

Seguridad y Cómputo forense

Manuel Aguilar Cornejo

Area de Computación y Sistemas
Universidad Autónoma Metropolitana Iztapalapa

Indice



- Introducción
- Tipos de ataques a los equipos de cómputo
- Prevención de ataques:
 - instalación de antivirus,
 - firewalls,
 - medidas preventivas, etc.
- Sistemas de detección de intrusos
- Herramientas para la detección de intrusos
- Cómputo Forense
- Conclusiones

Introducción

- **Objetivo:** dar un panorama sobre la importancia de la información, los cuidados necesarios, y algunos ejemplos de técnicas y herramientas para su protección, así como un panorama general de lo que es el cómputo forense.

Introducción

- **Importancia**

- **Tecnología => Valor de la información**
- **Conectividad => Riesgos**
- **Evidencias => Registros, bitácoras -
Nuevas técnicas**

Introducción

Tenemos diferentes tipos de amenazas a la seguridad de la información debido a:


- Fallas humanas
- Ataques malintencionados
- Catastrofes naturales

Para todos los casos una solución factible sería respaldar la información en algún lugar diferente y seguro.

Introducción

- Debemos de garantizar no solamente la seguridad de la información sino su confidencialidad y mal uso.
- Para ello debemos de evitar los accesos no autorizados al sistema, así como los ataques al mismo.

Índice

- Introducción
-  **Tipos de ataques a los equipos de cómputo**
- Prevención de ataques:
 - instalación de antivirus,
 - firewalls,
 - medidas preventivas, etc.
- Sistemas de detección de intrusos
- Herramientas para la detección de intrusos
- Cómputo forense
- Conclusiones

Tipos de ataques

- **sniffing:** Consiste en observar todos los paquetes que pasan por la red
- **Ataques de contraseña:**
 - Usando diccionario
 - Por fuerza bruta
- **DS:** Denegacion de servicio. consiste en mandar mas informacion de la que pueda ser atendida.

Tipos de ataques

- **Ingeniería social:** consiste en obtener información del sistema mediante engaños.
- **Phishing:** fraude electrónico, ejemplo mails de banamex.
- **Escaneo de puertos:** búsqueda de algún puerto para acceder los servicios del sistema.

Tipos de ataques


- **Código malicioso (virus)**

- **Bombas lógicas:** código que se activa bajo la ocurrencia de un evento
- **Troyanos:** programa que simula ejecutar una función mientras que ejecuta otra.
- **Cookies:** archivos de texto con información acerca de la navegación efectuada por el usuario en internet e información confidencial del usuario
- **Keyloggers:** programas que registran todas las teclas pulsadas
- **Spyware:** aplicaciones que recogen y envían información sobre el usuario de internet.

Tipos de ataques

- **Puertas traseras:** consiste en buscar huecos de seguridad en los sistemas operativos
- **Trashing:** consiste en buscar información importante en la “basura”

Índice

- Introducción
- Tipos de ataques a los equipos de cómputo
-  **Prevención de ataques:**
 - instalación de antivirus,
 - firewalls,
 - SDI, etc.
- Sistemas de detección de intrusos
- Herramientas para la detección de intrusos
- Cómputo forense
- Conclusiones

Prevención de ataques

Los métodos para reducir los riesgos debido a virus pueden ser activos o pasivos:

- Activos:
 - Antivirus
- Pasivos:
 - Copias de seguridad
 - Estudiar mas sobre el software de nuestra computadora
 - Desconfiar

Prevención de ataques

Antiespías gratuitos:

