticas del Kernel o núcleo del sistema y módulos.
- Conexiones, configuración de Routers o Switches
- Memoria Principal
- Archivos temporales del sistema
- Discos duros y dispositivos de almacenamiento
- Accesos remotos, datos de monitoreo (Logs)
- Configuración física de la red (topología)
- Medios de archivar información (backups, discos,)

Obtención de datos volátiles

- Obtención del tiempo de encendido y apagado
- Análisis de red
- Análisis web

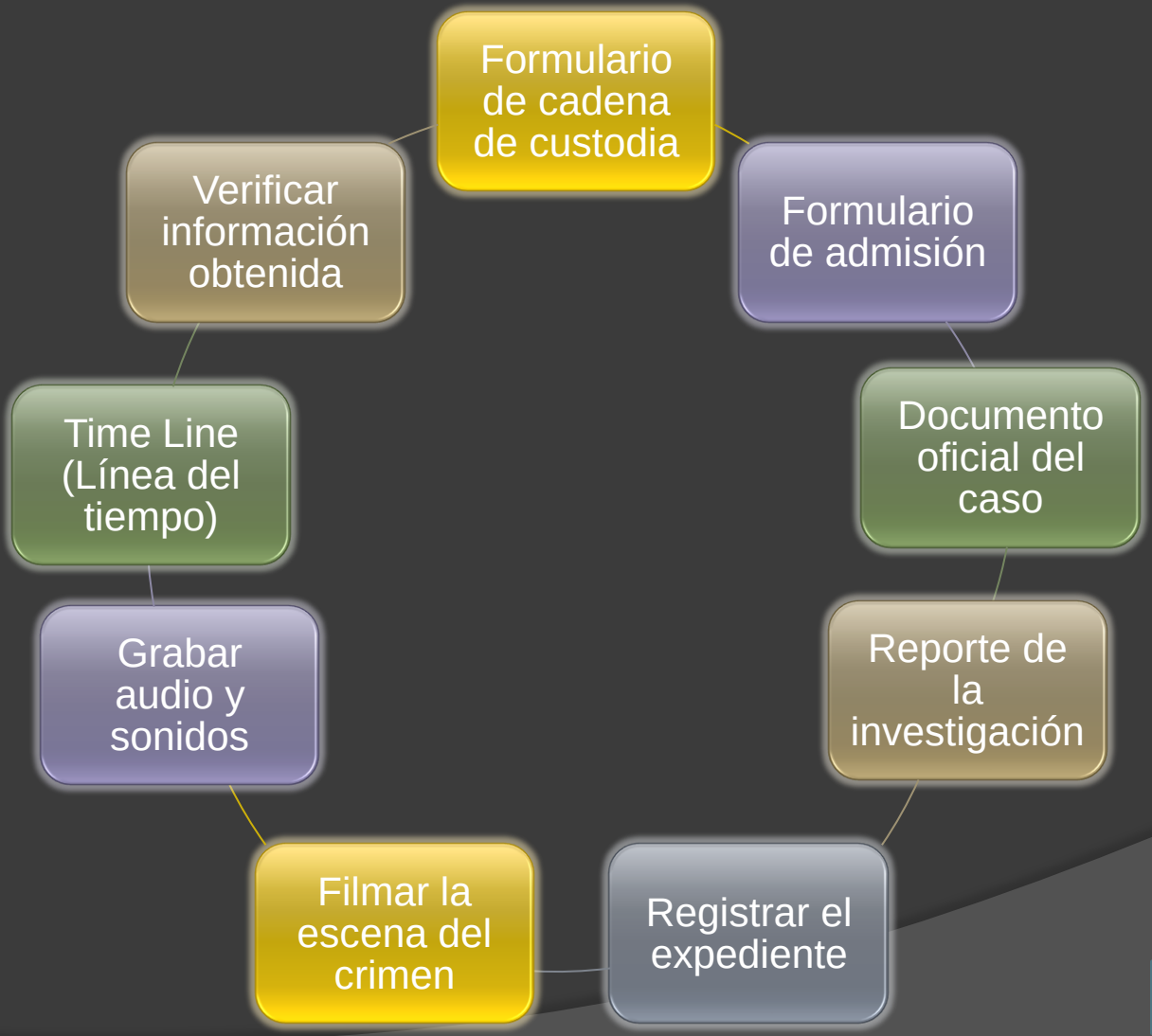
Creación de imagen forense

- Obtención de imágenes de un sistema apagado
- Adquisición física
- Adquisición a través de la red (máquina apagada)
- Adquisición a través de la red (máquina encendida

Análisis Forense

- Recuperación de información
- Análisis de logs
- Revisión de los archivos temporales
- Análisis de archivos

Documentación



Planteamiento del Caso

Datos Generales:

Equipo propiedad DiazProducctions,

Antecedentes

- Se sospecha que el sujeto usuario del computador es productor y comercializador de pornografía infantil.
- Existen personas capturadas como consumidores, quienes acusan a XXXX XXXX de enviar pornografía vía correo electrónico, así como de vender material con contenido obsceno en su domicilio, el cual aún no es localizado.

