OWASP
The Open Web Application Security Project

Informática Forense y Evidencia Digital en la Respuesta a Incidentes de Sistemas Web

Felipe Sánchez F.

Perito Judicial en Ingeniería Informática con mención Fraudes y Delitos Informáticos

Analista Forense Senior

fsanchez@fci.cl

http://cl.linkedin.com/in/fsanchezf

Forensic & Cybercrime Investigation

Prevención, Detección e Investigación de Delitos Informáticos

Currículum

OWASP
The Open Web Application Security Project

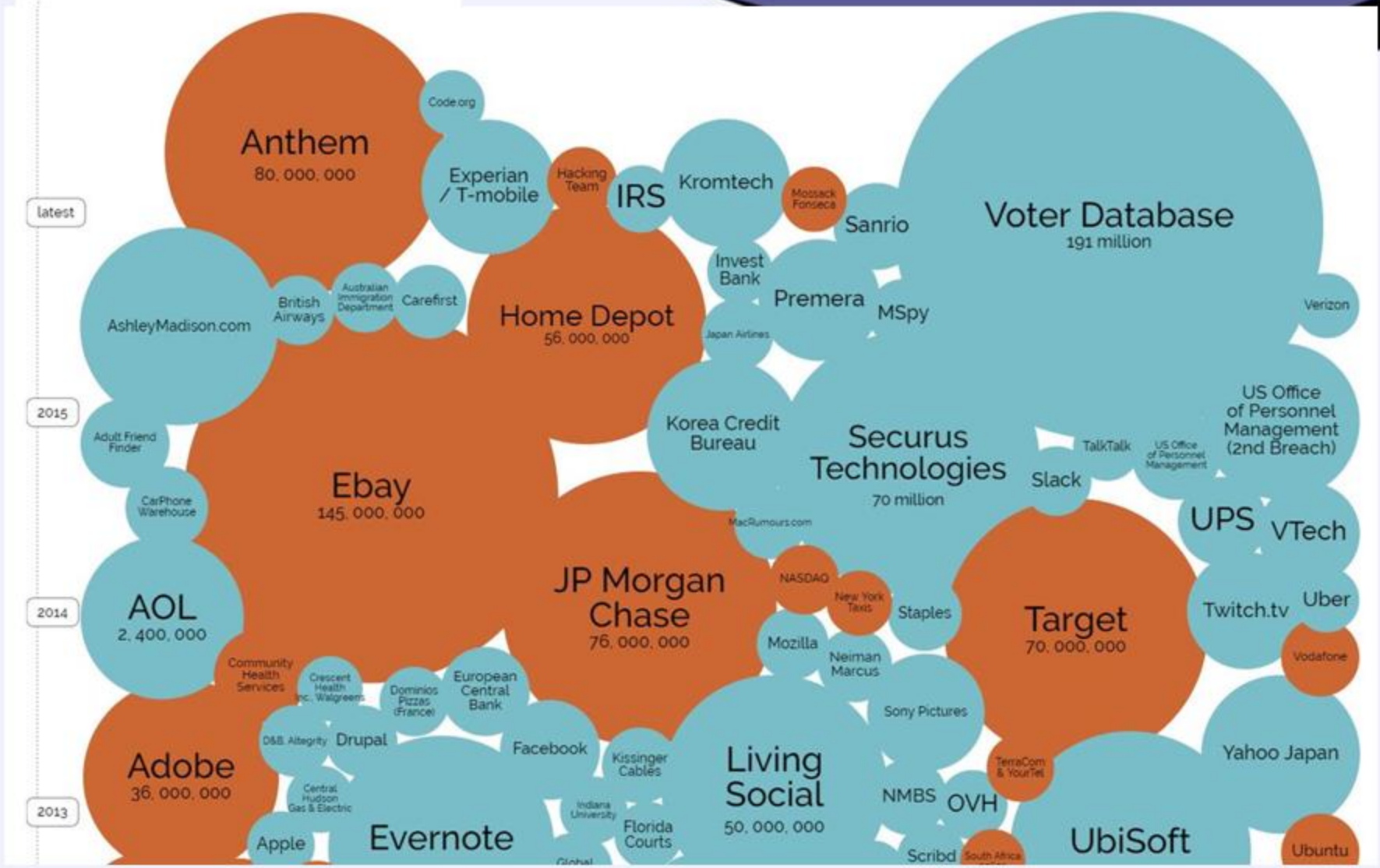
- Ingeniero de Ejecución en Computación e Informática – Universidad de Santiago de Chile.
- Perito Judicial en Ingeniería Informática con mención Fraudes y Delitos Informáticos, Ilustres Cortes de Apelaciones de Santiago, Valparaíso, San Miguel y Rancagua, actuando en sedes: Civil, Laboral, Familia, Penal, Arbitrajes, Contratación Pública, Policía Local y Libre Competencia.
- ex-Perito Informático del Laboratorio de Criminalística Central de la Policía de Investigaciones de Chile.
- Socio de FCI - Prevención, Detección e Investigación de Delitos Informáticos (www.fci.cl).
- Investigador de Delitos Informáticos y Tecnológicos en empresas e instituciones.
- Profesor Universidad de Santiago de Chile - Diplomado en Peritaje Informático. Cursos: "Peritaje Informático Avanzado" e "Informática Forense".
- Profesor Universidad de Chile - Diplomado en Prevención, Detección e Investigación de Fraude. Curso: "Investigación de Delitos Tecnológicos".
- Magister en Seguridad, Peritaje y Auditoría Procesos Informáticos - Universidad de Santiago de Chile (actualmente cursando 2do Año).
- Diplomado en Peritaje Informático – Universidad de Santiago de Chile.
- Perito Informático – Academia Superior de Estudios Policiales, Policía de Investigaciones de Chile.
- Diplomado en Criminalística y Metodología Forense – Universidad de Valparaíso.
- Diplomado en Control, Seguridad y Auditoria Computacional – Universidad de Santiago de Chile.
- Diplomado en Seguridad Integral de Empresas - Academia de Ciencias Policiales, Carabineros de Chile.