- Spybot – Search & Destroy
- Ad-Aware
- SpywareBlaster

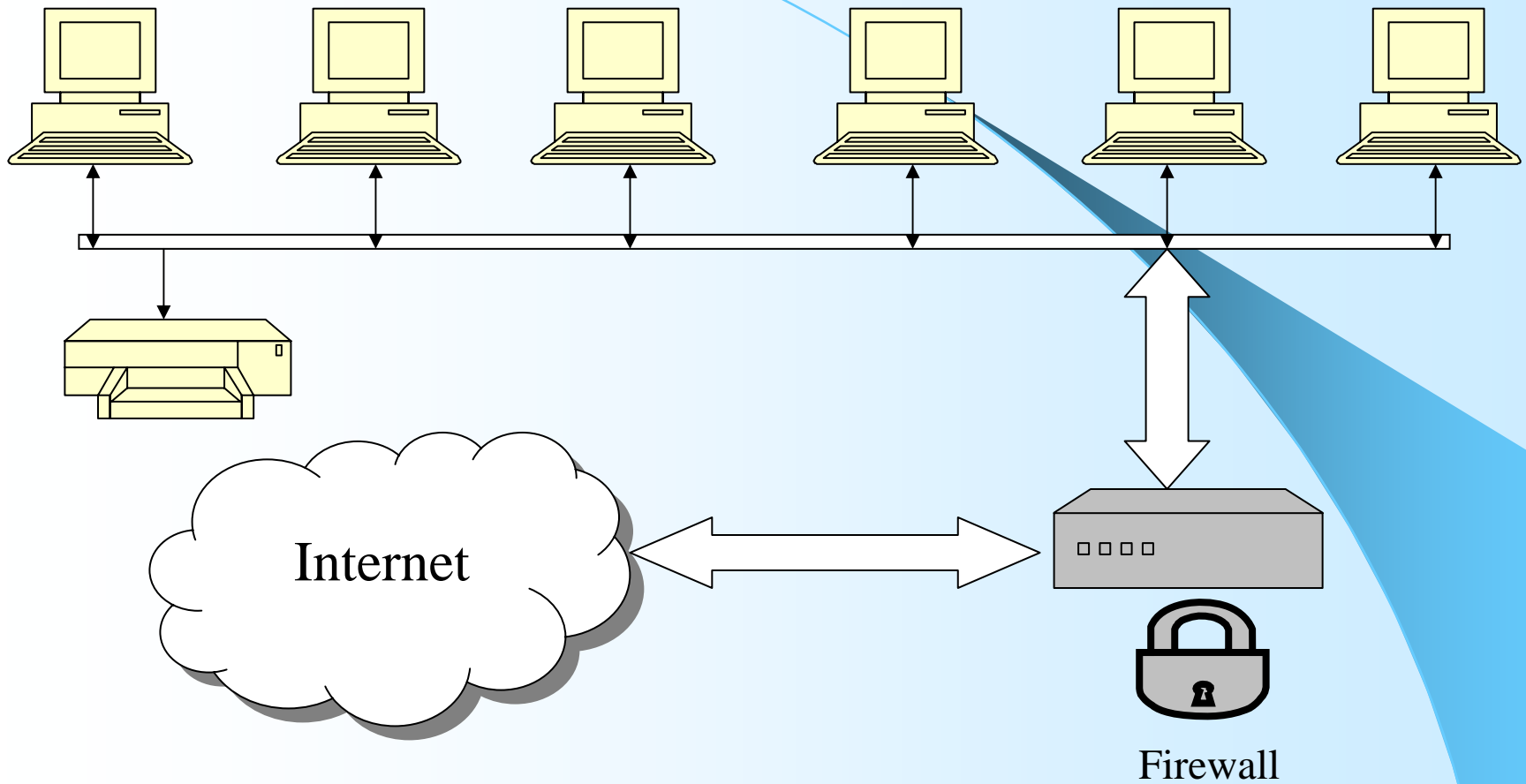
Se recomienda no usar un solo programa antiespía sino una combinación de varios

Prevención de ataques

- Por otro lado, también existen muchos programas que se presentan como "antiespías" y en realidad no lo son.
- Algunos de ellos hacen lo contrario de lo que predicán, instalan espías (ejemplos conocidos y comprobados, ver <http://www.vsantivirus.com/lista-nospyware.htm>)

Prevención de ataques


- Otro sistema de prevención de ataques efectivo son los firewalls (cortafuegos), que protege de accesos no autorizados hacia la red interna (pero no protege contra ataques desde dentro de la red).



Prevención de ataques

- Sistemas de Detección de Intrusos (SDI)
- Una intrusión es definida como un conjunto de acciones que intentan comprometer (poner en peligro) la integridad, la confidencialidad o la disponibilidad de un sistema informático.

Indice

- Introducción
- Tipos de ataques a los equipos de cómputo
- Prevención de ataques:
 - instalación de antivirus,
 - firewalls,
 - medidas preventivas, etc.
-  **Sistemas de detección de intrusos**
- Herramientas para la detección de intrusos
- Cómputo forense
- Conclusiones

SDI

Normalmente los intrusos (crakers) expertos siguen tres pasos para llevar un ataque:

- Preparan el ataque (ej. Búsqueda de puertos)
- Lanzan el ataque
- Borra todo rastro de su acceso

Nuestro objetivo es detectar y eliminar la intrusión lo antes posible para limitar el daño

SDI

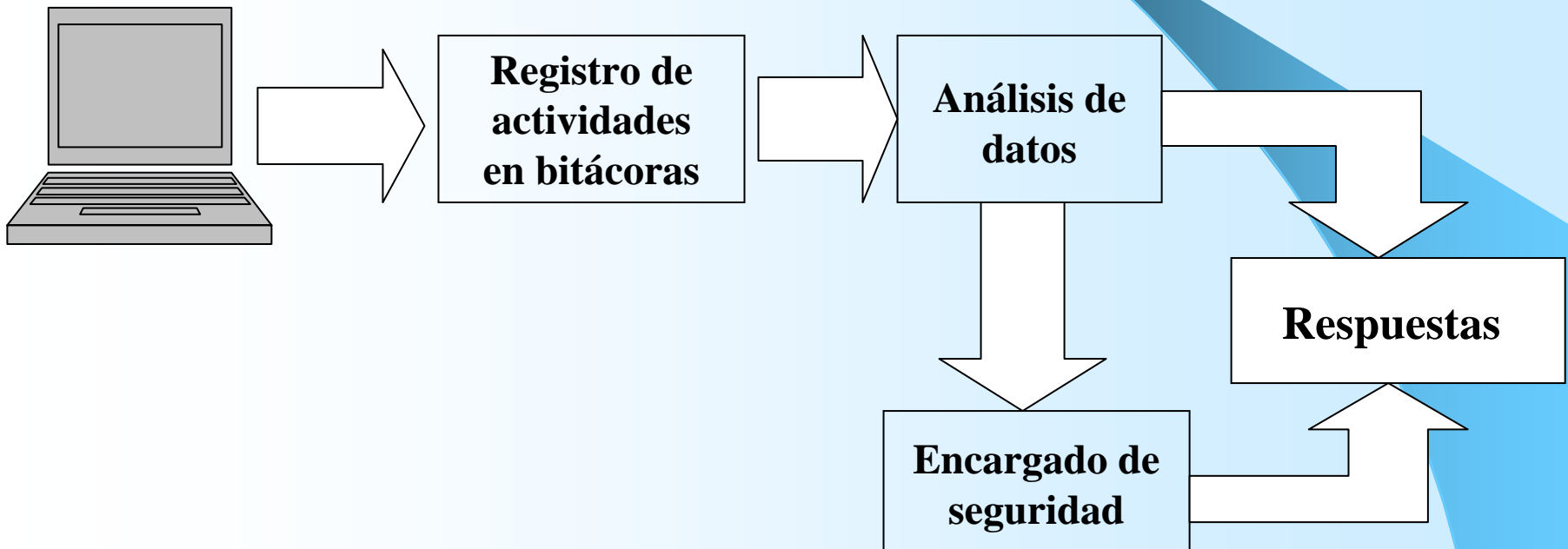
Existen dos tipos de sistemas de detección de intrusos:

- Los basados en host, SDIh
- Los basados en red, SDIr
- Actualmente se proponen una combinación de ambos, SDIh&r

SDIh

- Su fuente de información son las bitácoras del sistema prestando especial énfasis a los registros relativos a los demonios de red, como un servidor web o el propio demonio *inetd*.
- Problema: pocos administradores revisan esas bitácoras.

Esquema de un SDIh



SDIh

Entre las bitácoras del sistema, tenemos los archivos:

- *secure*: registra los accesos logrados y fallidos.
- *maillog*: supervisa el servicio de e-mail
- *message*: almacena mensajes de baja y media prioridad. Contiene información sobre el arranque del sistema, así como de las sesiones abiertas
- *acces_log*: almacena los accesos a la pag. del servidor
- *error_log*: presenta informes de todos los errores que provienen del servidor web.
- Etc.

SDIh

Ejemplo:

```
Oct 31 00:42:19 alpha sshd[12433]: Failed password for root  
from 67.33.168.95 port 54455 ssh2
```

Indica que un usuario con IP 67.33.168.95 intentó conectarse como root por el puerto 54455 en la fecha señalada, pero con contraseña incorrecta

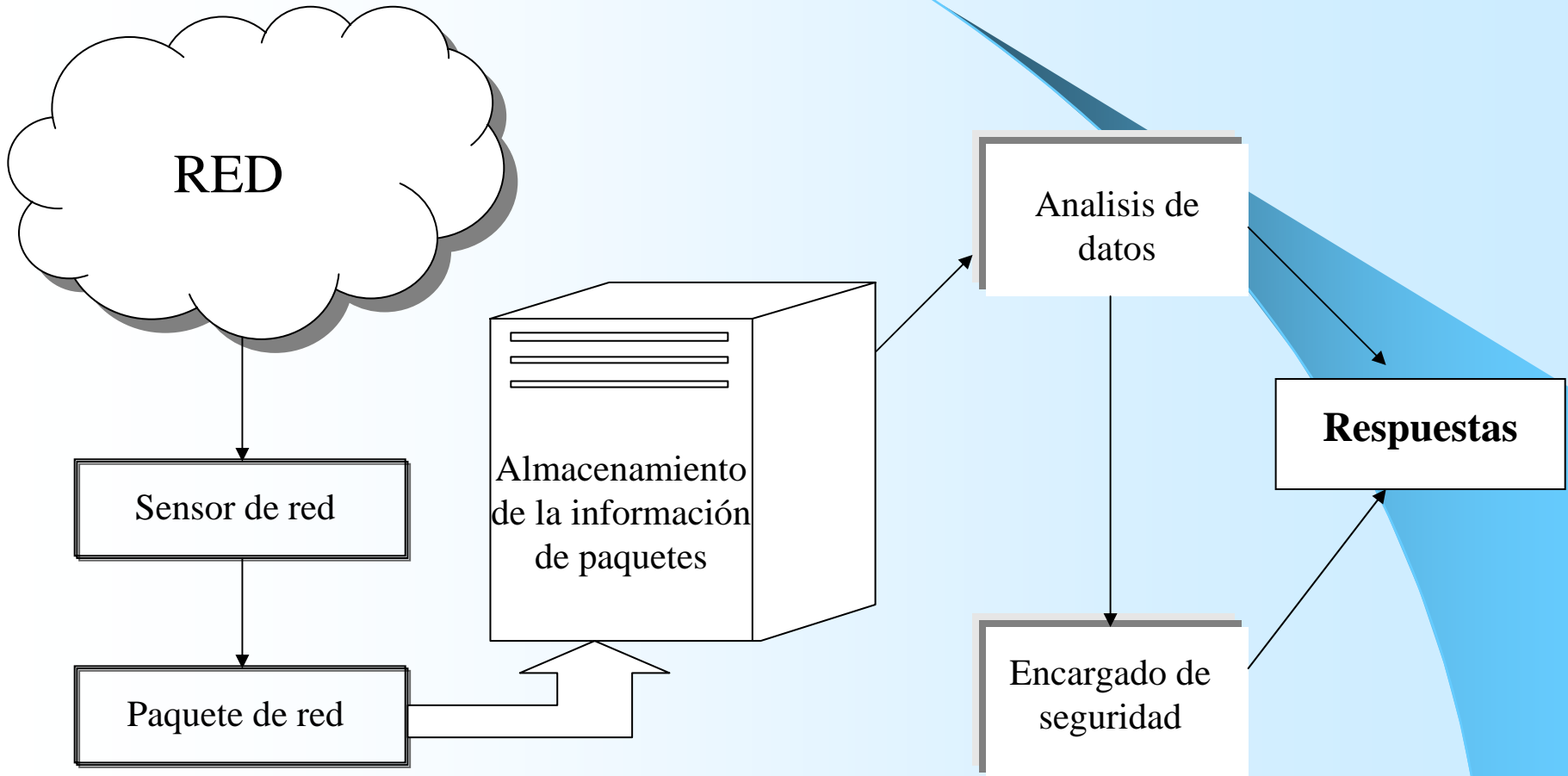
Ejemplos de SDIh

- OSSEC (<http://ossec.net>) de dominio público, actúa en tiempo real, puede responder de manera activa a los ataques y es compatible con Linux, MacOS, Solaris y Windows.