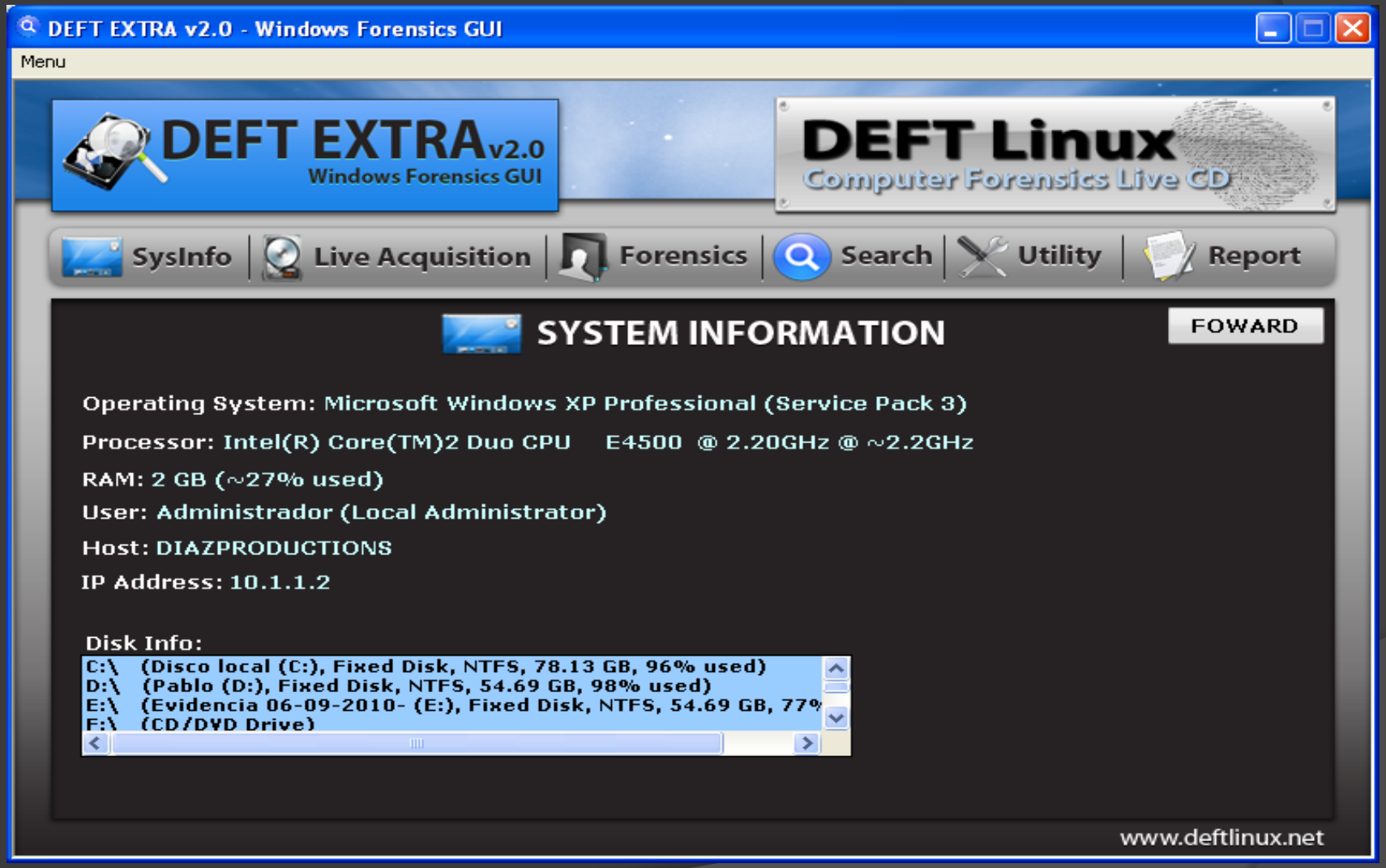
Planteamiento del Caso

- Los informantes testifican que el sujeto envía escondida la información, entre las personas sospechosas se encontró imágenes almacenadas en común.
- Existe la sospecha de que el hombre procuraba hacer un gran envió de mercancía, pero aún se desconoce la fecha y lugar del evento.
- Para el estudio se ha incautado un computador al cual estaba conectado una memoria flash USB, aún no se ha encontrado información culposa, razón por la cual es preciso proceder con un análisis de los dispositivos.

