Ingeniería de Sistemas

Gestión de Incidentes

Seguridad de Sistemas de TI

2022-1

UNIVERSIDAD DE LIMA

Agenda

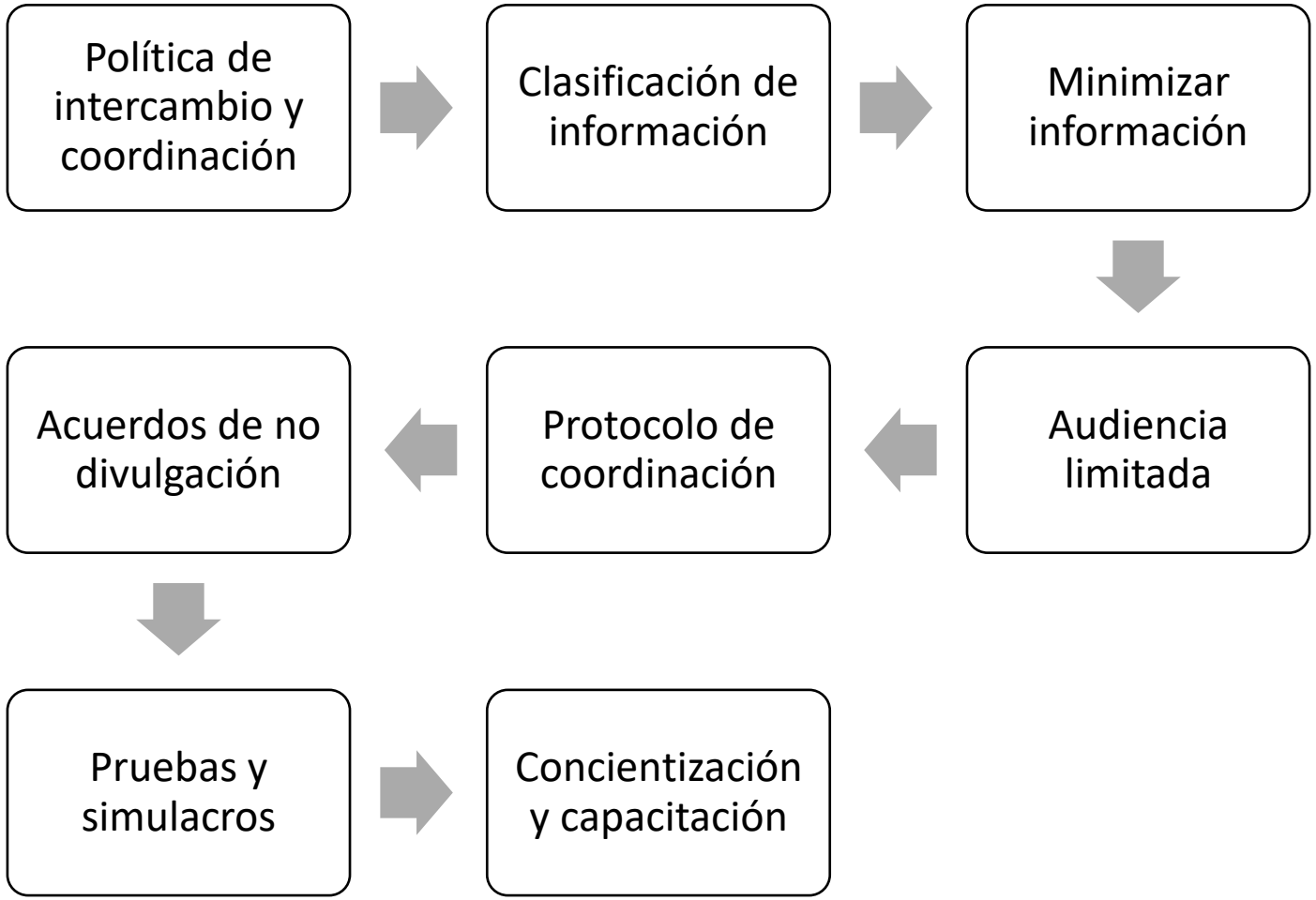
- Colaboración y coordinación de información de ciberseguridad
- Proceso de respuesta a incidentes
- Investigación forense digital
- Recuperación de desastres y planes de continuidad
- Gestión de crisis

Evento vs Incidente

- Evento: ***"cualquier ocurrencia observable en un sistema o red"*** *(NIST)*
- Incidente: "***una violación o una amenaza inminente de violación de las políticas de seguridad informática, las políticas de uso aceptable o las prácticas de seguridad estándar."*** (*NIST*)
- Incidente: "El intento o éxito en el acceso no autorizado, uso, revelación, modificación o pérdida de información o la interferencia con las operaciones de red o de sistemas".

UNIVERSIDAD DE LIMA

Clausula 13 ISO/IEC 27032



Se identifican los IRO e IPOS

UNIVERSIDAD DE LIMA

Incidentes de ciberseguridad

- Un incidente de ciberseguridad es un evento adverso que afecta negativamente a la confidencialidad, integridad y disponibilidad de los datos.
- Los incidentes de ciberseguridad pueden ser involuntarios.
  - Ej. Olvidar activar una lista de acceso en un router
- Los incidentes de ciberseguridad pueden ser intencionales
  - Ej: Malware, ataques de denegación de servicio (DoS), fallos del sistema, ingeniería social y la pérdida o robo dispositivos móviles.