- Tripwire, SDI comercial realiza análisis periódico con respuestas pasivas.

SDIr

- Son capaces de detectar ataques contra una red local.
- Detectan las anomalías en la red cuando el ataque está en curso.
- La prioridad de estos sistemas es detectar el ataque lo antes posible para que cause el menor daño posible.

Organización de un SDIr



SDIr

- Snort (<http://www.snort.org>) es un sniffer de paquetes (de dominio público).
- Es un detector de intrusos basados en anomalías del funcionamiento de la red
- Utiliza un lenguaje basado en reglas (definidas por el administrador, creadas automáticamente por el sistema, o una combinación de ambas) para detectar intrusos.

SDIr

- La característica más apreciada de Snort es su subsistema flexible de firmas de ataques que está actualizandose constantemente a través de internet.
- Los usuarios de Snort pueden enviar sus firmas de ataques para beneficiar a toda la comunidad.

SDIh&r

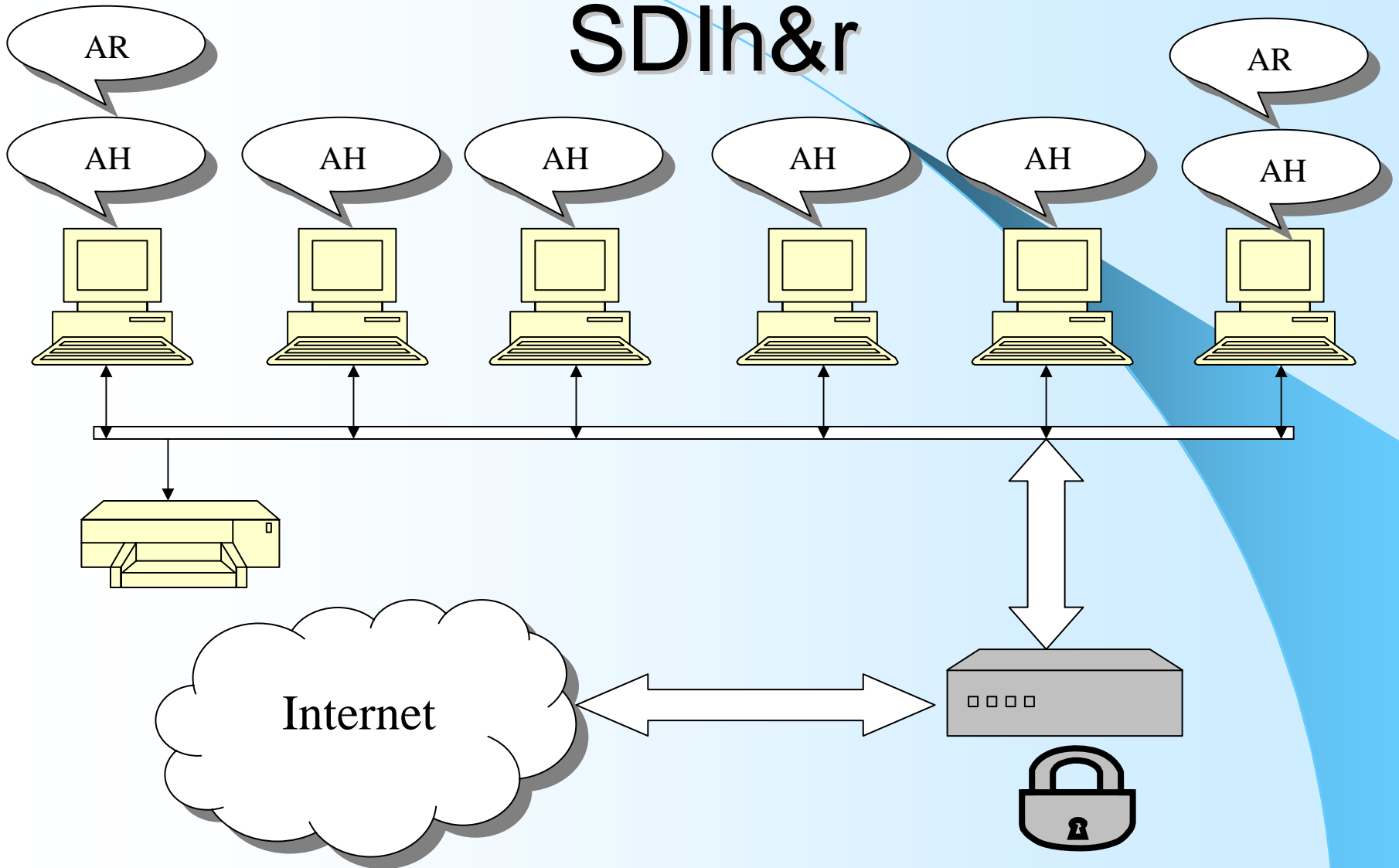
- Los SDIh y los SDIr se pueden complementar e implementar simultáneamente para obtener un alto nivel de seguridad.
- Un SDIh&r está constituido por sensores en cada huésped y un sensor en cada segmento de red.