OWASP
The Open Web Application Security Project

Tendencia actual

La pérdida de información de las compañías tienen como principal atacante, el personal interno por sobre la acción de *hacker's*. El 35% de las veces que se tiene pérdida de información, es por la acción ilegal de los empleados y sólo un 17% por acción de *hacker's*

Fuente: Kroll Informe Global sobre Fraude 2012-2013


Selected losses greater than 30,000 records
(updated 16th Feb 2016)
YEAR
latest
2015
2014
2013
Anthem
80, 000, 000
Code.org
Experian / T-mobile
Hacking Team
IRS
Kromtech
Mossack Fonseca
Sanrio
Voter Database
191 million
Invest Bank
Premera
MSpy
Verizon
Japan Airlines
AshleyMadison.com
British Airways
Australian Immigration Department
Carefirst
Home Depot
56, 000, 000
Adult Friend Finder
CarPhone Warehouse
Ebay
145, 000, 000
Korea Credit Bureau
Securus Technologies
70 million
TalkTalk
US Office of Personnel Management
US Office of Personnel Management (2nd Breach)
Slack
MacRumours.com
UPS
VTech
AOL
2, 400, 000
JP Morgan Chase
76, 000, 000
NASDAQ
New York Taxis
Staples
Target
70, 000, 000
Twitch.tv
Uber
Vodafone
Mozilla
Neiman Marcus
Sony Pictures
Community Health Services
Crescent Health Inc., Walgreens
Dominos Pizzas (France)
European Central Bank
D&B, Allegrity
Drupal
Facebook
Kissinger Cables
Living Social
50, 000, 000
TerraCom & YourTel
Yahoo Japan
Adobe
36, 000, 000
Central Hudson Gas & Electric
NMBS
OVH
Indiana University
Florida Courts
Apple
Evernote
Scribd
South Africa
UbiSoft
Ubuntu

Concientización

OWASP
The Open Web Application Security Project

"You're going to be hacked. Have a plan."

Joseph Demarest, FBI cyber division chief.

20 de Octubre de 2014

Ley 19.223:
Tipifica figuras penales relativas a la Informática

OWASP
The Open Web Application Security Project

Análisis de la Ley

- Sujeto activo
- Parte Subjetiva
- Parte Objetiva
- Figuras Penales

1.-El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento.

