Nuevo Curso Online de Análisis Forense Digital en Profundidad

PRESENTACIÓN

Desde hace unos años, estamos viviendo una convulsión en el área de la seguridad informática. Cada vez, la seguridad está tomando más peso en los procesos internos y externos de las organizaciones, las cuales empiezan a tomar conciencia de que la seguridad es una inversión a futuro.

Por otro lado, cada vez son más frecuentes los ataques dirigidos a empresas y multinacionales de una forma que hasta ahora nunca habíamos visto. El objeto de estos ataques, aparte de tener control de los servidores y bases de datos, se centran en el usuario y la información que éstos disponen, ya sea personal o confidencial.

Los diferentes ataques que inundan las noticias de portada de los diferentes medios digitales, dejan claro (independientemente del origen del atacante) que el malware y las intrusiones se han profesionalizado, hasta llegar a puntos que sólo vale una revisión manual por parte de un analista para detectar donde se encuentra el fallo o el malware.

En la era que vivimos, el antivirus pasa a ser una “comodidad” detectando muestras pasadas y muy difícilmente va a adelantarse a la ingeniería de los atacantes.

Desde Securízame, presentamos un renovado curso online de Análisis Forense en Profundidad, en el que veremos de una forma práctica los entresijos en la detección de intrusiones, análisis forense y peritaje.

El curso tiene una duración de **104 horas** y está orientado a administradores de sistemas o especialistas en el sector de la seguridad que ya dispongan de conocimientos de nivel medio y quieran afianzar su saber en el análisis forense. Asimismo, son objetivo de este curso todas aquellas personas que deseen dedicarse al mundo del peritaje informático forense, siendo un carril de aceleración, que pondrán al alumno a la velocidad adecuada, en las diferentes materias que aquí se detallan.

CONTENIDOS

Módulo I – Informática Forense y Evidencia Digital – 4 horas – Profesor: Alfonso González de Lama

- Actuaciones legales de un perito
- Terminología Jurídica básica
- Cadena de custodia, la importancia de la prueba
- Tareas de gestión con el cliente
- Documento de encargo
- Documento de confidencialidad y deber de secreto
- Honorarios
- Concepto de informe pericial
- Elementos de un informe pericial
    - Identificación
    - Cuerpo del informe
    - Redacción y evidencias
    - Conclusiones
    - Anexos
- ¿Qué espera un cliente, un abogado y un Juez?
- La labor del perito en un juzgado
- Responsabilidad jurídica
- Código deontológico
- Casos prácticos de peritajes y planteamiento judicial

Módulo II – Delitos Informáticos y Criminalidad en Internet – 4 horas – Profesor: Álvaro Andrade

- Terminología e Introducción a los delitos informáticos y la criminalidad en internet
- Organismos Internacionales de Persecución y Represión del Cibercrimen.
- Tipos de delitos reconocidos por la ONU
- Análisis técnico jurídico sobre “la Flagrancia” en Delitos Informáticos o caso de estudio
- Jurisprudencia internacional. (Cómo encontrarla en segundos)
- Evidencia digital y sus características
- Reglas de la evidencia digital para procesos judiciales
- Cadena de custodia en materia de evidencia digital o caso de estudio
- Como desestimar rápidamente evidencia o prueba digital en procesos judiciales o caso de estudio

Módulo III – Análisis forense en Mac OS X – 8 horas – Profesor: Jaime Andrés Restrepo

- Introducción a sistemas Mac OS y sus componentes
- Adquiriendo la evidencia digital
  - Buenas prácticas para la recogida y análisis de los datos en Mac OS
  - Recogida de información en entornos vivos y muertos
  - Recopilación de evidencias en Mac OS ¿Qué herramientas usar?
- Análisis de la evidencia adquirida
  - Análisis forense de la Memoria RAM para Mac OS X
  - Análisis con herramientas del sistema Mac OS X
  - Análisis forense de extensiones del kernel, agentes y demonios del sistema
  - Análisis forense de archivos binarios y aplicaciones integradas
  - Análisis de Navegadores web y sistemas de mensajería
  - Análisis de conexiones, Ethernet, Wifi, Bluetooth
- Análisis con herramientas libres o gratuitas
- Análisis con herramientas comerciales

Módulo IV – Análisis forense en Windows – 8 horas – Profesor: Juan Garrido

- Sistema operativo Windows
  - Diferencias entre Windows 7 y Windows 8
- Tratamiento de las evidencias
  - Análisis de navegación
  - Análisis temporal de la información
  - Búsquedas basadas en firmas
  - Análisis de la papelera de reciclaje
  - El registro del sistema
  - Prefetching en sistemas Windows
  - Copias en la sombra. Diferencias entre Windows 7 y Windows 8
  - Análisis Forense de procesos
    - Procesos en Windows

- Tipos de cuentas en Windows
- Análisis y correlación de procesos
- Relación de procesos, puertos y conexiones realizadas
- Análisis Forense de logs
    - Las auditorías de los sistemas
    - Análisis de registros
    - Consolidación del logs
    - Correlación y forense

Módulo V: Análisis de sistema de ficheros NTFS. Los ficheros del registro de Windows. Análisis de la memoria en Windows. Indicadores de compromiso – 8 horas – Profesor: Pedro Sánchez

- Obtención de evidencias con TRIAGE
    - Introducción al scripting avanzado con Powershell y WMI
    - Creación de un USB para la adquisición de evidencias