SDIh&r


Sus principales componentes son:

- Agentes huesped
- Agentes de red
- Transeptores (comunicación)
- Consola de eventos (interfaz con el operador)

SDIh&r



Índice

- Introducción
- Tipos de ataques a los equipos de cómputo
- Prevención de ataques:
 - instalación de antivirus,
 - firewalls,
 - medidas preventivas, etc.
- Sistemas de detección de intrusos
-  **Herramientas para la detección de intrusos**
- Cómputo Forense
- Conclusiones

Ejemplos de herramientas de SDI

SDI	Sensor	Ejecución	Respuesta	Arquitectura	Distribucion
Tripware	Huésped	Periódico	Pasivas	Centralizado	Comercial
OSSEC	Huésped	T. Real	Activas	Distribuido	Libre
RealSecure	Red	T. Real	Activas	Distribuido	Comercial
Snort	Red	T. Real	Activas	Centralizado	Libre
Prelude	Híbrido	T. Real	Activas	Distribuido	Libre
DIDS	Híbrido	T. Real	Activas	Centralizado	No disp.

Índice

- Introducción
- Tipos de ataques a los equipos de cómputo
- Prevención de ataques:
 - instalación de antivirus,
 - firewalls,
 - medidas preventivas, etc.
- Sistemas de detección de intrusos
- Herramientas para la detección de intrusos
- **Cómputo Forense**
- Conclusiones



Cómputo Forense

- Evidencia digital:
 - Es un tipo de evidencia física. Esta construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.(Casey 2000, pág.4)
- Computación forense
 - Es la aplicación legal de métodos, protocolos y técnicas para obtener, analizar y preservar evidencia digital relevante a una situación en investigación. (Kovacich 2000, pag.243)

Cómputo Forense

- Provee principios y técnicas que facilitan la investigación de ofensas catalogadas como criminales.
 - Implica la aplicación de la ciencia al campo legal
 - Cualquier principio científico o técnica puede ser aplicada para:
 - Identificar,
 - Recuperar,
 - Reconstruir y
 - Analizar evidencia durante un investigación de un delito.
 - Aplicando métodos científicos los especialistas forenses pueden analizar la evidencia para:
 - Crear hipótesis, efectuar pruebas para verificar dichas hipótesis, generando posibilidades claras sobre lo que ocurrió.

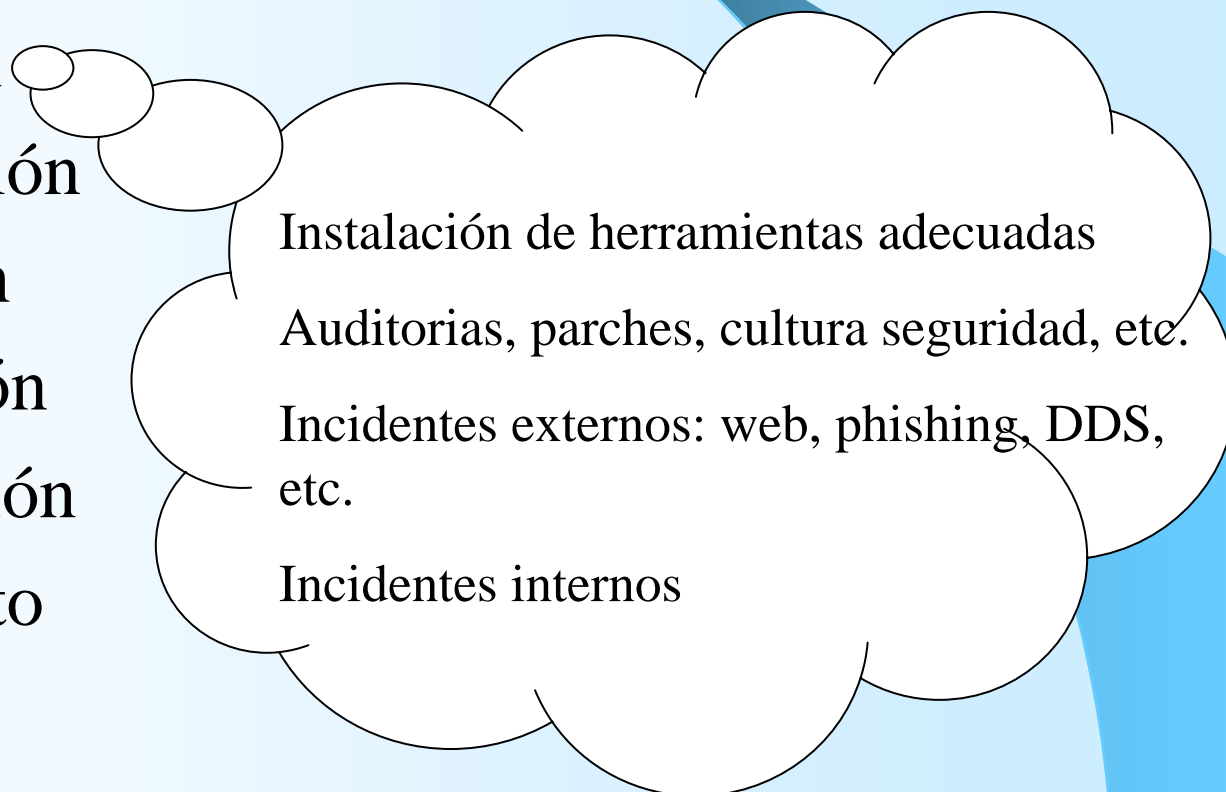
Atención a un incidente y análisis forense