2.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de información, lo intercepte, interfiera o acceda a él.

3.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

4.- El que maliciosamente revele o difunda los datos contenidos en un sistema de tratamiento de información. Si quien incurre en estas conductas es el responsable del sistema de tratamiento de información se aumenta un grado.

Sabotaje

Espionaje

Definiciones

OWASP
The Open Web Application Security Project

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

- **Evento:** Una ocurrencia identificada en el estado de un sistema, servicio o red, indicando una **posible** violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

- **Incidente:** Un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información del organismo.

Definiciones

OWASP
The Open Web Application Security Project

- Punto de Contacto (PoC): persona, departamento u organización que sirve como coordinador o punto focal de la información relativa a una actividad o programa.

- Gestión de incidentes de seguridad: procesos para planificar, detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Respuesta a Incidentes Intuitiva

OWASP
The Open Web Application Security Project

No se preocupa de encontrar y analizar las causas subyacentes a un determinado incidente sino exclusivamente a restaurar el servicio

Los pasos principales para reducir al mínimo el impacto directo de los incidentes de Seguridad de la Información son los siguientes:

- Detener o contener???,
- Erradicar???,
- Restaurar
- Informe??, y
- y Seguimiento ???...

Situaciones Habituales

OWASP
The Open Web Application Security Project

- Falta de normativas o desconocimiento de las mismas
- Notificación de eventos o posibles vulnerabilidades a diferentes departamentos y personal
- Tratamiento de los incidentes de la misma manera
- Desconocimiento de problemas suscitados por parte de autoridades y personal involucrado
- **Falta de investigación y tratamiento de evidencias**
- Desconocimiento de ataques
- Falta de evidencias en problemas legales
- Personal no posee información ni conocimiento de problemas
- Problemas repetitivos

OWASP
The Open Web Application Security Project

Propósito

Proporcionar a la organización la capacidad adecuada para reportar, evaluar, responder y aprender de los incidentes de Seguridad de la Información mediante una correcta planificación

OWASP
The Open Web Application Security Project

Propósito

Planificar y Preparar	Notificar	Evaluar	Responder	Aprender
• Esquema de Gestión de incidentes • Política de Gestión de incidentes (alineada a la Política de Seguridad)	• Recibir notificaciones en un solo punto • Telefónicas, mails, por formulario, monitoreo	• Clasificar eventos o debilidades • Categorizar incidentes • Priorizar incidentes (nivel de pérdida de negocio, repercusión social, importancia del sistema afectado)	• Solucionar de manera adecuada • Escalamiento del incidente • Recolección de evidencias • Investigación del incidente • Comunicación oportuna • Acciones Disciplinarias	• Tener usuarios capacitados • Estadísticas de los incidentes para tomar decisiones • Monitoreo de incidentes cerrados, pendientes