- Estructura interna de NTFS
    - Estructura de una partición
    - La tabla Maestra de Archivos (MFT)
    - Cabeceras e identificadores
    - Los Metadatos de ficheros
    - Ficheros de atributos $MFT, $LogFile, $Volume
    - Ficheros INDEX
    - Cómo extraer evidencias de la tabla maestra de archivos
    - Herramientas de extracción
    - Recuperación de ficheros
    - Cómo crear una línea de tiempo (Timeline)

- Ficheros persistentes de entradas de registro
    - Cómo extraer evidencias de información de dispositivos
    - Cómo obtener claves y datos del registro de Windows

- La memoria en Windows
    - Arquitectura de la memoria en Intel 32 y 64
    - Cómo obtener la memoria RAM y fichero Pagefile.sys
    - Cómo extraer contraseñas de la memoria
    - Cómo analizar Malware utilizando la memoria
    - Cómo obtener un ejecutable o fichero de la memoria
    - Herramientas de extracción
    - Cómo automatizar los procesos de búsqueda en memoria

- Obtención de la memoria RAM en frío – “Cold boot”
    - Configuración y diseño de una arquitectura en frío
    - Ventajas e inconvenientes

- Proceso de un USB para la adquisición

- Indicadores de compromiso
  - Ataques APT, ejemplos reales
  - Cómo se desarrolla un indicador de compromiso
  - Cómo se aplica en la búsqueda de una intrusión
  - Ejemplos de indicadores de compromiso
  - Búsqueda de ataques APT utilizando indicadores de compromiso
  - Aplicando Indicadores a la memoria RAM y a dispositivos
  - Inteligencia
  - Modelos Open Source para la mitigación de ataques

Módulo VI: Análisis Forense en Linux – 8 horas – Profesor: Lorenzo Martínez

- Análisis Forense a entornos Linux
- Distribuciones Live Forenses
- Forense de la memoria RAM
- Análisis forense de sistemas de ficheros
- Análisis de la memoria SWAP
- Líneas de tiempo
- Recuperación avanzada de ficheros
- Recuperación de elementos clave
- Cómo descubrir malware pasivo en el sistema
- Artifacts en Linux
- Análisis forense en sistemas GNU/Linux con kernel 3.x
- Casos prácticos: Escenarios de un ataque

Módulo VII: Análisis Forense de discos SSD, Malware y Amenazas – 8 horas – Profesores: Gustavo Presman y Yago Jesus

Análisis de dispositivos SSD – Gustavo Presman

- ¿Qué es un SSD?
  - Comparación con almacenamiento rotacional
  - Ventajas y desventajas
- Arquitectura
  - Tecnología NOR y NAND
  - Firmware SSD
- Adquisición forense de dispositivos SSD
  - Problemática para el analista forense
  - Wear Leveling y Garbage collection
  - Comando TRIM
  - Algunas debilidades de la tecnología

Análisis forense de malware y amenazas – Yago Jesús

- Fundamentos de ingeniería inversa.
- Debuggers.
- Análisis estático de ejecutables.
- Análisis dinámico de ejecutables.
- Fundamentos sobre rootkits.
- Tipos de rootkits.
- Detección de rootkits.
- Análisis de documentos (Doc,PDF) sospechosos.
- Amenazas de tipo Ransomware.

Módulo VIII Análisis Forense de Documentos – 8 horas – José Aurelio García Mateos

- Introducción
  - Qué se en tiende por peritaje de documentos
  - Terminología general en Documentoscopia
  - Terminología específica para escritura mecánica
- Bases de la investigación pericial
  - Clasificación pericial
  - Metadatos en Documentos
    - La fotografía
    - Documentos de Adobe
    - Herramientas de extracción de metadatos
  - Documentos dubitados e indubitados
  - Análisis en el laboratorio
  - Clasificación de la pericial, según el tipo de documento
  - Principio de certeza e infalibilidad
- Medios técnicos para la investigación documental
  - Lentes y lupas
    - Tipos de iluminación
  - Microscopios
  - Elementos de medición
  - Equipo informático
  - Instrumental básico para un laboratorio
- La fotografía en la documentoscopia
  - Elementos necesarios en la reproducción fotográfica
  - Metadatos de la fotografía
- Escrituras mecánicas e informáticas
  - Máquinas de escribir
  - Impresión térmica
  - Impresión por sublimación
  - Impresión por tinta
  - Impresión láser
  - Sistemas mixtos

    - Peritajes de fotocopias
- Elementos que transforman a los documentos
    - Marcas, desgarros, cosidos
    - Alteraciones y transformaciones
- Grafismo y Escritura
    - El proceso grafogenético
    - Principios fundamentales de la escritura
    - La escritura como elemento físico de estudio en laboratorio
        - Estudio de las tintas bajo el microscopio
        - Transparencia, porosidad, penetración
    - La escritura como hecho dinámico
        - Velocidad y dirección
        - Inclinación y continuidad
        - Presión, dimensión, forma
        - Métodos calígrafo, grafonómico y grafométrico
    - Falsificación de documentos

Módulo IX Análisis Forense de virtualización y RAID – 8 horas – Profesor: Gustavo Presman

- Análisis forense en entorno RAID
    - Array de discos
        - Estructura básica de un disco duro- Modelización
        - Tipos de Array RAID
        - Array por Hardware y por software en entornos Linux y Windows
        - Imágenes Forenses de RAID
        - Adquisición lógica y física
        - Herramientas open source y gratuitas
        - Identificación y rearmado del arreglo
        - Ejemplos prácticos
- Virtualización de evidencia digital
    - Máquinas virtuales
        - Por qué utilizarlas en ambiente forense?
        - Arquitectura
    - Virtualización de imágenes forenses
        - Virtualización de unidades lógicas
        - Virtualización de equipo completo
        - Herramientas open source y gratuitas
        - Ejemplos prácticos
        - Solución de problemas
        - Ejecución de aplicaciones en la maquina a investigar