UNIVERSIDAD DE LIMA

Plazos de atención

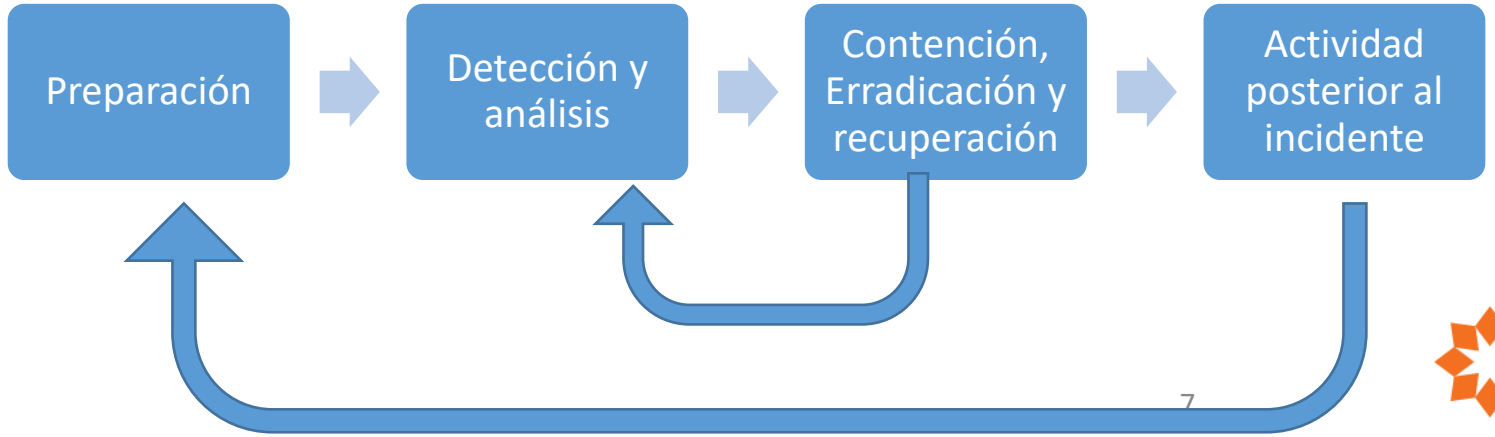
Categoría	Nombre	Descripción	Plazos de Presentación de Informes
CAT 1	Acceso no autorizado	Un individuo obtiene acceso lógico o físico sin permiso a una red, sistemas, aplicaciones, datos u otro recurso	Dentro de 1 hora del descubrimiento/detección
CAT 2	Denegación del servicio (DoS)	Un ataque que con éxito impide o perjudica la funcionalidad normal autorizada de redes, sistemas o aplicaciones por agotamiento de recursos	Dentro de dos horas del descubrimiento o detección si el ataque exitoso continúa
CAT 3	Código malicioso	La instalación exitosa de software malicioso (por ejemplo, virus , gusano, troyanos u otra entidad maliciosa basada en código) que infecta un sistema operativo o aplicación	Diariamente; dentro de una hora del descubrimiento o detección si se extiende
CAT 4	Uso impropio	Una persona viola las políticas aceptables de uso de los ordenadores	Semanalmente
CAT 5	Escáneres/ Sondas/Intentos de acceso	Cualquier actividad que pretende acceder o identificar un ordenador, puertos abiertos , protocolos , servicios o cualquier combinación	Mensualmente
CAT 6	Investigación	Incidentes sin confirmar que son actividades potencialmente maliciosas o anómalas	N/A

Fuente: ISACA

Respuesta a incidentes

1. **Preparación** para establecer los roles, responsabilidades y planes de cómo será manejado un incidente.
2. Capacidades de **detección y análisis** para identificar incidentes tan pronto como sea posible y evaluar eficazmente la naturaleza del incidente
3. Capacidad de **investigación** si se requiere la identificación de un adversario.
4. Procedimientos de **mitigación y recuperación** para contener el incidente, reducir las pérdidas y volver las operaciones a la normalidad
5. **Análisis posterior al incidente** para determinar las acciones correctivas para prevenir incidentes similares en el futuro

Elementos de la respuesta a incidentes



UNIVERSIDAD DE LIMA

Plan de respuesta de incidentes

- **Preparación**:
  - Establecer un enfoque para manejar incidentes
  - Establecer la política y los banners de advertencia en los sistemas de información para disuadir a intrusos y permitir la recopilación de información
  - Establecer un plan de comunicación para las partes interesadas
  - Desarrollar criterios sobre cuándo reportar un incidente a las autoridades
  - Desarrollar un proceso para activar el equipo de gestión de incidentes
  - Establecer un lugar seguro para ejecutar el plan de respuesta a incidentes
  - Asegurar que el equipo necesario está disponible
- **Identificación**: Las actividades en esta fase incluyen:
  - Asignar la propiedad de un incidente o potencial incidente a un gestor de incidentes.
  - Verificar que los informes o eventos se califican como un incidente
  - Establecer la cadena de custodia durante la identificación al manipular evidencias potenciales
  - Determinar la gravedad de un incidente y escalarlo según sea necesario