- Atención a un incidente:
 - Prevención
 - Identificación
 - Contención
 - Erradicación
 - Recuperación
 - Seguimiento

Atención a un incidente y análisis forense

- Atención a un incidente:

- Prevención
- Identificación
- Contención
- Erradicación
- Recuperación
- Seguimiento



Instalación de herramientas adecuadas
Auditorias, parches, cultura seguridad, etc.
Incidentes externos: web, phishing, DDS,
etc.
Incidentes internos

Atención a un incidente y análisis forense

● Atención a un incidente:

- Prevención
- Identificación
- Contención
- Erradicación
- Recuperación
- Seguimiento

- Verificar que no sea falsa alarma
- Buena documentación
- Iniciar una cadena de custodia
- No hay receta: hay que utilizar bitacoras, firewall, IDS, etc. y correlacionar la información
- Cualquier comando modifica la evidencia, el no hacer nada también la modifica.

Atención a un incidente y análisis forense

- Atención a un incidente:

- Prevención
- Identificación
- Contención
- Erradicación
- Recuperación
- Seguimiento

Evitar daños colaterales

- Limitar el control de acceso
- Cambiar contraseñas
- Deshabilitar cuentas, etc.

Analizar riesgos de cada acción

- Intruso observando
- Evidencia volátil

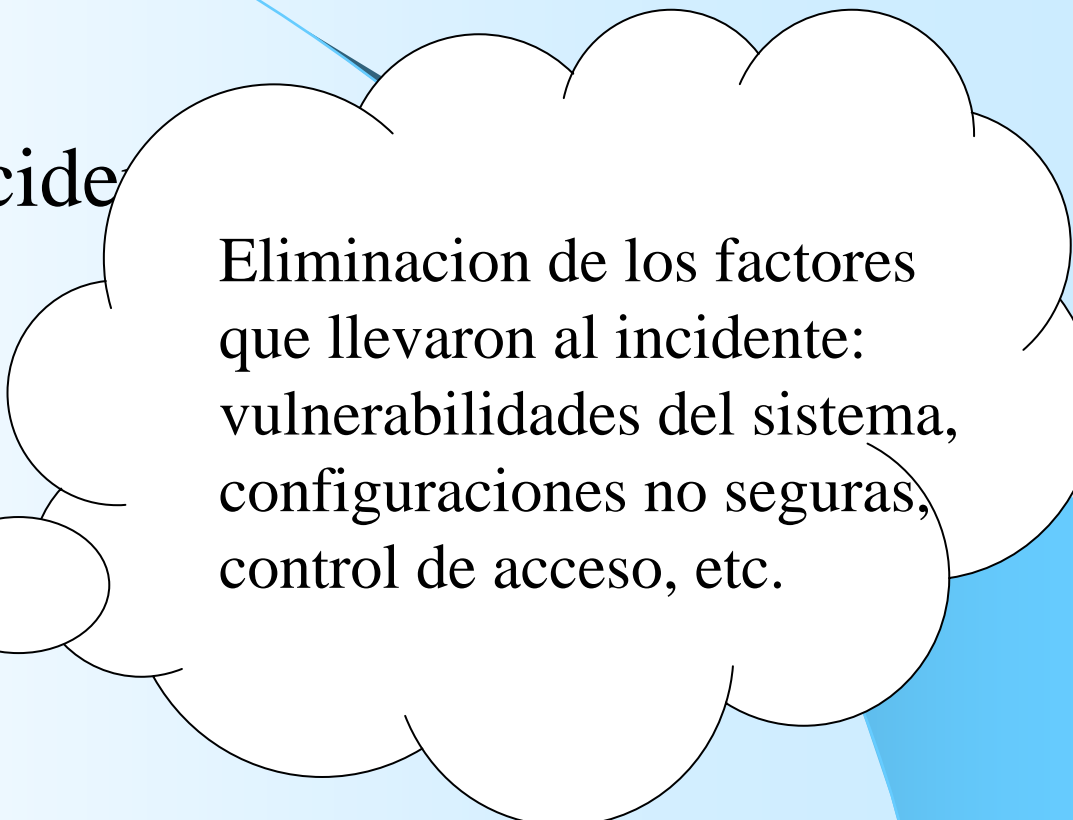
Atención a un incidente y análisis forense

- Atención a un incidente
 - Prevención
 - Identificación
 - Contención
 - Erradicación
 - Recuperación
 - Seguimiento
- Evitar al máximo la contaminación de la evidencia
- Apagar el sistema?
- Desconectar el sistema de la red?
- Acciones a evitar:
- Escribir en medios originales,
 - Matar algún proceso
 - Modificar el sistema antes de obtener evidencia (apagar, actualizar, etc.)