Módulo X: Análisis Forense en Redes, antiforense, correos electrónicos y VoIP – 8 horas – Profesor: Giovanni Cruz

- Análisis Forense en red

    - Definición
    - Desafíos
    - Principales herramientas
    - Análisis de protocolos
- AntiForense
    - Desafíos
    - Principales técnicas
    - Ejemplos
- Forense en correos electrónicos
    - Cabeceras de correo electrónico
    - Identificación de elementos forenses
    - Artefactos en navegadores
    - Artefactos en clientes de correo
    - Artefactos en servidores de correo
- VoIP
    - Ataques a plataformas VoIP
    - Logs generados dentro de los eqipos
    - Artefactos VoIP

Módulo XI: Análisis Forense de aplicaciones Microsoft: Active Directory, IIS, SQL Server, Exchange – 8 horas – Profesor: Juan Garrido Caballero

- Active Directory
    - Esquemas y bosques
    - Autenticación y autorización
    - Captura de evidencias
    - Auditoría de eventos
    - Análisis NT Directory Services database (NTDS)
    - Realización de consultas
    - Extracción de datos online y offline

- IIS
    - Arquitectura IIS 7.5
    - Registros y log
    - parseo y normalización de IIS logs
    - Análisis de .NET logs

- SQL Server
    - Ficheros de datos y log
    - Recolección de evidencias
    - Búsqueda de cadenas
    - Creación de línea temporal
    - Recuperación de datos

- Exchange

    - Identificación y extracción de datos
    - Log Tracking
    - Auditoría de accesos a buzones
    - Outlook Web Access (OWA)

- Windows
    - Análisis de navegación (IE, Chrome, Firefox)
    - Análisis temporal de la información
    - Búsquedas basadas en firmas
    - Análisis de la papelera de reciclaje
    - El registro del sistema
    - Prefetching en sistemas Windows
    - Copias en la sombra. Diferencias entre Windows 7 y Windows 8
    - Tipos de cuentas en Windows
    - Análisis Forense de logs
        - Las auditorías de los sistemas
        - Consolidación del logs

Módulo XII: Análisis Forense de tarjetas SIM, Blackberry y Windows Phone – 8 horas – Profesor: Pedro Sánchez Cordero

- Tarjetas SIM/USIM
    - Descripción y arquitectura interna
    - Datos en las tarjetas SIM/USIM
    - Clonado físico de tarjetas SIM
    - Adquisición de evidencias
- Dispositivos windows phone
    - Arquitectura de Windows Phone
    - Estructura de la memoria
    - Estructura de ficheros
    - Arquitectura interna y modelo de seguridad
    - Sistema de ficheros iNTFS
    - Recovery
    - Tarjetas SD
    - Adquisición de evidencias
    - Clonados vs ficheros
    - Herramientas de extracción.
    - Utilidades comerciales
- Dispositivos Blackberry
    - Arquitectura interna y modelo de seguridad
    - Sistema de ficheros
    - Tarjetas SD
    - Adquisición de evidencias
- Modelos no convencionales
    - Chip Off

- Reanimate

Módulo XIII: Análisis Forense en IOS – 8 horas – Profesor: Jaime Andrés Restrepo

- Introducción – ¿Por qué hacer análisis forense digital a un móvil?
- Adquiriendo la evidencia digital
  - Adquisición desde un Backup de iTunes
  - Adquisición desde iCloud
  - Adquisición de copia bit a bit
  - Adquisición de copia lógica
- Análisis de la evidencia adquirida
  - Análisis de Contactos, Llamadas, Mail, Fotos y Videos, Mensajes de Texto, Notas, Calendario de Eventos, Navegación desde Safari, Spotlight, Mapas, Notas de Voz, Preferencias del Sistema, Logs del Sistema, Diccionarios Dinámicos, Aplicaciones Third Party, Información Eliminada
  - ¿Novedades en iOs 8 a Analizar?
  - Análisis Con Herramientas libres o gratuitas
  - Análisis Con Herramientas Comerciales

Módulo XIV: Análisis Forense en Android – 8 horas – Profesor: Lorenzo Martínez

- Android Internals
- Sistema de ficheros YAFFS2
- Información y configuración del sistema
- Dalvik VM vs ART
- Adquisición de evidencias
- Análisis de la memoria
- Bloqueo/desbloqueo del dispositivo
- Emuladores: SDK & Genymotion
- Los Logs en Android
- Las aplicaciones en Android: Estructura interna de APKs
- Análisis forense de aplicaciones
- Exposición de un caso real
- Cooking your own malware in Android

Observaciones: Los módulos 1 y 2 son una unidad indivisible de 8 horas.

SOBRE EL PROFESORADO

ALFONSO GONZÁLEZ DE LAMA

Alfonso es abogado en ejercicio del Ilustre Colegio de Abogados de Madrid, cuya especialización se ha centrado en el derecho informático, LOPD, LSSI y delitos penales relacionados con la informática y las tecnologías.