Plan de respuesta a incidentes

- **Contención**: El equipo llevará a cabo una evaluación detallada y se pondrá en contacto con el propietario de la red o el gerente de negocio de los sistemas/ activos de información afectados para coordinar nuevas acciones. La medida adoptada en esta fase es la de limitar la exposición. Las actividades en esta fase incluyen:
  - Activación del equipo de gestión/respuesta de incidentes para contener el incidente
  - Notificación a las partes interesadas pertinentes afectadas por el incidente
  - Acordar las medidas adoptadas que puedan afectar a la disponibilidad de un servicio o el riesgo del proceso de contención
  - Conseguir la involucración del representante de TI y los miembros del equipo virtual relevantes para implementar los procedimientos de contención
  - Obtener y conservar evidencias
  - Documentar y realizar copias de seguridad de las acciones desde esta fase en adelante
  - Controlar y gestionar la comunicación al público por el equipo de relaciones públicas
- **Erradicación**: Cuando se han desplegado medidas de contención, es el momento de determinar la causa raíz del incidente y erradicarla. La erradicación puede hacerse de varias maneras: restaurar las copias de seguridad para lograr un estado limpio del sistema, eliminar la causa raíz, mejorar las defensas y realizar un análisis de vulnerabilidades para encontrar otros daños potenciales de la misma causa raíz. Las actividades en esta fase incluyen:
  - Determinar las señales y la causa de los incidentes
  - Localizar la versión más reciente de copias de seguridad o soluciones alternativas
  - Eliminar la causa raíz. En el caso de una infección de gusano o virus, se puede eliminar mediante el despliegue de parches adecuados y software antivirus actualizado.
  - Mejorar las defensas mediante la implementación de técnicas de protección
  - Realizar un análisis de vulnerabilidades para encontrar nuevas vulnerabilidades introducidas por la causa raíz

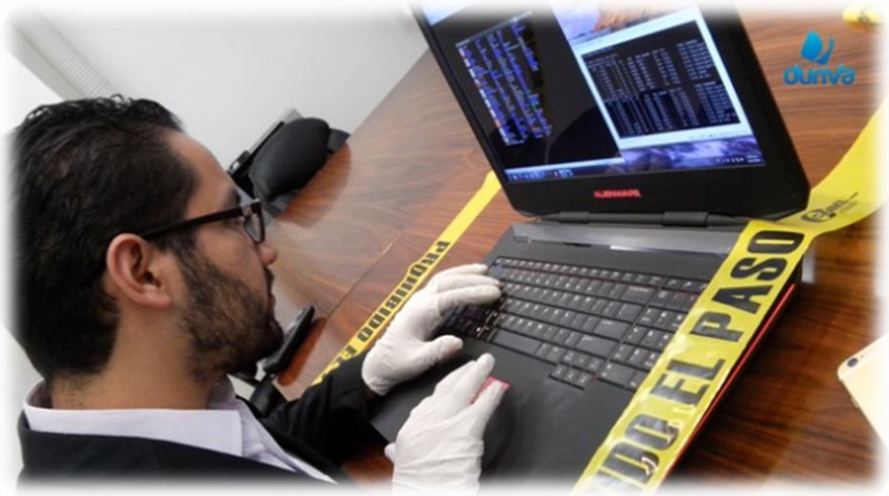
Plan de respuesta a incidentes

- **Recuperación**: Esta fase asegura que los sistemas o servicios afectados son restaurados a una condición especificada en los objetivos de prestación de servicios (SDO) o en el plan de continuidad del negocio (BCP). Las restricciones de tiempo se documentan en el RTO. Las actividades en esta fase incluyen:
  - Restaurar las operaciones a la normalidad
  - Validar que las medidas adoptadas en los sistemas restaurados tuvieron éxito
  - Conseguir la participación de los propietarios del sistema para probar el sistema
  - Facilitar que los propietarios del sistema declaren la operación normal
- **Lecciones aprendidas**: Al final del proceso de respuesta a incidentes, siempre se debe realizar un informe para compartir lo que ocurrió, qué medidas fueron tomadas y los resultados una vez que el plan fue ejecutado. Parte del informe debe contener lecciones aprendidas que proporcionen al IMT y a otras partes interesadas puntos de aprendizaje valiosos de lo que se podría haber hecho mejor. Estas lecciones deben desarrollarse en un plan para mejorar la capacidad de gestión de incidentes y la documentación del plan de respuesta a incidentes. Las actividades en esta fase incluyen:
  - Escribir el informe del incidente
  - Analizar los problemas encontrados durante los esfuerzos de respuesta a incidentes
  - Proponer mejoras en base a los problemas encontrados
  - Presentar el informe a las partes interesadas relevantes

¿Qué es informática forense?

- "Es una serie metodológica de técnicas y procedimientos para la recopilación de la evidencia digital de un equipo informático que pueden ser presentados en un formato coherente y significativo"

Dr. H.B. Wolfe



UNIVERSIDAD DE LIMA

Historia de la ciencia forense

- Francis Galton (1822-1911)
  - Hizo el primer estudio de huellas de dactilares.
- Leone Lattes (1887-1954)
  - Descubrió los grupos sanguíneos (A, B, AB, & O)
- **Calvin Goddard (1891-1955)**
  - **Permitió la comparación entre la bala y el arma de fuego para resolver diferentes casos.**
- Albert Osborn (1858-1946)
  - Desarrollo las características esenciales del examen de documentos.
- Hans Gross (1847-1915)
  - Uso el estudio científico para resolver investigaciones criminales
- **FBI (1932)**
  - **Se implemento un laboratorio para proporcionar servicio forense para todos los agentes de campo y otras autoridades de ley en todo USA**.

Historia de la ciencia forense

- 1984
  - Se creo el **Computer Analysis and Response Team (CART)** para dar soporte al FBI en la búsqueda de evidencia digital.
- 1993
  - Se lleva a cabo la Primera Conferencia Internacional sobre como tratar la evidencia digital.
- 1995
  - Se crea la International Organization on Computer Evidence (IOCE).
- 1998
  - Se crea el International Forensic Symposium (IFSS) para crear forum con los gerentes f
- ***2000***
  - ***El FBI crea el primer laboratorio de computo forense.***

UNIVERSIDAD DE LIMA

Tipos de investigaciones

- Las investigaciones forense digital son:
  - Corporativas: Investigaciones que no pasan al ámbito legal.
  - Judiciales: Investigaciones que se llevan a jucio.