Proceso del Caso

- Objetivo: Determinar la posesión de imágenes dentro del computador que contienen pornografía infantil
- Tipo de computadora
- El sistema Operativo
- Ofensa: Posesión de pornografía infantil
- Agente del Caso
- Numero de Evidencia
- Cadena de Custodia
- Lugar donde se examino
- Herramientas utilizadas

Herramientas Windows



Pruebas de DEFT en caliente

- Datos generales del computador
- Procesos actuales corriendo
- Auditoria de programas instalados (fechas)
- Dispositivos externos conectados (fechas)
- Perfiles de Usuarios
- Información de Hardware del equipo
- Tiempos de encendido y apagado
- Análisis Web
  - Cuentas de Correo
  - Cookies y temporales de los diferentes navegadores
- Imagen del disco y dispositivos de almacenamiento extraíbles
- Montar imagen
- Recuperar datos eliminados

Herramientas Linux

Autopsy Forensic Browser

- Permite crear una imagen disco o dispositivo almacenamiento extraíble
- Crear un caso de investigación
- Montar la imagen extraída
- Comprobar código MD5
- Recupera archivos eliminados
- Revisar codificación de archivos

Forma de acción del criminal

niño raza blanca 8 años

soñe 8 ɐɔuɐlq ɐzɐɹ oñiu

Hexadecimal:

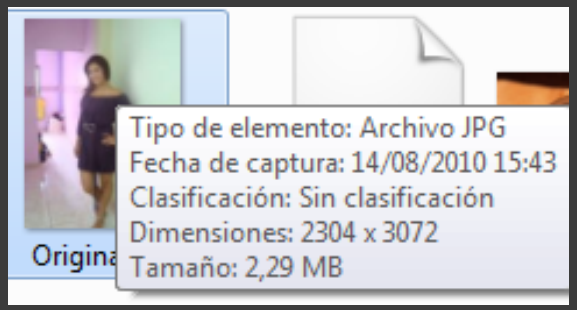
```
73:6f:1f:1f:20:38:20:1f:1f:75:1f:6c:71:20:1f:7a:1f:1
f:20:6f:1f:1f:75
```

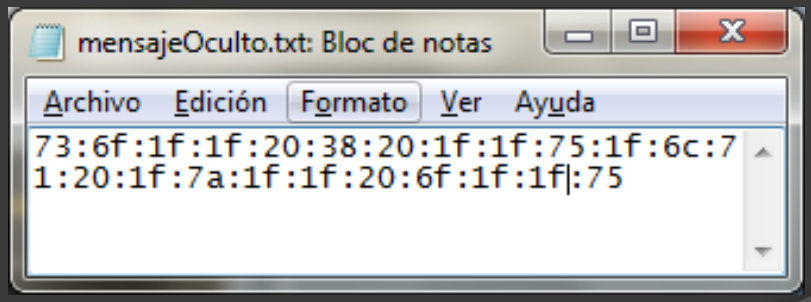
De Hexadecimal a ASCII

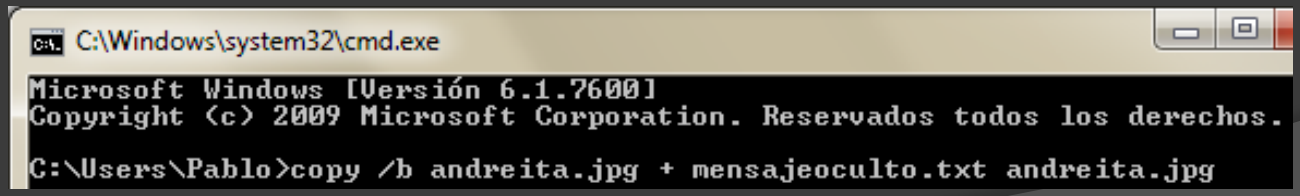
Ascii:

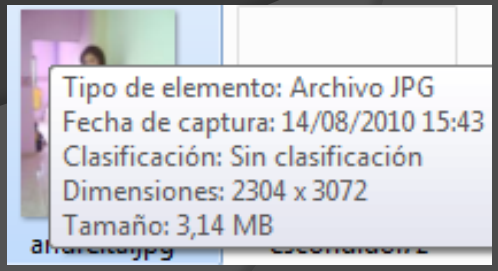
```
soñe 8 ɐɔuɐlq ɐzɐɹ oñiu
```

De ASCII a Hexadecimal









Evidencia encontrada

A partir del análisis forense de la información volátil, del ordenador DiazProductions, se obtuvo que:

- Entre los procesos que se encontraron activos en el momento de la recolección de evidencias, se destacan el software de diseño Adobe Photoshop CS3 y Microsoft Office Picture Manager, que es un visualizador de fotos de Windows.
- Se han conectado dos dispositivos extraíbles al ordenador, uno de los cuales se encontraba presente en la escena del crimen.
- El computador era usado por dos personas, entre semana en el horario de 14h00 a 22h00.

Evidencia encontrada

- Entre los archivos temporales de internet se halló que el sospechoso visitaba frecuentemente páginas web de contenido obsceno y que realizaba investigaciones sobre la adquisición de pornografía infantil.
- En el ordenador se accedía a una sola cuenta de correo electrónico la cual es diazmail@hotmail.com

Una vez que conseguida la información del ordenador, a partir del análisis del dispositivo encontrado se halló lo siguiente:

- Se encontró que se habían eliminado recientemente ficheros de extensión JPG de tamaño inconsistente.
- Ya recuperados los archivos se encontró que en su mayoría se trataba de imágenes de animales con información oculta.

Conclusión del Caso

A partir del análisis de los archivos recuperados se concluyó lo siguiente:

- Los archivos arrojaban datos sobre el lanzamiento de comercialización de un evento de pornografía infantil a efectuarse el día 30 de diciembre del 2010 en la ciudad de Quito, en la calle Calypso N4-5 y Rendón.
- Para poder asistir a este evento se requiere de una contraseña la cual es: 50000_.THIS

Conclusiones

- En torno a la clasificación de los delitos informáticos en el Ecuador, aún no se ha formalizado las leyes para muchos de los casos que afectan la integridad de los datos que viajan a través de la red y son parte de la Sociedad de la Información, esto facilita que ciertas malas conductas aún no sean sancionadas, como por ejemplo el abuso de dispositivos, la instalación no autorizada de cookies, o la intercepción de comunicaciones.

- El éxito de los casos depende en gran parte de las primeras acciones que son tomadas para responder a los incidentes informáticos, dado que el más mínimo error echará a perder los datos, imposibilitando el proceso forense para el investigador designado por la Fiscalía General del Estado.

Conclusiones

- La información normalmente no se presentará de forma evidente, dado que los individuos involucrados en actividades ilegales, intentarán eliminar u ocultar cualquier dato culposo. Es por esto que resulta muy importante analizar tanto el ordenador como los dispositivos encontrados, en búsqueda de archivos ocultos o eliminados.

- Para el análisis informático forense se cuenta con herramientas tanto de software libre como propietario, que permiten obtener y analizar evidencia en los diferentes escenarios que pueden presentarse en los diferentes casos. Estas agilitan la obtención y facilitan la interpretación de la evidencia independientemente del sistema operativo.

Recomendaciones

- Es necesario contar con profesionales capacitados para dar asistencia a ilícitos informáticos, ya que en muchas ocasiones la falta de preparación en muchas ocasiones echa a perder la evidencia que es determinante al momento de aclarar un caso o tomar una decisión penal.

- Se debe seguir una metodología adecuada para el tratamiento de delitos informáticos, dada la susceptibilidad de los datos, ya que la evidencia es de suma importancia en el momento de juzgar los ilícitos en los cuales se hayan usado medios electrónicos o digitales. Es por esto que es indispensable mantener la cadena de custodia y contar con herramientas adecuadas y debidamente certificadas en el momento de recolectar evidencia manteniendo su fiabilidad.

Recomendaciones

- Es recomendable contar con los utilitarios necesarios al momento de acudir al lugar de los hechos de un incidente tomando en cuenta que los profesionales deben estar familiarizados con las herramientas a utilizar y verificar la validez de los resultados obtenidos.

- Debemos tener en cuenta que en el proceso de recaudación y transporte de la evidencia esta puede sufrir alteraciones físicas y lógicas, para lo cual se debe tomar todas las medidas precautelares para evitar echar a perder la evidencia.

Recomendaciones

- Es importante considerar que cualquier actividad que se realice en el computador en caliente, puede generar un proceso que altere la integridad de la evidencia, por lo cual es recomendable el uso de software portable, liveCds que interactúen lo menos posible con la información y procesos que en el instante estén corriendo y que minimiza el impacto sobre la ejecución de módulos, ddls, etc.