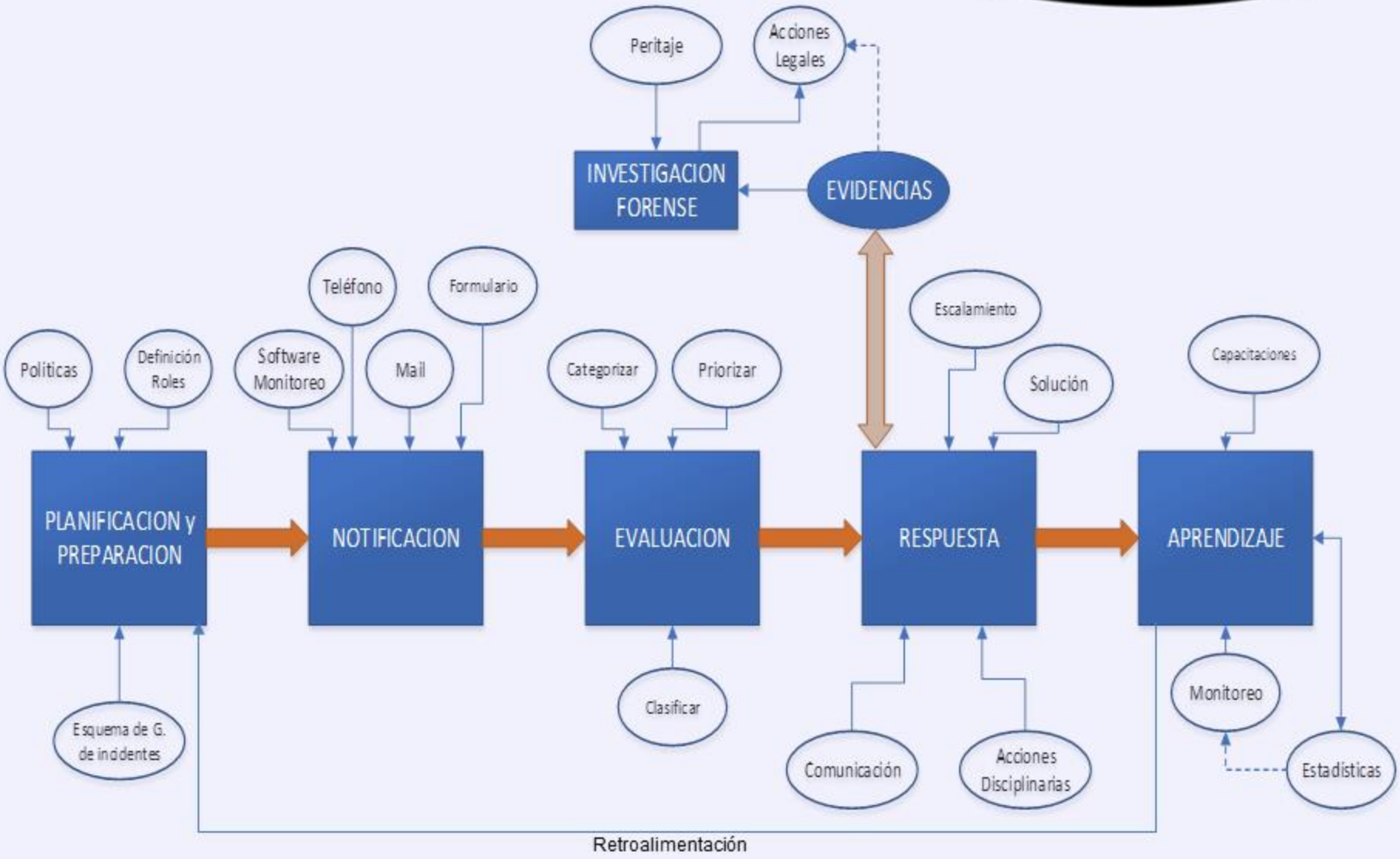
ISO 27035 vs ISO 27001Dom16 vs ISO 27037

OWASP

ISO 27035	ISO 27001 Anexo A Dom16	ISO 27037
1. Planificar y preparar	1. Establecer responsabilidades y procedimientos	
2. Detección y notificación	2. Notificación de Eventos	
	3. Notificación de Debilidades	
3. Evaluación y decisión	4. Valoración de eventos y toma de decisiones	
4. Respuestas	5. Respuesta ante incidentes	
	7. Recopilación de evidencia	Identificación, recopilación, adquisición y preservación de evidencia digital
5. Lecciones	6. Aprendizaje de los incidentes	

Ciclo de Gestión de Incidentes

OWASP
The Open Web Application Security Project



Evidencia Digital

OWASP
The Open Web Application Security Project

Información o datos, almacenados o transmitidos en forma binaria que pueden ser consideradas como evidencia.

Prueba

OWASP
The Open Web Application Security Project

Justificación de la verdad de los hechos controvertidos en un juicio, hecha por los medios que autoriza y reconoce por eficaces la ley.

Anexo: Fruto del árbol envenenado

DICCIONARIO DE LA LENGUA ESPAÑOLA - Vigésima segunda edición

Sitio del Suceso

OWASP
The Open Web Application Security Project

- Su abreviatura es SS.
- Internacionalmente también es conocido como la Escena del Crimen

Definición: Lugar donde ha ocurrido un hecho que es necesario investigar, ya sea desde el punto de vista policial o judicial. Debe ser analizado en búsqueda de señales, rastros o indicios.