Evidencia digital

- La evidencia digital es cualquier dato o información de valor probativo que es almacenado o transmitido en formato digital.
- Se puede mostrar en diversos tipos de información:
  - ***Creados por el usuario*:** bases de datos, audio, video, documentos, imágenes, marcadores web, hojas de calculo
  - ***Protegidos por el usuario*:** archivos comprimidos, archivos encriptados, protegidos por password, archivos ocultos y esteganografia.
  - ***Creados por el computador*:** archivos de backup, archivos de logs, archivos de cola de impresión, cookies, archivos ocultos, de sistema, historial y temporal.

UNIVERSIDAD DE LIMA

Evidencia digital

- Dispositivos donde encontrar información:
  - Disco duro
  - Tarjetas inteligentes
  - Escáner biométrico
  - Maquina contestadora
  - Cámara digital
  - Modem
  - Routers, Hub, Switches
  - Servidores
  - Impresoras
  - CDs, DVDs
  - Teléfonos inteligentes
  - Fotocopiadoras
  - GPS
  - USB

UNIVERSIDAD DE LIMA

Características de la evidencia digital

Creíble	• La evidencia debe ser clara y entendible para los jueces.
Confiable	• No debe haber duda sobre la autenticidad o veracidad de la evidencia.
Admisible	• La evidencia debe estar relacionada al hecho que se esta probando
Autentica	• La evidencia debe ser real y relacionada al incidente de una manera adecuada.
Completa	• La evidencia debe proporcionar pruebas de las acciones del atacante o su inocencia.

Tipos de datos digitales

- Dato Volátil
  - Se pierde al apagar computador.
  - Contiene el tiempo de sistema, el acceso del usuario, archivos abiertos, información de red, procesos de información, mapeo de puertos a procesos, procesos de memoria, contenido de portapapeles, información de servicios e historia de comandos.
- Dato No volátil
  - Se almacena y es persistente en el tiempo.
  - Contiene los archivos escondidos, slack space, swap file, archivos index.dat, particiones no usadas, particiones escondidas, configuraciones de registros y logs de eventos.