Atención a un incidente y análisis forense

- Atención a un incidente

- Prevención
- Identificación
- Contención
- Erradicación
- Recuperación
- Seguimiento

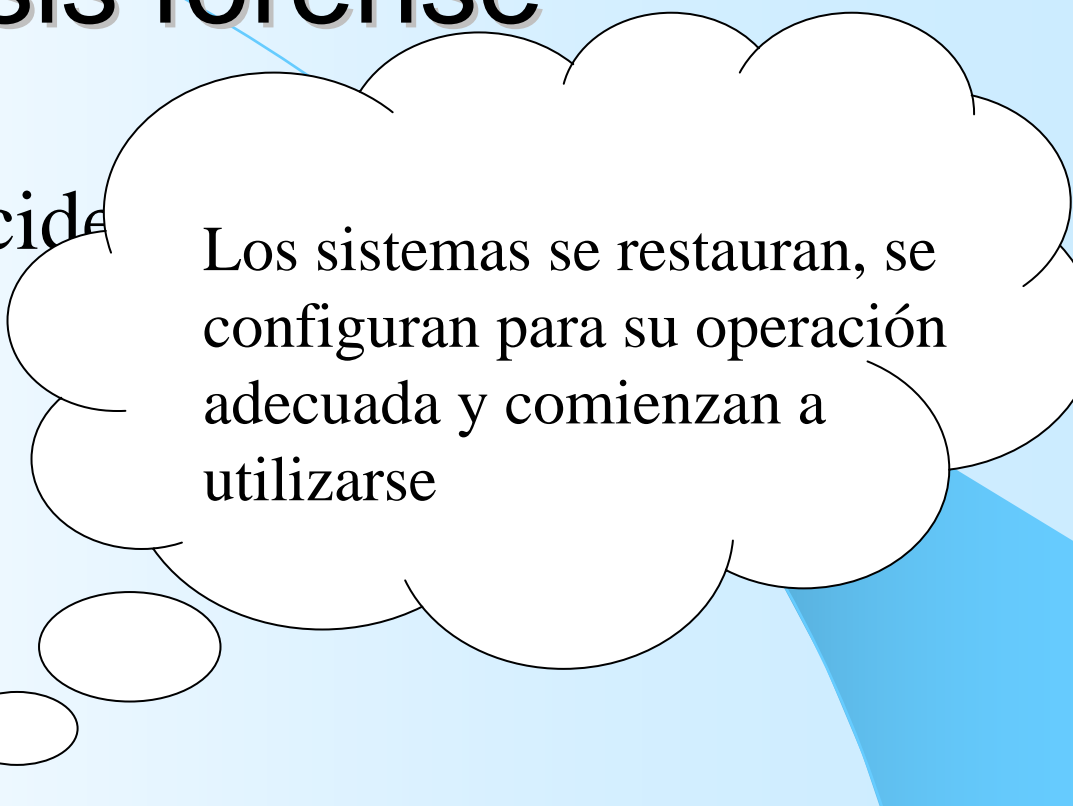


Eliminación de los factores que llevaron al incidente: vulnerabilidades del sistema, configuraciones no seguras, control de acceso, etc.

Atención a un incidente y análisis forense

- Atención a un incidente

- Prevención
- Identificación
- Contención
- Erradicación
- Recuperación
- Seguimiento

