

INVESTIGACIÓN DE DELITOS INFORMÁTICOS

INTRODUCCIÓN

Las intrusiones de seguridad dejaron de ser parte de la ciencia ficción que se ha visto reflejada en varias producciones cinematográficas a ser parte de la realidad cotidiana. Es posible constatar la cantidad de transacciones que ya pueden realizarse a través de Internet sin necesidad de desplazamiento del hogar o la oficina, tales como operaciones bancarias, compras de boletos de cine, pago de los servicios públicos, entre otros.

Al igual que estas actividades cotidianas, las actividades delictivas también han trascendido y se han instalado en el mundo virtual. Ya es normal escuchar de estafas informáticas a personas que nunca conscientemente han brindado sus datos financieros y han sido víctima de robos a través de numerosos métodos, compañías que han sido defalcadas desde el interior mediante el robo de información estratégica que ha llegado a sus competidores y les ha hecho perder clientes y ventaja competitiva en el mundo empresarial, entre muchos otros casos.

Las empresas invierten dinero en las herramientas establecidas en el modelo de seguridad de la información, pero aún así existe un riesgo residual que implica la posibilidad que incidentes de seguridad se materialicen, lo cual implica perjuicios a las compañías y la correspondiente violación de leyes establecidas en los códigos penales de los distintos países, lo cual implica que es posible buscar el respectivo resarcimiento vía judicial por los inconvenientes causados. ¿Cómo debe procederse técnicamente para establecer el fundamento probatorio de un delito informático?

OBJETIVO GENERAL

Los asistentes estarán en la capacidad de aplicar los conceptos fundamentales para la realización de una investigación de un delito informático en cualquier tipo de organización.

Este seminario está dirigido a:

- Gerentes y especialistas en seguridad de la información interesados en conocer sobre los conceptos fundamentales en la investigación de delitos informáticos.
- Especialistas del Derecho interesados en conocer el fundamento probatorio de los casos de delitos informáticos.
- Asesores de empresas interesados en profundizar en el tema de seguridad de la información.

BENEFICIOS

Al finalizar el seminario, los participantes alcanzarán las siguientes competencias:

- Entender como se organiza la investigación de un delito informático.
- Definir el proceso de cadena de custodia al interior de la organización.
- Aplicar la metodología de investigación de delitos informáticos para construir el fundamento probatorio legal de un caso en donde se haya cometido un delito informático.
- Para la práctica del análisis forense, es necesario configurar una estación de trabajo con las herramientas necesarias para la realización de la tarea. **En este curso le suministraremos una máquina virtual VMWARE basada en la ampliamente conocida distribución de Linux para análisis forense HELIX 3.**

EXPOSITOR

Manuel Humberto Santander, Es Ingeniero de Sistemas de la Universidad EAFIT y MBA. Actualmente está cursando el programa Master of Science in Information Security Engineering de SANS Technology Institute. Ha sido coautor de los cursos de SANS Institute Browser Forensics y Protecting your personal privacy on the internet.

Coordinador del Equipo de Seguridad y líder del proceso de atención de incidentes de Las Empresas Públicas de Medellín E.S.P., la segunda empresa más grande de Colombia.

Posee las siguientes certificaciones:

- GIAC GOLD Certified Forensic Analyst (GCFA) #148
- GIAC GOLD Certified Intrusion Analyst (GCIA) #864
- GIAC .NET Security (GNET) #31
- GIAC Certified Firewall Analyst (GCFW) #2213
- GIAC Leadership #228

Actualmente es docente de la Universidad Pontificia Bolivariana y la Universidad de Medellín en Medellín, Colombia, en los temas de Seguridad de la Información, Sistemas Operativos y Arquitectura del Computador. Ha sido docente de cursos de SANS Institute en la modalidad de Local Mentor y de diplomados y cursos en el área de Seguridad de la Información.

Ha sido conferencista invitado en diversos eventos a nivel nacional e internacional en los temas de delitos informáticos y seguridad de la información. Amplia experiencia internacional en el asesoramiento a empresas en la organización para investigar delitos informáticos.

Herramientas Metodológicas a Utilizar

- **Clases lectivas:** Presentación explícita del contenido y de los aspectos conceptuales y técnicos asociados a cada tema en formato Powerpoint.
- **Ejercicios prácticos:** Se realizarán varios ejercicios prácticos a partir de casos de delitos informáticos reales para desarrollar las destrezas necesarias para la solución de los mismos tomando como base la metodología expuesta.

DESCRIPCIÓN DE LA ESTRUCTURA DEL PROGRAMA

Introducción

Temario

- Conceptos fundamentales
- Principios del análisis forense
- Metodología de investigación forense
- Fundamentos de sistemas operativos
- Manejo de memoria en sistemas operativos Windows
- Manejo de procesos en sistemas operativos Windows
- NTFS
- Manejo de memoria en sistemas operativos UNIX
- Manejo de procesos en sistemas operativos UNIX
- Sistemas de archivos UNIX: ext2, ext3, UFS, HFS

Respuesta a incidentes

Temario

- Verificación del incidente
- Estrategia de contención para un incidente de seguridad
- Contención y aislamiento del incidente
- Adquisición de evidencia
- Proceso de Cadena de Custodia de Evidencia
- Ejercicio práctico: Respuesta a incidentes y manejo de evidencia de un delito informático.

Análisis forense

Temario

- Establecimiento de líneas de tiempo
- Análisis de medios
- Modelo de Sistemas de Archivos
- Recuperación de archivos

- Examinación de metadatos
- Creación de líneas de tiempo
- Búsqueda de cadenas de caracteres basada en la lista de palabras interesantes
- Fundamentación del caso
- Realización de Reporte
- Ejercicio práctico: Realización del fundamento probatorio de un caso originado por un delito informático.