Caso Enron

https://archives.fbi.gov/archives/news/stories/2006/december/enron_121306

UNIVERSIDAD DE LIMA

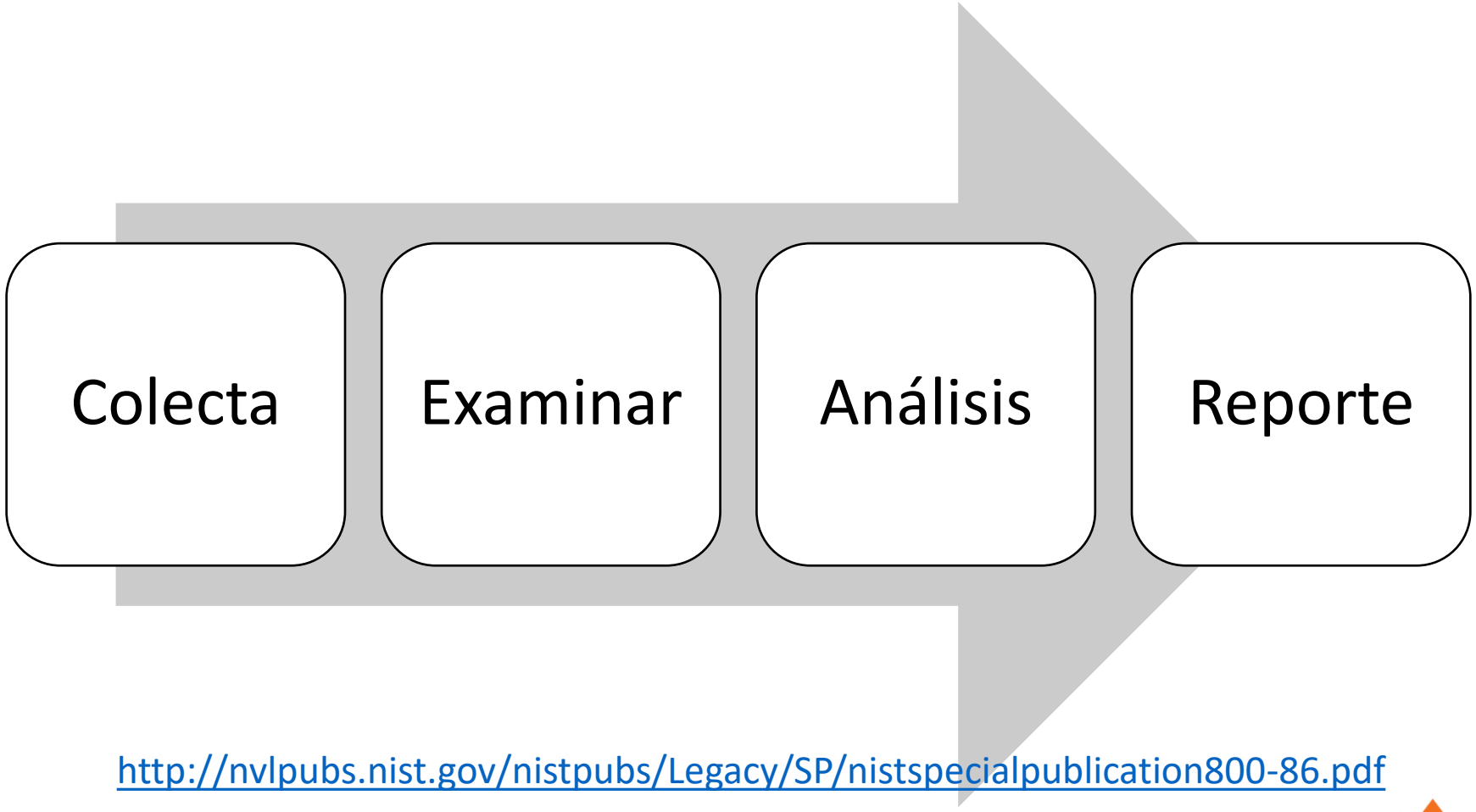
Giannotti y los USB

https://idl-reporteros.pe/exclusivo-el-video-cuando-se-detuvo-a-giannotti-y-se-hallo-los-usb/