Actualmente es Project Manager en HP, con más de 15 años de experiencia en el mundo de IT, definiendo las líneas tecnológicas empresariales y llevando a cabo diversos proyectos de gran envergadura, tanto nacional como internacional.Asimismo, forma parte de la Asociación Nacional de Ciberseguridad y Pericia Tecnológica, ANCITE (www.ancite.es)

ÁLVARO ANDRADE (@aandradex)

Es MCSE, Ingeniero de Sistemas Certificado por Microsoft. Actualmente se desempeña como CEO de la firma Ethical Hacking Consultores desde la cual brinda servicios a Gobiernos, entidades financieras, empresas de telecomunicaciones y policías en varios países de Latinoamérica. Desde el 2014 invirtió en la compañía KAS (Krypto ATM Systems) de la cual es CEO & Founder desde donde se desarrollan soluciones de alta seguridad para más de 70 bancos internacionales en el diseño de Software y Hardware de Seguridad para cajeros ATMs y servicios especializados de forense en ATMs. Lleva 14 años dedicado a la Seguridad informática e informática Forense y desde hace 10 años en materia de Derecho Informático, como consultor en varias organizaciones gubernamentales como privadas en Bolivia, Brasil, Ecuador, México, Costa Rica, Puerto Rico y Panamá. Dirige un programa de certificaciones internacionales en Informática Forense, Ciberdelitos y Seguridad Informática con la Universidad Latina de Panamá. Fue asesor en materia de Inteligencia Informática e Informática Forense para el grupo de inteligencia del presidente Rafael Correa de Ecuador 2011-2013. Fue Presidente del Capítulo FIADI Bolivia para el XVII Congreso Iberoamericano de Asociaciones de Derecho e Informática en el 2013.

JAIME ANDRÉS RESTREPO (@dragonjar)

Ingeniero en Sistemas y Telecomunicaciones de la Universidad de Manizales. Information Security Researcher con más de 10 años de experiencias en Ethical Hacking, Pen Testing y Análisis Forense.

Docente Universitario en Pre y Post-Grado, Speaker y Organizador de diferentes eventos de Seguridad Informática, Creador de La Comunidad DragonJAR (www.dragonjar.com), una de las comunidades de seguridad informática más grandes de habla hispana.

Dirige DragonJAR Soluciones y Seguridad Informática, empresa de consultoría y servicios de seguridad para Colombia y Latinoamérica.

JUAN GARRIDO (@tr1ana)

Es un apasionado de la seguridad. Nombrado por Microsoft MVP Enterprise Security, es un consultor especializado en análisis forense y test de intrusión, trabajando en proyectos de seguridad desde hace más de 8 años. Autor del libro "Análisis forense digital en entornos Windows", el cual se encuentra en su tercera edición, así como de artículos técnicos publicados en prensa especializada y medios digitales. Juan es un ponente común en muchas de las conferencias más importantes a nivel nacional y del panorama internacional, como bien pueden ser NoConName, RootedCon, Defcon, Troopers, etc…

Podrás encontrar referencias de artículos, presentaciones y Webcast directamente en su blog http://windowstips.wordpress.com además de su twitter (@tr1ana).

PEDRO SANCHEZ (@conexioninversa)

Ingeniero informático. Ha trabajado en importantes empresas como consultor especializado en Computer Forensics, Honeynets, detección de intrusiones, redes trampa y pen-testing. Ha implantado normas ISO 27001, CMMI (nivel 5), PCI-DSS y diversas metodologías de seguridad, especialmente en el sector bancario, durante más de diez años. También colabora sobre seguridad, peritaje y análisis forense informático con diversas organizaciones comerciales y con las fuerzas y empresas de seguridad del estado, especialmente con el Grupo de Delitos Telemáticos de la Guardia Civil (GDT), la Brigada de Investigación Tecnológica de la policía nacional (BIT), INCIBE y Ministerio de Defensa.

Ha participado en las jornadas Locked Shields organizadas por el ministerio de defensa, en donde obtuvo la certificación OTAN SECRET.

Ha trabajado en grandes compañías como responsable del equipo de respuesta ante incidentes e inteligencia de BITDEFENDER.

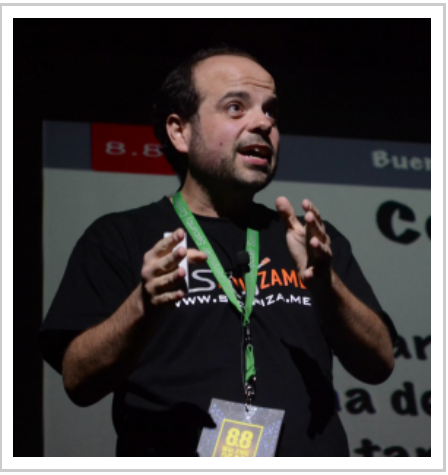
Actualmente es miembro de la Spanish Honeynet Project, fundador del blog Conexión Inversa (www.conexioninversa.com) y trabaja como Director del CyberSOC de Deloitte en Barcelona.

Es Perito Judicial Informático, adscrito a la Asociación Nacional de Ciberseguridad y Pericia Tecnológica (ANCITE www.ancite.es).

Además, es ponente en conferencias Nacionales e Internacionales presentando diversos estudios y vulnerabilidades sobre seguridad informática.

Ha publicado cientos de artículos en revistas especializadas y está pendiente de una patente sobre tecnologías de seguridad.

LORENZO MARTINEZ (@lawwait)



Lorenzo Martínez Rodríguez es Ingeniero en Informática licenciado por la Universidad de Deusto (1996-2001). Especializado en seguridad informática, cuenta con certificaciones de seguridad como CISSP de ISC2 y CISA de ISACA. Dispone de una amplia experiencia laboral en empresas consultoras en el mundo de la seguridad informática española, así como fabricantes de seguridad multinacionales.