REQUERIMIENTOS

Cada participante debe llevar su Laptop la misma que debe cumplir con los siguientes requerimientos técnicos:

- Equipo con mínimo 1 GB de RAM, Windows, 40 GB libres en su disco duro y VMWARE Player, el mismo que puede descargarlo desde la siguiente dirección url: http://www.vmware.com/download/player/player_reg.html

MATERIAL DIDÁCTICO

Cada participante recibirá la presentación en powerpoint realizada por el instructor y lecturas complementarias para profundizar en el tema.

DURACIÓN - HORARIO

Duración: 16 horas

Horario: 9:00 am a 5:00 pm

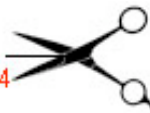
INFORMACIÓN E INSCRIPCIÓN

servicios@eficienciagerencial.com

www.eficienciagerencial.com

Av. Del Pinar # 134, Edificio El Pinar II, Ofic. 803,
Chacarilla del Estanque, Santiago de Surco, Lima – Perú
Telf. (511) 372 1441 / 372 1415 fax (511) 436 6144

Favor completar y enviar vía email a cursos@eficienciagerencial.com o por fax al (511) 436-6144



FORMULARIO DE INSCRIPCIÓN (Para países de América del Sur)

INVESTIGACIÓN DE DELITOS INFORMÁTICOS

INFORMACIÓN DE LA EMPRESA

Nombre de la Empresa _____
RUC _____
Actividad Especifica de la Empresa _____
Dirección _____
Ciudad _____ Provincia _____
Teléfono _____ Fax _____

INFORMACIÓN DEL PARTICIPANTE

Nombres y Apellidos _____
Cargo _____
Email Empresa _____ Email Personal _____
Teléfono (Empresa) _____ Teléfono (Móvil) _____
Sexo F M Fecha Nacimiento (Día/Mes) _____

¿Cómo desea que aparezcan sus datos en su certificado de participación?

(Indique Nombres y Apellidos)

Objetivos que espera lograr asistiendo a este seminario

¿Cómo se enteró del curso?

Prensa Revista Email Google Website Un amigo

Otros, indique _____

DATOS DE FACTURACIÓN

Formas de Pago (*) Depósito en cuenta bancaria Pago en línea vía web EGP
<http://www.eficienciagerencial.com/tienda>
Facturar a Participante Empresa

Si eligió **facturar a empresa** llene la siguiente información:

Persona responsable de la inscripción _____
Departamento _____ Posición _____
Teléfono _____ Fax _____

(*) Datos para depósito en cuenta bancaria:

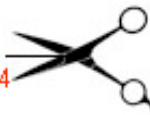
Abono en cuenta ahorro US \$:

- Banco: BBVA
Beneficiario: EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.C.
Cuenta US \$ N° 0011-0194-0200289850-86

Abono en cuenta corriente en nuevos soles S/:

- Banco: SCOTIABANK
Beneficiario: EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.C.
Cuenta N° 6459374

Favor completar y enviar vía email a [cursos@eficienciagerencial.com](mailto: cursos@eficienciagerencial.com) o por fax al (511) 436-6144



FORMULARIO DE INSCRIPCIÓN (Países de America del Norte, Central y Europa)

INVESTIGACIÓN DE DELITOS INFORMÁTICOS

INFORMACIÓN DE LA EMPRESA

Nombre de La Empresa _____
RNC _____
Actividad Especifica de la Empresa _____
Dirección _____
Ciudad _____ País _____
Teléfono _____ Fax _____

INFORMACIÓN DEL PARTICIPANTE

Nombres y Apellidos _____
Cargo _____
Email Empresa _____ Email Personal _____
Teléfono (Empresa) _____ Teléfono (Móvil) _____

Sexo F M Fecha Nacimiento (Día/Mes) _____

¿Cómo desea que aparezcan sus datos en su certificado de participación?
(Indique Nombres y Apellidos)

Objetivos que espera lograr asistiendo a este seminario

¿Cómo se enteró del curso?

Prensa Revista Email Google Website Un amigo

Otros, indique _____

DATOS DE FACTURACIÓN

Formas de Pago (*)Transferencia Bancaria Pago en línea vía web EGP
<http://www.eficienciagerencial.com/tienda>
Facturar a Participante Empresa

Si eligió **facturar a empresa** llene la siguiente información:

Persona responsable de la inscripción _____
Departamento _____ Posición _____
Teléfono _____ Fax _____

(*) Transferencia Bancaria a:

- Banco: BHD (República Dominicana)
Beneficiario: EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.
Cuenta US \$ N° 747777-001-5

POLÍTICAS DE CANCELACIÓN Y REEMBOLSOS

1. Nos reservamos el derecho de cancelar el curso si no se cumplen con las condiciones estipuladas, en este caso el costo de inscripción será reembolsado a los participantes.
2. No nos hacemos responsables por gastos de pasaje u hospedaje en el cual el participante haya incurrido. Toda notificación de cambio o cancelación por parte de nuestra empresa será indicada no menos de quince (15) días antes del inicio del curso.
3. Los asistentes que den por cancelada su participación en el curso quince (15) días antes del inicio del curso tendrán un cargo del 20% del valor de la inscripción del curso, correspondiente a gastos administrativos.
Cancelaciones después de este período no tendrán reembolso, sin embargo el cupo puede ser usado por otro participante de la misma empresa
4. Sólo el envío de la solicitud de inscripción debidamente llenada y el pago adelantado del importe del evento formalizará la inscripción.
5. El curso debe ser pagado en su totalidad antes de la fecha de inicio.