UNIVERSIDAD DE LIMA

Proceso de Informática Forense

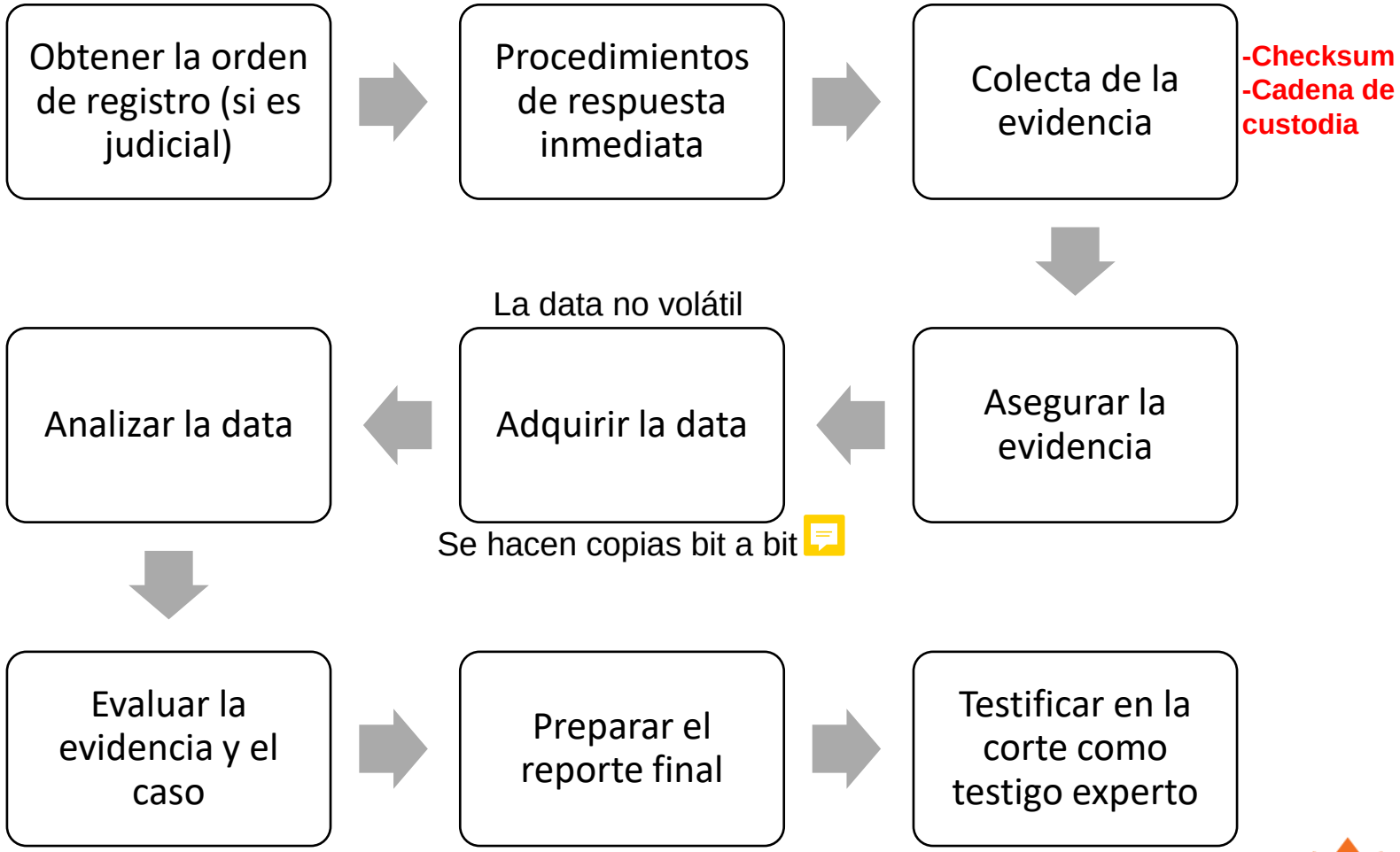
Metodología de la informática forense



http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

UNIVERSIDAD DE LIMA

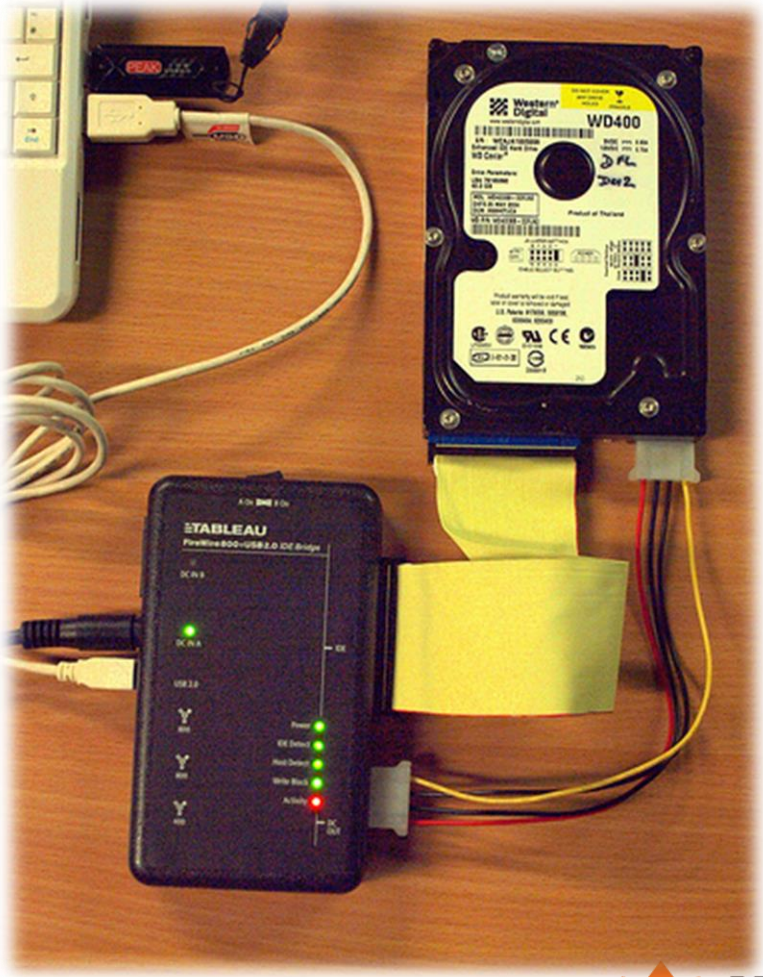
Metodología de informática forense digital



UNIVERSIDAD DE LIMA

Antes de iniciar la investigación

- Contar con herramientas necesarias para capturar datos volátiles y no volátiles
- Contar con estación de trabajado dedicada para análisis y recuperación de datos.
- Formar equipo de investigación.
- Asesoría de un abogado y autorización de la investigación.
- Revisar políticas y normativas de la organización.
- Evaluar el riesgo.



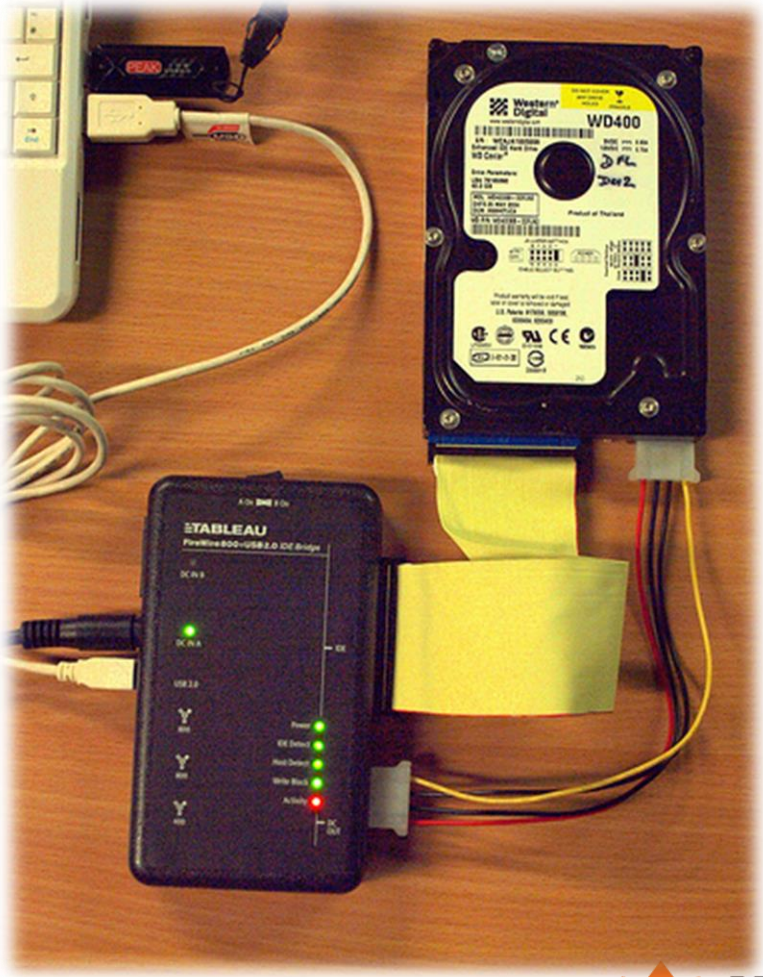
UNIVERSIDAD DE LIMA

Procedimientos de respuesta inmediata

- Fotografiar toda la evidencia.
- Restringir el acceso a la evidencia digital.
- Identificar el alcance de los dispositivos.
- Aislar dispositivos magnéticos.
- Identificar testigos
- Colecta de datos volátiles.