Actualmente dirige su propia compañía, Securízame (www.securizame.com), especializada en seguridad de sistemas y redes de comunicaciones.

Lorenzo es co-fundador y editor del blog de seguridad en español Security By Default (www.securitybydefault.com).

Asimismo, forma parte de la Asociación Nacional de Ciberseguridad y Pericia Tecnológica, ANCITE (www.ancite.es).

GUSTAVO PRESMAN (@gpresman)

Gustavo Presman es Ingeniero Electrónico por la Universidad de Buenos Aires (UBA) y Master en Tecnologías de la Información en el programa Gadex . Posee las certificaciones en Informática Forense EnCE, ACE, CCE, NPFA y FCA. Es miembro del capítulo sudamericano HTCIA.

Actualmente es Profesor titular de Análisis Forense y Delitos Informáticos en la Maestría de Seguridad Informática en la UBA y en la Universidad Don Bosco en El Salvador. Profesor titular del posgrado de Derecho Informático de la UBA. Profesor de la Academia de la magistratura del Perú Consultor en tópicos de Informática Forense en fuerzas de la ley y organizaciones públicas y privadas en Uruguay, Paraguay, Bolivia, Perú, Ecuador, Colombia, Panamá, Costa Rica y México. Expositor Frecuente en eventos de toda Latinoamérica.

YAGO JESUS (@yjesus)

Profesional con más de 10 años de experiencia en el sector de la seguridad informática, ha trabajado

para importantes empresas como Telefónica, Caja-Madrid, sector defensa y administraciones públicas.

Editor del blog Security By Default (www.securitybydefault.com), ha desarrollado multitud de herramientas relacionadas con la seguridad informática.

Fundador de eGarante (www.egarante.com), ha publicado decenas de herramientas que se pueden consultar en www.security-projects.com. **JOSÉ AURELIO GARCÍA**

Auditor y Perito Informático. Ha estudiado Ingeniería Técnica en Informática de Sistemas, en la Universidad de Salamanca. Es igualmente Diplomado en "Perito en Piratería Industrial e Intelectual", por la Universidad de Valladolid, y por la Escuela de Criminología de Cataluña; además es "Auditor y Perito Informático", titulado por la Universidad de Ávila. Sus primeros pasos se encaminaron hacia el mundo de la programación, realizando varios proyectos en lenguajes ensamblador y C, entre los que destacó el desarrollo de un programa financiado por la Unión Europea, para la implantación de un sistema automatizado de búsquedas de Normativa Europea, a través del entorno Videotex, antecesor de Internet. Ha sido administrador de sistemas UNIX y profesor experto en diversas áreas de programación y sistemas computacionales, impartiendo cursos en colaboración con varios organismos estatales y privados. Actualmente compagina su carrera profesional como desarrollador de sistemas de interconexión de redes seguras y Cloud Computing, con el Despacho de Auditoría y Peritaje Informático de Salamanca. Es, además, vicepresidente de la Asociación Nacional de Ciberseguridad y Pericia Tecnológica.

GIOVANNI CRUZ (@fixxx3er)

Master en Seguridad de la información con 8 años de experiencia en diferentes áreas como Ethical Hacking, Respuesta a Incidentes, Sistemas de Gestión de Seguridad de la Información e Investigación.

Giovanni es el CEO de CSIETE donde, con su experiencia de 10 años en consultoría técnica y de gestión en seguridad de la información genera, junto a su equipo de trabajo, propuestas de investigación, desarrollo e innovación en dicho tema. Es Master en Seguridad de la Información, Especialista en Gestión de proyectos de I+D y certificado en GSEC, CEH, LA 27000, CWSP y CEI.

Disfruta en compartir su pasión y conocimiento como profesor en diferentes universidades, entrenador de certificaciones y cursos abiertos y en diferentes eventos. Es fundador y organizador de BSides Colombia, cofundador de Barcamp Security Edition y Busy Tone Group.

INFORMACIÓN GENERAL

- El curso completo se ha estructurado en 13 módulos de 8 horas cada uno, según las diferentes materias cubiertas.
- Los módulos I y II duran 4 horas cada uno y se venden como uno sólo, juntos y de forma inseparable.
- El temario expuesto anteriormente, será el mínimo a exponer en cada módulo. Es decir, que queda en manos de cada profesor agregar nuevos contenidos, si así lo considera necesario, para dar mayor profundidad a la asignatura correspondiente.
- Este curso, que será impartido de manera online, y en idioma español, se llevará a cabo en directo por cada profesor, en sesiones de dos horas por día.
- Es posible que haya recursos externos compartidos por los profesores que estén en inglés.
- El objetivo de cubrir un módulo por semana, permite al alumno asimilar cada tema, realizando las prácticas necesarias para ello.
- **Como plataforma de streaming para impartir el curso, se ha elegido la herramienta Cisco Webex. Cada alumno confirmado recibirá un usuario válido por correo electrónico.**
- Igualmente, se pondrá a disposición de los alumnos una plataforma dedicada de e-learning, en la que, vía web, cada profesor dejará la documentación, herramientas, enlaces, imágenes, ejemplos y cuanto considere necesario para impartir los módulos.
- Si, a lo largo del curso, os surge cualquier duda técnica, relativa a algún módulo en concreto, la forma de contacto entre profesores y alumnos, será de forma obligada mediante la plataforma de e-learning, donde además centralizaremos el material de descarga del curso, y que se proporcionará por cada profesor en cada módulo.
- El **curso se impartirá entre el 23 de Febrero y el 21 de Mayo de 2015**
- El curso se realizará en horario de **16:00 a 18:00 GMT+2** (horario peninsular de España) y de **10:00 a 12:00 GMT-5** (Horario de Colombia, Perú, Ecuador), de **Lunes a Jueves**.
- En algunos casos (por ser fiesta de Semana Santa y San José en España), se impartirán dos sesiones el día viernes en el horario mencionado en el punto anterior
- Las plazas para acceder a este curso son limitadas. Por ello, se ha definido un periodo de **registro y pago adelantado** que va desde el **21 de Enero al 13 de Febrero de 2015.**
- Si decides llevar a cabo el registro y/o pago entre el 14 de Febrero y el 20 de Febrero de 2015, el coste de tu matrícula se verá incrementada en un 10%. Esto se aplicará aunque el registro se haga anteriormente al 14 de Febrero, mientras el pago no se formalice antes del 13 de Febrero.
- El **pago será la única garantía de formalización de registro.** A los pocos días de registrarte nos pondremos en contacto contigo para indicarte la forma de pago.
- Securízame proveerá los datos necesarios para las empresas que así lo soliciten, en caso de querer tramitar la bonificación del curso con la Fundación Tripartita. Desde Securízame **NO EFECTUAREMOS NINGÚN TRÁMITE CON LA FUNDACIÓN TRIPARTITA** para este fin, siendo tarea del alumno (o de su empresa).