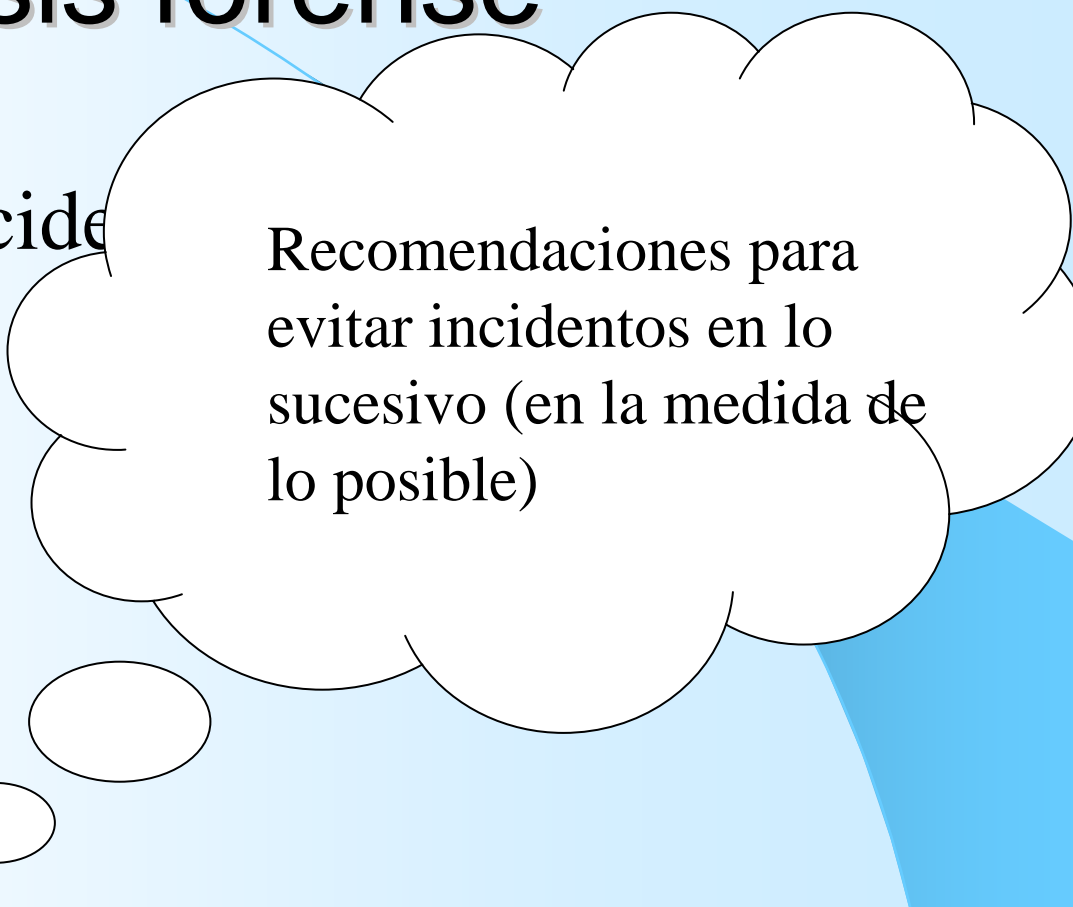


Los sistemas se restauran, se configuran para su operación adecuada y comienzan a utilizarse

Atención a un incidente y análisis forense

- Atención a un incidente

- Prevención
- Identificación
- Contención
- Erradicación
- Recuperación
- Seguimiento



Recomendaciones para evitar incidentos en lo sucesivo (en la medida de lo posible)

Herramientas

Deben de cubrir los siguientes aspectos:

- Información sobre procesos
- Información sobre cuentas de usuarios
- Información para la revisión de bitácoras e historiales
- Búsqueda de malware
- Información sobre los datos alojados en memoria volátil
- Búsqueda de archivos
- Creación de imágenes

Herramientas

Las herramientas para el análisis forense se enfocan a las fases de preservación y búsqueda, ejemplos de ellas son:

- ❑ Encase producido por *Guidance Software*.
- ❑ Forensic Toolkit producido por *Acces Data Corp* (*FTK™*) FTK, tiene indexado total en texto, búsquedas avanzadas, recuperación de archivos eliminados, búsqueda detallada de datos, análisis de e-mail, etc. disponible en:

<http://www.accessdata.com/common/pagedetail.aspx?PageCode=downloads>

(incluye manuales)

Herramientas

- ❑ ProDiscovery facilita la localización de datos sobre una computadora mientras protege la evidencia. Se puede descargar un demo y manuales de:

<http://www.techpathways.com/ProDiscoverDFT.htm>

- ❑ SMART creada por *ASData*, versión de evaluación

<http://www.asrdata2.com/>

- ❑ The Coroner's Toolkit (TCT): es una colección de programas escritos por Dan Farmer and Wietse Venema para análisis post-mortem de sistemas UNIX.

<http://www.porcupine.org/forensics/tct.html>

Ejemplos de sus uso se encuentran en su libro

Herramientas

- ❑ The Sleuth Kit/Autopsy Browser son herramientas open source (disponibles de manera gratuita) de investigación digital que corren sobre sistemas unix (tal como: [Linux](#), [OS X](#), [FreeBSD](#), [OpenBSD](#), and [Solaris](#)). Pueden analizar los sistemas de archivos NTFS, FAT, Ext2, Ext3, UFS1 y UFS2 y varios tipos de volúmenes de sistemas, disponible en:

<http://www.sleuthkit.org/sleuthkit/download.php>

<http://www.sleuthkit.org/autopsy/download.php>

Documentación

- Internet
- Libros
- Entre las revistas especializadas se encuentran [International Journal of Digital Evidence](#), que acaba de liberar su edición Winter 2004; y [Digital Investigation](#), que ofrece de forma gratuita su primer número.
- Dentro de las distribuciones linux específicas para informática forense destacan [F.I.R.E. Linux](#) (Forensic and Incident Response Environment) y [Honeynet CD-ROM](#).

Índice

- Introducción
- Tipos de ataques a los equipos de cómputo
- Prevención de ataques:
 - instalación de antivirus,
 - firewalls,
 - medidas preventivas, etc.
- Sistemas de detección de intrusos
- Herramientas para la detección de intrusos
- Cómputo Forense
- **Conclusiones**



Conclusiones

- Es más que indispensable la prevención
- Es necesario el conocimiento de qué nos vamos a prevenir
- Es necesario el conocimiento de herramientas para la prevención de ataques: antivirus, anti-spyware, firewalls, etc.
- Se hace necesaria la instalación de herramientas como los SDI

Conclusiones

- Faltan profesionistas con conocimiento especializado en el área.
- Existen organismos internacionales que certifican los conocimientos en esta área de dominio.
- Es necesario conocer herramientas existentes para el cómputo forense.

Muchas gracias !!!