Sitio del Suceso – Evidencia Digital

OWASP
The Open Web Application Security Project

Registro de Direcciones IP

Código Procesal Penal

Artículo 222. Inciso quinto.

"… los proveedores de tales servicios (empresas telefónicas y de comunicaciones) deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, **no inferior a un año, de los números IP de las conexiones que realicen sus abonados."**

OWASP
The Open Web Application Security Project

INFORMATICA FORENSE

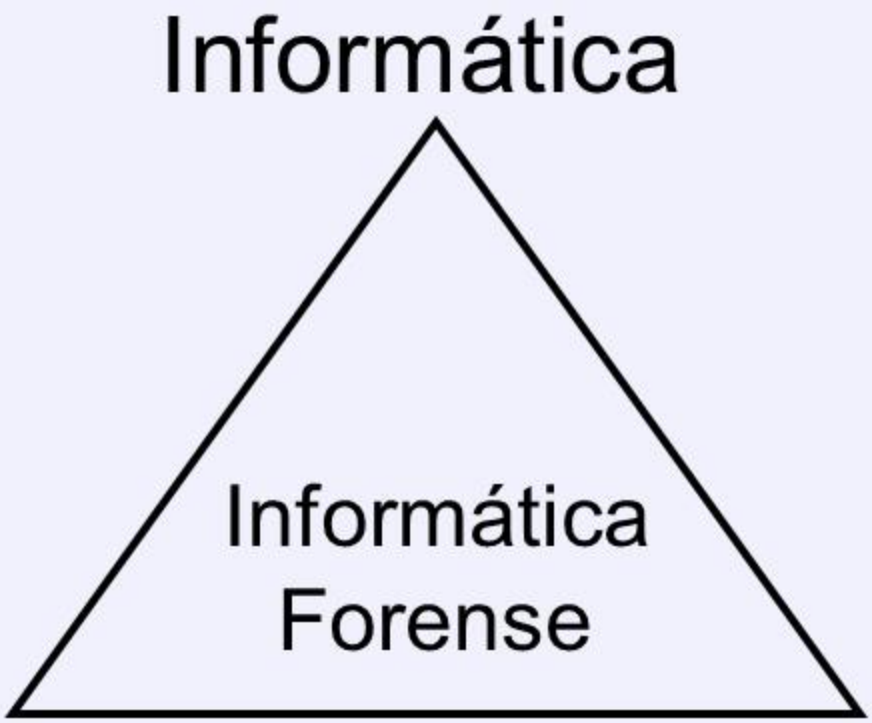
Área de la informática que es auxiliar de la justicia en los ámbitos legales correspondientes a la informática.

Según FBI, es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional.

(http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm)