Colecta de la evidencia

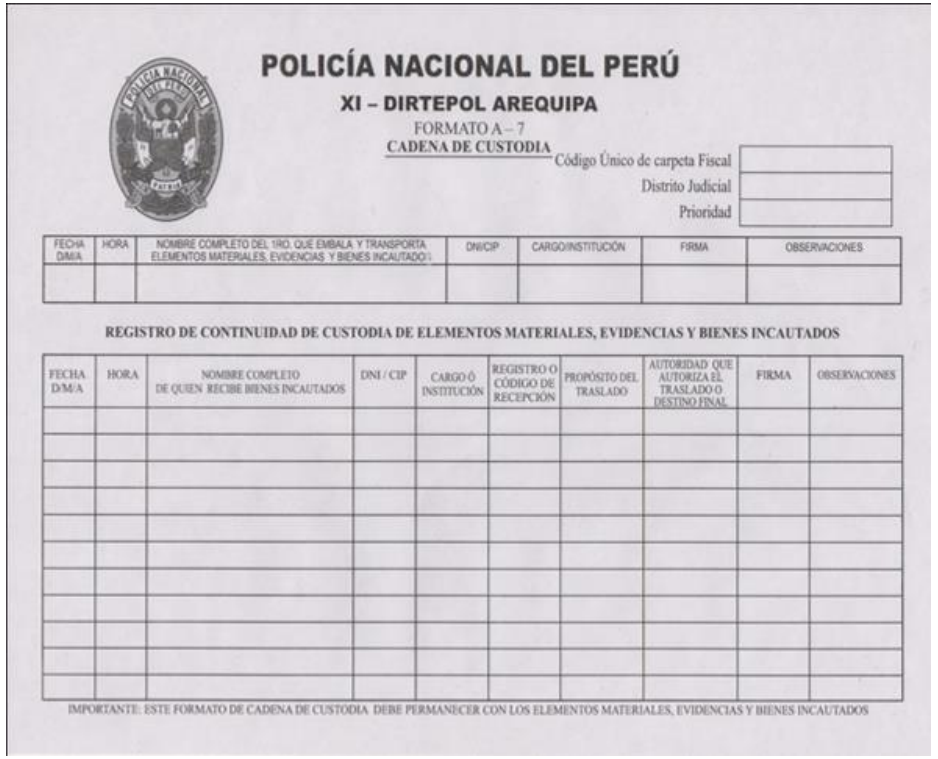
- Obtener función hash de integridad.
- Cadena de custodia
- Embargar evidencia



UNIVERSIDAD DE LIMA

La cadena de custodia

- Es un documento legal que muestra como la evidencia se ha transportado desde la ubicación original al laboratorio forense.
  - Funciones:
    - Abarca la colecta, manejo, almacenamiento, pruebas y disposición de la evidencia.
    - Es un control contra la manipulación de la evidencia o su sustitución.
    - Se documenta que pasos han sido realizados con la evidencia.



POLICÍA NACIONAL DEL PERÚ

XI – DIRTEPOL AREQUIPA

FORMATO A – 7

CADENA DE CUSTODIA

Código Único de carpeta Fiscal

Distrito Judicial

Prioridad

FECHA D/M/A	HORA	NOMBRE COMPLETO DEL 1RO. QUE EMBALA Y TRANSPORTA ELEMENTOS MATERIALES, EVIDENCIAS Y BIENES INCAUTADOS	DNI/CIP	CARGO/INSTITUCIÓN	FIRMA	OBSERVACIONES

REGISTRO DE CONTINUIDAD DE CUSTODIA DE ELEMENTOS MATERIALES, EVIDENCIAS Y BIENES INCAUTADOS

FECHA D/M/A	HORA	NOMBRE COMPLETO DE QUIEN RECIBE BIENES INCAUTADOS	DNI / CIP	CARGO Ó INSTITUCIÓN	REGISTRO O CÓDIGO DE RECEPCIÓN	PROPÓSITO DEL TRASLADO	AUTORIDAD QUE AUTORIZA EL TRASLADO O DESTINO FINAL	FIRMA	OBSERVACIONES

IMPORTANTE: ESTE FORMATO DE CADENA DE CUSTODIA DEBE PERMANECER CON LOS ELEMENTOS MATERIALES, EVIDENCIAS Y BIENES INCAUTADOS

Asegurando la evidencia

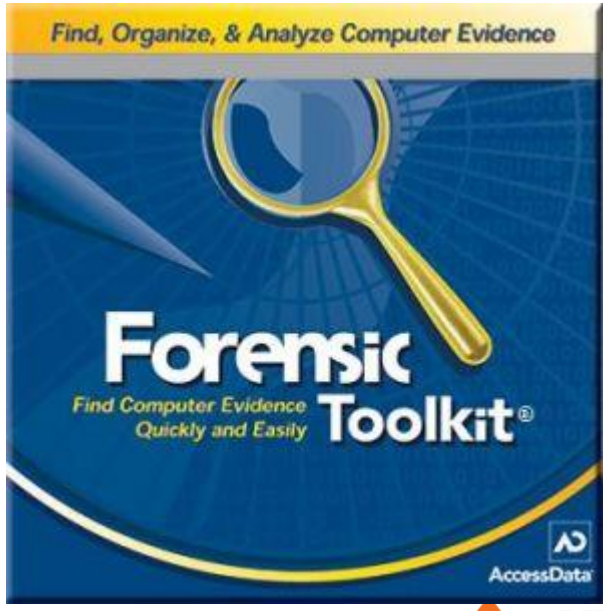
- Asegurar la evidencia sin dañarla.
- Ubicar la evidencia en un lugar seguro.
- Mantener la cadena de custodia.
- Contar con libro de registro en la entrada del lugar donde se almacena la evidencia.
- Ubicar un sistema de alarmas en la entrada del laboratorio forense.