INSCRIPCIONES EN GRUPO

1. Para las inscripciones de grupos, de máximo 5 personas, se recibirá un único código de acceso al curso, por lo que los integrantes del grupo (hasta 5 personas) sólo podrán acceder desde una misma ubicación (ordenador). Esta modalidad está pensada fundamentalmente para empresas u organizaciones que inscriban a varias personas de forma conjunta. Es decir, **no se podrá acceder a las sesiones en vivo, con un mismo usuario, desde más de una ubicación, esto es desde el mismo ordenador.**
2. El procedimiento de inscripción al curso para grupos, es nombrar un portavoz del mismo, que será quien realice el alta en la web, indicando su nombre, apellidos, país, correo electrónico y teléfono. En el campo comentarios, indicad los nombres y apellidos de los demás inscritos. Si sois entre 5 y 10 usuarios, se os asignarán dos diferentes, para que podáis conectaros en grupos de hasta 5 alumnos.
3. La matriculación en formato grupo no permite la acumulación de otras ofertas, siendo un pack único e indivisible para el curso completo.

MATERIAL DEL CURSO

1. Cada profesor decidirá qué material quiere poner a disposición de sus alumnos en cuanto a prácticas, documentación extra, etc. se refiere.
2. Como mínimo, los alumnos dispondrán de la documentación en PDF relativa a las slides de presentación que cada profesor utilice en sus sesiones.
3. Todo el acceso a documentación, ejemplos, binarios, capturas de red, máquinas virtuales, etc, etc,… se centralizará en la plataforma de formación de Securízame.
4. Se proporcionará un usuario a cada alumno, para acceso a todo el material y aunque haya enlaces de descarga a recursos externos, todo lo disponible se publicará en dicha ubicación centralizada

REQUISITOS MÍNIMOS PARA LOS ALUMNOS

1. Como requisitos hardware, será necesario un ordenador o computadora que sea capaz de ejecutar con soltura un entorno de como máximo dos o tres máquinas virtuales. Se recomienda un procesador de unos 2 Ghz. y 4 GB de RAM.
2. Como requisitos software, se necesitará un ordenador o computadora con sistema operativo Windows, Linux o Mac, donde se ejecutará Virtualbox como plataforma gestora de máquinas virtuales.
3. Los profesores proveerán imágenes con máquinas virtuales de aquellos sistemas operativos que no tengan derechos de difusión o que sean de uso libre. Desde Securízame no compartiremos imágenes de sistemas operativos que requieran licencia de pago.
4. Para las sesiones de formación se utilizará WebEx, por lo que los requisitos mínimos software para poder asistir, serán los soportados por WebEx

CERTIFICADO DE ASISTENCIA

1. A la finalización del curso, se expedirá un certificado de asistencia con aprovechamiento, avalado por Securízame, y firmado digitalmente por eGarante. Dicho certificado desglosará los módulos a los que se ha asistido, así como el número de horas total, a nombre de cada

asistente.

2. Para la expedición del certificado, Securízame tendrá que haber verificado que el alumno **ha asistido a un 80% de las sesiones**, así como **que ha rellenado la encuesta de cada uno de los módulos** a los que se ha matriculado.
3. En el caso de grupos de menos de 5 personas, se generará un certificado para cada uno de los 5 integrantes del curso, con idéntico contenido
4. Dicho certificado será en formato PDF, firmado digitalmente por eGarante
5. El curso no cuenta con un examen o evaluación del alumno, sino que está pensado como una transferencia de conocimientos de ***Análisis Forense Digital y Peritaje***. Es decir, que el certificado que se envía por email al alumno indica matriculación y asistencia, pero no evaluación de conocimientos.