Aspectos involucrados en la Informática Forense

OWASP
The Open Web Application Security Project

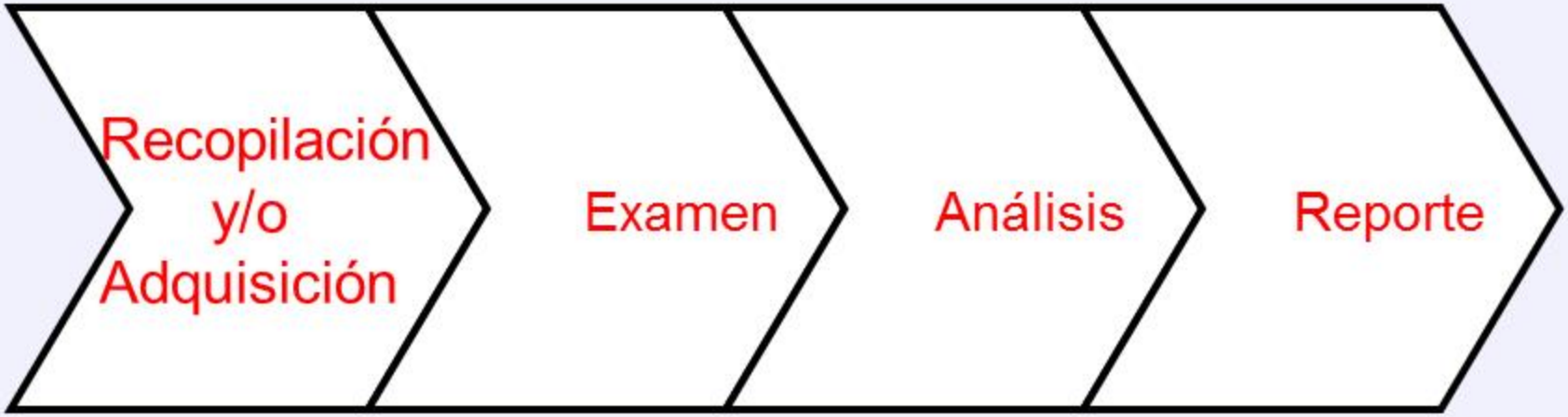


Metodología de trabajo en Sitio del Suceso.
Principios de la Criminalística.
Tratamiento de la evidencia digital.

Define marco legal de acción.
Derechos constitucionales.

Etapas de la Informática Forense

OWASP
The Open Web Application Security Project



Recopilación y/o Adquisición	Examen	Análisis	Reporte
La evidencia digital es identificada, etiquetada, registrada y recolectada y/o adquirida.	Se extrae la información de los dispositivos.	Se verifica la información y se selecciona aquella que es relevante para la investigación.	Se informa sobre lo efectuado.

Importante: Durante todas las etapas la evidencia digital se debe mantener sin ningún tipo de modificación o alteración

Normativas existentes

OWASP
The Open Web Application Security Project

- Norma ISO/IEC 27037:2012 “Directrices para la identificación, recopilación, adquisición y preservación de la evidencia digital”
- Además existen una amplia gama de normas, directrices y buenas prácticas enfocadas en la evidencia digital y su admisibilidad en caso de ser utilizada como medio de prueba.

Es importante conocer que para la implementación de un SGSI basado en ISO 27001:2013, siguiendo los controles de ISO 27002:2013, se deben generar procedimientos documentados para la identificación, recopilación, adquisición y preservación de la evidencia digital.

Normativas existentes

OWASP
The Open Web Application Security Project

El siguiente diagrama nos gráfica, como a través de estándares internacionales se busca llegar a una forma común de trabajar al momento de realizar una investigación forense, con sistemas de tratamiento de la información.

Diagrama básico del proceso

ISO 27037

OWASP
The Open Web Application Security Project

Tres características importantes De la evidencia digital

OWASP
The Open Web Application Security Project

- **Relevancia**: La evidencia digital que será levantada es de importancia para la resolución del caso que se investiga.

- **Suficiencia**: La evidencia digital seleccionada es suficiente para realizar la investigación, no hay evidencia digital de más ni de menos.

- **Confiabilidad**: Todo el proceso por el cual la evidencia fue manejada debe ser auditadable y repetible.

Requerimientos para el manejo De la evidencia digital

OWASP
The Open Web Application Security Project

Auditable: Documentar todas las decisiones y el porqué de estas.

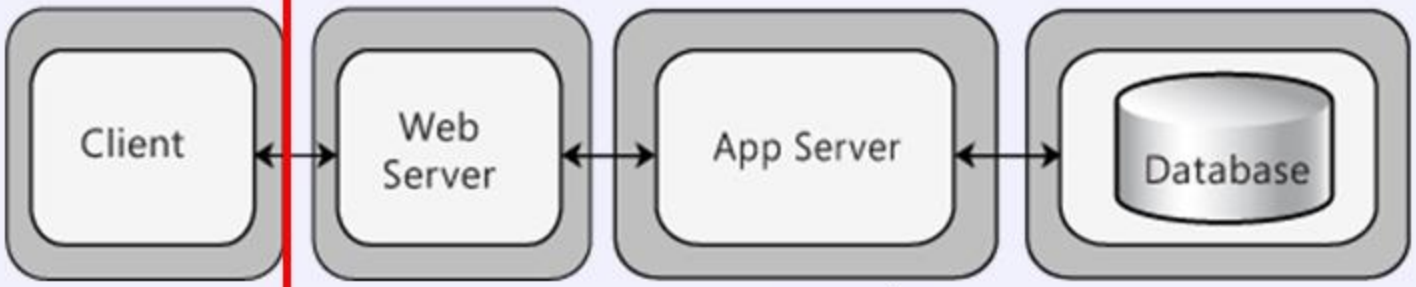
Repetible: Poder realizar el mismo procedimiento, mismas herramientas y obtener el mismo resultado, de esta forma otra persona siguiendo lo documentado obtendrá exactamente lo mismo.