Adquirir la data

La evidencia original nunca debe ser usada para el análisis

Adquirir la data

- Aplicar hash de integridad
- Aplicar bloqueo contra escritura
- Copia bit a bit (obtener la Imagen)
  - Duplicar la data para preservar la original.

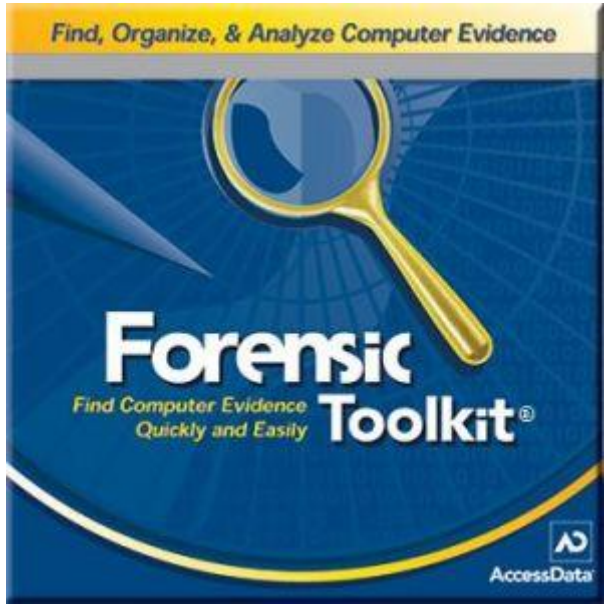


Demo: HashCalc

UNIVERSIDAD DE LIMA

Analizar la data

- Se recuperan datos eliminados.
- Se diseñan las palabras claves para la búsqueda de evidencia según el caso.



UNIVERSIDAD DE LIMA

Informe de investigación

- El informe de investigación debe contar por lo menos con lo siguiente:
  - **Propósito del reporte**: Explicar de manera clara el objetivo, la audiencia objetivo y por que fue preparado el informe.
  - **Autor del reporte**: Listar los autores del reporte, incluir sus cargos y responsabilidades durante la investigación y el detalle de contacto.
  - **Resumen del incidente:** Presentar el incidente y explicar su impacto, el resumen debe explicar claramente que y como el incidente ocurrió.
  - **Evidencia:** Proporcionar la descripción de la evidencia que fue adquirida durante la investigación.
  - **Detalles:**
    - Dar detalle de la descripción de que evidencia fue analizada y los métodos de análisis que fueron usados.
    - Explicar los hallazgos del análisis
    - Listar los procedimientos que fueron seguidos y técnicas usadas durante la investigación
    - Incluir pruebas de los hallazgos.
  - **Conclusiones:**
    - Resume el resultado de la investigación
    - Citar evidencia especifica para probar la conclusión
  - **Documentos de soporte:**
    - Incluye información de respaldo como diagramas de red, descripción de procedimientos usados, información de tecnología utilizada.

Testigo experto

- Es la persona que tiene el conocimiento del objeto de investigación que expondrá los hallazgos y conclusiones a la corte.
  - El rol de un investigador forense es:
    - Investigar un crimen
    - Evaluar la evidencia
    - Documentar el informe
  - El rol de un testigo experto es llevar la evidencia a la corte
    - Asistir a la corte a entender el informe.
    - Ayudar al abogado a llegar a la verdad.
    - Expresar su opinión de experto.

Caso: Testigo Experto

- El testigo experto va a sustentar un informe de investigación forense.
  - Su informe se basa en el análisis de un correo electrónico sobre una infidelidad.
  - Para el adquisición, análisis y reporte el testigo experto menciona haber utilizado herramientas reconocidas en la industria forense.
  - Cuenta con excelentes certificaciones.
  - Expone sus hallazgos ante el juez.
  - El testigo experto esta asesorando al esposo afectado.
  - El informe era impecable.

Caso: Testigo Experto (Evidencia)

Return-Path: <shellyd@xjewellery.com>
X-SpamCatcher-Score: 1 [X]
Received: from [207.3.3.3] (HELO xjewellery.com)by fe3.xjewellery.com
(CommuniGate Pro SMTP 6.1.2) with ESMTP-TLS id 61258719 for
roubx@xmenc.com; Mon, 23 Aug 2004 09:40:10 -0400
Message-ID: <4129F3CA.2020509@xjewellery.com>
Date: Mon, 23 Aug 2004 09:40:26 -0400
From: Sheela Rally
<shellyd@xjewellery.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1)
Gecko/20020823 Netscape/7.0
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Rouba Bandoras <zroubx@xmenc.com>
Subject: Your Sexy Girl Alone at home
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit
Message:
Dear Rouba Bandoras,
My husband is going on a business trip to Italy on the 25th of this month. He will be back on the 29th. Let's meet at our usual hotel Hilton Suite 333 at 8.0 PM tomorrow. I will wait for you with roses, red wine and no clothes on me :)

Its party time honey! Today is very special because we are celebrating
20 weeks of our secret affair.
With lots of love
Sheela Rally

UNIVERSIDAD DE LIMA

Caso: Testigo Experto

- El abogado defensor de la esposa menciona que la versión del correo cliente ***CommuniGate Pro SMTP 6.1.2*** no existe.
- El abogado menciona que se comunico con el mismo fabricante y solo se publico dicha tecnología hasta la versión 6.1.0, por consiguiente, su informe es invalido y no se ha realizado el debido proceso de informática forense.
- **¿En que se pudo haber equivocado el investigador forense digital o testigo experto?**