CURSO PRESENCIAL vs. DIFERIDO

1. Los contenidos referenciados de cada módulo se encontrarán actualizados en la plataforma de formación de Securízame, como mínimo media hora antes del inicio de la primera sesión del módulo, aunque se hará todo lo posible por ponerlo a disposición de los alumnos con el mayor tiempo posible.
2. Por motivos de protección de propiedad intelectual, las transparencias a utilizar en cada módulo por cada profesor, serán enviadas de forma personalizada y con marca de agua a cada alumno. Dicha marca de agua contendrá el nombre, apellidos y DNI (en caso de nacionalidad española) o pasaporte (en caso de nacionalidad no española) del alumno al que es expedido, si es a título individual, y del portavoz del grupo si es en formato grupo.
3. Por tal motivo, es que durante el periodo de inscripción se te solicitará copia escaneada de tu DNI o pasaporte, en el entendido que los datos contenidos en el tales documentos serán recopilados y tratados exclusivamente para llevar a cabo las finalidades establecidas en el párrafo anterior, ello con apego al Aviso de Privacidad de Securízame.
4. Media hora antes de que comience cada sesión, se enviarán a cada alumno (o portavoz en el caso de los grupos) un correo vía WebEx y otro vía la plataforma de formación de Securízame, con el enlace a la sesión WebEx.
5. Ya sea porque los horarios en los que se harán las sesiones presenciales no te encajen por tu trabajo o compromisos diarios, como porque te pierdas alguna, las clases quedarán grabadas en WebEx. A los minutos de haber terminado una sesión, te llegará un correo con un enlace para poder visualizar dicha sesión desde WebEx.
6. Por motivos de protección de propiedad intelectual del curso, las sesiones no serán descargables, por los usuarios para visionado offline, sino que se tendrá que disponer de conexión a Internet para poder acceder al contenido del mismo
7. El acceso a los videos offline y las sesiones online se hará mediante WebEx por lo que los sistemas operativos y navegadores soportados serán aquellos soportados por WebEx.
8. Aunque las sesiones en vivo de dicho curso terminan el Jueves 21 de Mayo, Securízame se compromete a mantener dichos videos accesibles vía WebEx, al menos, hasta el lunes 30 de Junio de 2015. Los usuarios creados en la plataforma de e-learning estarán disponibles para acceso a los contenidos de los módulos matriculados hasta la misma fecha.

OTRAS OBSERVACIONES

- La organización se reserva el derecho de posponer el curso en el caso de que los pagos formalizados no superen el 75% de los registrados.
- La organización se reserva el derecho a elegir una plataforma distinta a Webex para las sesiones online. En este caso, se elegirá otra solución que permita las mismas posibilidades de impartición de sesiones, así como de requisitos similares para los alumnos.
- La organización se reserva el derecho a adelantar la fase de formalización de pago del curso, en caso de que el aforo máximo de usuarios se alcance en fechas de pre-registro. En este caso, Securízame se comunicará con cada pre-registrado en la dirección de correo electrónico suministrado, y la plaza se garantizará exclusivamente por el orden de pago recibido.
- En el caso que algún profesor, decidiera no impartir su módulo, la organización se encargará de la sustitución del mismo por otro profesional capaz de impartir dichos conocimientos. En caso que esto no fuese posible, o que el alumno no esté de acuerdo con la sustitución, se devolvería la parte proporcional del dinero pagado por el módulo correspondiente al alumno. Llegados a este caso, el alumno deberá indicar a Securízame su disconformidad por el cambio y solicitar la devolución de la parte proporcional del módulo ANTES de que este comience. No se devolverá el dinero al alumno, en este caso, una vez que el módulo se haya comenzado a impartir.
- Toda comunicación con los alumnos registrados se llevará a cabo por correo electrónico exclusivamente.
- **Importante:** Con determinadas plataformas de correo como Hotmail y Gmail, a veces, los correos con comunicaciones enviados desde Securízame van a parar a la carpeta de “Correo No Deseado” o SPAM. Por favor, monitoriza dicha carpeta con cierta frecuencia y, si esto llega a suceder una vez, márcanos como remitentes confiables. Así, los siguientes correos irán a parar a tu Inbox.

COSTES DEL CURSO

- Curso completo en formato individual: 1.900 € + 21% IVA
- Curso completo en formato grupo (máximo 5 asistentes): 5.900 € + 21% IVA
- Módulo separado de 8 horas en formato individual (los módulos I y II se venden como un único módulo indivisible): 275 € + 21% IVA (por módulo)
- Pack de 3 módulos de 8 horas en formato individual: 745 € + 21% IVA
- Pack de 5 módulos de 8 horas en formato individual: 1210 € + 21% IVA
- **Importante**: Para los residentes en la Unión Europea, se facturará el IVA del país de residencia (según los datos de facturación proporcionados). Para aquellos residentes fuera de la Unión Europea, así como Islas Canarias, estarán exentos de pagar el impuesto del 21%.

Se ha establecido dos rangos de fechas para llevar a cabo la matriculación y pago del curso:

- Desde el 23 de Enero al 13 de Febrero de 2015, los costes del curso serán los indicados anteriormente.
- Si la matriculación y/o el pago se hace efectiva desde el 14 al 20 de Febrero de 2015, el coste del mismo se incrementará en un 10%, no considerándose la matrícula formalizada hasta que

se lleve a cabo el pago en su completitud.

Medios de pago aceptados

- Transferencia bancaria a una cuenta en España de Banco Santander, o Paypal
- En caso de que el pago se realice por **Paypal**, llevará un **incremento del 6%** del coste total.
- No se aceptarán pagos por UKASH, Western Union, Bitcoins, ni mecanismos de pago diferentes a Transferencia Bancaria o Paypal.
- Los pagos se realizarán de forma completa (en un solo pago). No se contempla el pago fraccionado, ni en cuotas.
- Se ha contemplado un **descuento del 10% del precio** de los módulos matriculados para aquellos que se encuentren en **situación de desempleo**. Al hacer la pre-inscripción, por favor indicadlo en el campo comentarios. Se os solicitará documentación oficial escaneada que así lo acredite. El simple envío de la documentación no garantiza el descuento, si ésta no puede ser verificada satisfactoriamente por parte de Securízame. En caso de ser aceptada, se te informará por correo electrónico de la cantidad final a transferir.