Reproducible: Usando el mismo método, pero diferentes herramientas y diferentes condiciones, se produce el mismo resultado.

Justificable: Toda decisión debe justificarse, demostrando que la decisión que se tomo era la más eficiente

Fuentes de Evidencia Digital

OWASP
The Open Web Application Security Project



Servidor

Fuente

- Archivos de Registros Históricos (Logs).
- Archivos de Configuración.
- Considerar también aplicaciones y scripts propietarios.

Análisis

- Peticiones con parámetros fuera de lo común, tales como strings y comandos, incluso codificados Ej) %HH.
- Tiempos de respuesta muy altos.
- Frecuencia de peticiones de direcciones IP.

Recomendaciones

OWASP
The Open Web Application Security Project

Evaluar la monitorización de integridad de archivos de configuración.

Personalizar registros históricos (logs), en cuanto a ubicación, tamaño, nivel de auditoría y políticas de respaldo, entre otras.

Centralizar respaldo de registros históricos (logs)

- Syslog
- Contenedor centralizado
- SIEM

1er Caso de éxito de FCI

OWASP
The Open Web Application Security Project

Implementación de Laboratorio de Informática Forense a Transbank S.A., dando cumplimiento a cada uno de los requerimientos y alcance que fue definido como ámbito de acción, para su funcionamiento de forma óptima y puedan prestar el servicio sin inconvenientes.

Primera etapa:

- Levantamiento de requerimientos, definiendo ámbito de acción del laboratorio de informática forense.
- Elaboración de Procedimientos documentados y formularios que apoyan la ejecución de los procedimientos.
- Establecer requisitos de equipamiento para el correcto funcionamiento del laboratorio de informática forense en el ámbito definido previamente.
- Capacitación en la ejecución de los Procedimientos documentados y sus respectivos formularios.

Segunda etapa:

- Compra de equipamiento para el funcionamiento del laboratorio de informática forense.

2do Caso de éxito de FCI

OWASP
The Open Web Application Security Project

Implementación del Área de Informática Forense en Banco del Austro (Ecuador), conformado por 3 Equipos Forenses de Primera Respuesta en: Quito, Cuenca y Guayaquil, y un Laboratorio de Informática Forense en la casa matriz en Cuenca. Dando cumplimiento a cada uno de los requerimientos y alcance que fue definido como ámbito de acción, para su funcionamiento de forma óptima y puedan prestar el servicio sin inconvenientes.

Primera etapa:

- Levantamiento de requerimientos, definiendo ámbito de acción del laboratorio de informática forense.
- Elaboración de Procedimientos documentados y formularios que apoyan la ejecución de los procedimientos.
- Establecer requisitos de equipamiento para el correcto funcionamiento del laboratorio de informática forense en el ámbito definido previamente.
- Capacitación en la ejecución de los Procedimientos documentados y sus respectivos formularios.
- Capacitación en el uso de todas las herramientas de software y hardware para desarrollar sus funciones.

3er Caso de éxito de FCI

OWASP
The Open Web Application Security Project

Implementación interna en FCI del proceso “planificación, identificación, recopilación, adquisición, análisis, presentación y preservación de evidencia digital”, superada 1era Fase de Auditoría de Certificación de Sistema de Gestión de Calidad 9001.

Referencias

OWASP
The Open Web Application Security Project

- ISO/IEC 27035:2011
- ISO/IEC 27037:2012
- Ley 19.223 – Delitos Informáticos.

OWASP
The Open Web Application Security Project

Preguntas y Agradecimientos

Forensic & Cybercrime Investigation

Atte.,
Felipe Sánchez Fabre
Perito Judicial en Ingeniería Informática con mención Fraudes y Delitos Informáticos
Analista Forense Senior
fsanchez@fci.cl
http://cl.linkedin.com/in/fsanchezf

www.fci.cl · info@fci.cl