Otras ventajas

1. Securízame tiene un acuerdo de colaboración con la Asociación Nacional de Ciberseguridad y Pericia Tecnológica (ANCITE), por el cual, **sus socios contarán con un descuento del 10%** para acceso a todos los cursos del catálogo de formación propuesto por Securízame.
2. Para aquellos **socios de ANCITE**, que además se encuentren en una **situación de desempleo, el descuento pactado será del 15%**.
3. Igualmente, ambas organizaciones hemos acordado que para todos aquellos asistentes al curso, que quieran darse de alta en ANCITE posteriormente a la realización del mismo, ANCITE llevará a cabo un descuento equivalente al 10% del precio invertido en formación por el asistente. Por ejemplo: Si un alumno ha realizado un pack de 5 módulos del curso, cuyo coste son 1210 euros + 21% IVA, y quiere darse de alta en ANCITE, según el coste que le corresponda, siguiendo los criterios de ANCITE, se descontarán HASTA 121 euros en el alta para ese alumno. El máximo permitido en el descuento de alta en ANCITE será de 150 euros, que es el coste del alta. El dinero invertido en este curso de formación no podrá descontarse de la parte del mantenimiento anual de socio de ANCITE.
4. En el caso que el pago total para acceso a ANCITE sea inferior a los 150 euros (o al descuento que corresponda, como sucedería en el acceso como simpatizante), no se devolverá el dinero restante por parte de ANCITE ni Securízame.
5. En el caso de grupos, se dividirá el dinero invertido en formación, entre el número de alumnos del grupo de hasta 5 personas.
6. El acceso a ANCITE, está sujeto a los criterios de evaluación por parte de dicha organización, por lo que el alta no está garantizada en ninguno de los niveles de perito de ANCITE, por haber llevado a cabo el curso online de **Análisis Forense Digital en Profundidad**

CALENDARIO PROPUESTO

- Fechas de registro y pago: 23 de Enero al 13 de Febrero de 2015
- Fechas de pago con pago incrementado de un 10%: 14 al 20 de Febrero de 2015
- Impartición de curso: 23 de Febrero al 21 de Mayo de 2015

Las fechas estimadas para la impartición del curso son las siguientes:

Fechas por cada módulo:

- **Módulo I Informática Forense y Evidencia Digital:** Lunes 23 y Martes 24 de Febrero
- **Módulo II Delitos Informáticos y Criminalidad en Internet:** Miércoles 25 y Jueves 26 de Febrero
- **Módulo III Análisis Forense en Mac OS X:** Lunes 2, Martes 3, Miércoles 4 y Jueves 5 de Marzo
- **Módulo IV Análisis Forense en Windows:** Lunes 9, Martes 10, Miércoles 11 y Jueves 12 de Marzo
- **Módulo V Análisis de sistema de ficheros NTFS. Ficheros de Registro de Windows. Memoria en Windows. IOCs:** Lunes 16, Martes 17, Miércoles 18 y Viernes 20 de Marzo (El Jueves 19 de Marzo es Fiesta Nacional en España)
- **Módulo VI Análisis Forense en Linux:** Lunes 23, Martes 24, Miércoles 25 y Jueves 26 de Marzo
- **Módulo VII Análisis Forense de Discos SSD, Malware y Amenazas:** Viernes 27 de Marzo, Lunes 30 de Marzo, Martes 31 de Marzo y Miércoles 1 de Abril (el jueves 2 de Abril es Jueves Santo, Fiesta Nacional en España)
- **Módulo VIII Análisis Forense de Documentos:** Lunes 6, Martes 7, Miércoles 8 y Jueves 9 de Abril
- **Módulo IX Análisis Forense de virtualización y RAID:** Lunes 13, Martes 14, Miércoles 15 y Jueves 16 de Abril
- **Módulo X Análisis Forense en Redes, antiforense, correos electrónicos y VoIP:** Lunes 20,

Martes 21, Miércoles 22 y Jueves 23 de Abril

- **Módulo XI Análisis Forense de aplicaciones Microsoft: Active Directory, IIS, SQL Server, Exchange:** Lunes 27, Martes 28, Miércoles 29 y Jueves 30 de Abril
- **Módulo XII Análisis Forense de tarjetas SIM, Blackberry y Windows Phone:** Lunes 4, Martes 5, Miércoles 6 y Jueves 7 de Mayo
- **Módulo XIII Análisis Forense en IOS:** Lunes 11, Martes 12, Miércoles 13 y Jueves 14 de Mayo
- **Módulo XIV Análisis Forense en Android:** Lunes 18, Martes 19, Miércoles 20 y Jueves 21 de Mayo

DUDAS Y CONTACTO

- Para cualquier duda que pueda surgir referente a este curso, **DESPUÉS DE LEER** la información aquí detallada, contacta con nosotros en: formacion@securizame.com, indicando "Curso Forense 2015" como asunto del correo.

REGISTRO

- Si estás interesado en pre-registrarte a este curso (o alguno de sus módulos) hazlo a través del siguiente formulario.
- Al pre-registrarte te llegará un mensaje de confirmación a la cuenta de correo que hayas indicado.
- Por favor, comprueba a los pocos minutos de tu pre-registro, que el correo no ha llegado a la carpeta de "Correo No Deseado" o Spam.