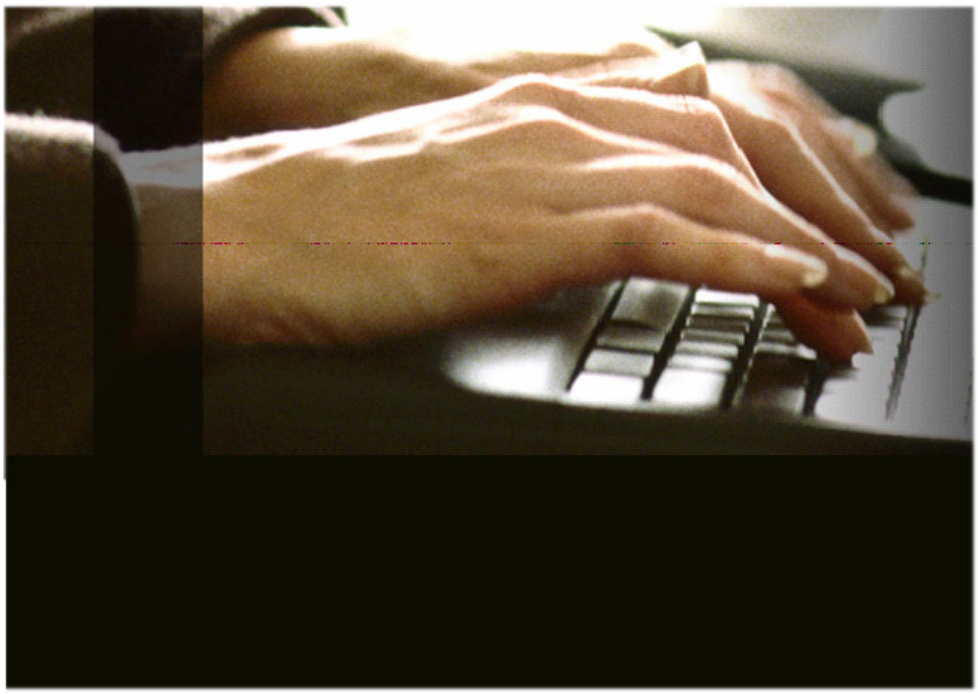
Curso 2007-2008

Master en
Tecnologías de Seguridad Informática

Titulación esCERT-UPC, 6a edición



LUGAR DE REALIZACIÓN	CALENDARIO	HORARIO	MATRÍCULA
En Barcelona esCert UPC Gran Capitana, 2-4 08034 Barcelona	22 de octubre a 27 de junio	L, X, V 18:30 – 21:30	5.400 euros

Participantes

Este Master ha sido diseñado para todos aquellos profesionales a quienes les interese profundizar en el conocimiento de las tecnologías de la seguridad informática y es especialmente recomendable para:

• Responsables informáticos

• Administradores de sistemas

• Profesionales que hayan de desarrollar tareas relacionadas con la seguridad de la información

• Evaluadores de seguridad en organizaciones y/o sistemas informáticos

• Gestores de proyectos en tecnologías de la información

Objetivos

El objetivo final se traduce en el hecho que el participante, al finalizar el curso, sea capaz de:

• Evaluar y mejorar la seguridad de sistemas informáticos.
• Obtener una visión completa y actual de los mecanismos de seguridad informática.
• Identificar y dimensionar amenazas en los sistemas informáticos.
• Hacer prácticas de configuración y administración de mecanismos de seguridad.
• Definir estrategias, políticas, estándares y procedimientos para la administración de sistemas de información.
• Garantizar la continuidad de negocio y los procesos empresariales vinculados a los sistemas de información

"El Master da una visión global sobre como gestionar la seguridad de los sistemas informáticos"

Contenido del curso

Visión general de la seguridad
•Introducción a la seguridad
•Panorama actual del mercado
•La seguridad y su justificación desde el punto de vista del negocio

Redes de comunicaciones
•Modelo OSI, Redes LAN, nivel 3-IP, nivel de transporte
-Segregación de redes: nivel 1, 2, 3, 4

Criptografía y sistemas de certificación digital
•Fundamentos
•Criptografia simétrica o asimétrica, funciones de Hash
•Estándares: X509, PKCS, FIPS, RFC.
•Aplicaciones:
-PKI, entidades de certificación.
-Terceras partes confiables: Time Stamping, OCSP
-Autenticación, single sing-on y gestión de claves
-Seguridad en Internet basada en criptografía: firma de codigo, ssh, ssl, ipsec, firma y cifreado de datos, pgp, etc.
•Criptografía actual:
-XML Signatura y XML Encryption
-Medios de pago: m-commerce, identrus, set.
-Protección de propiedad intelectual: Watermaking, fingerprinting
-Criptografía avanzada: blind signatura, privacidad, e-voting, e-gambling, e-cash
•Smart Card:
-Estándares y productos: ISO 7816, PKCS11, Crypographic and Memory Card, JavaCard, OpenCard, PS/SC
-Aplicaciones: DNI digital, autenticación, SSO

Seguridad en Redes
•VPN: IPSec
•Routers y protocolos
•Cisco IOS
•QoS
•VLAN y routing
•Protocolos en el ámbito de la aplicación
•Herramientas para el análisis de tráfico

Seguridad en redes sin hilos
•Comunicaciones sin hilos
•Wireless LAN: regulación (CNAF), OSI, 802.11, equipamientos
•Seguridad en sistemas de comunicación celulares: DECT;TETRA:GSM/GPRS y UMTS
•Seguridad en servicios móviles: localización, WAP, (WTLS, TLS, WIM, SIM) y MEXE (Java)
•Seguridad básica y avanzada en Wireless LAN
-Triangulo CIA
-Defense-in-depth
-Mecanismos 802.11: WEP, filtrado
-Futuro: WPA, 802.11 i: AES
-Amenazas: Spoofing, Dos, Suplantación, Man-in-the-middle
-Soluciones prácticas seguras: filtrado MAC, Activación WEP, Closing Node, EAP/802.1x, VPN
•Utilidades/Programas Wireless Lan
-Coexistencia: comunidades libres, wardriver/walkers.
-Utilidades y programas: Kismet, Netstunbler, FakeAP, Libpcap, Airsnort, WEPCrack, etc

Seguridad de los sistemas operativos: Windows
• Repaso histórico: DOS/3x, W9x/Me, NT/2000, Windows 2003/Xp
-Arquitecturas orientadas a la seguridad
-Modelo de red
-Active Directory
-Autenticación y encriptación de red, transporte y aplicación
-Protección de ficheros con EFS
-PKI en Windows
-Gestión de VPN
-Seguridad en servicios nativos
-Seguridad aplicada
-Construcción de un servidor seguro
•Tunning, mantenimiento de la seguridad: herramientas de ayuda
•Control, auditoria de sistemas
•Disponibilidad
•Gestión de parches y actualizaciones
•Scripting, WM

Seguridad de los sistemas operativos Unix/Linux
• Seguridad física: BIOS, Lilo, Grub, syslog
•Autenticación: Kerberos, LDAP, PAM, NIS
•Discos y sistemas de ficheros: Cuota, ACLS, RAID, LVM, ext3 JFS, ReiserFS

•Seguridad de servicios: inetd, xinitd, iptables, tcp wrapper, Seguid, SeGID
•Gestión i monitorización: shells, logs
•Seguridad del kernel

Contenido del curso

Intrusiones en sistemas informáticos
•Gestión de un test de intrusión
•Integración BS7799 / auditoriatécnica
•Limitaciones del osstm
•Metodología
-Obtención de información
-Obtención de acceso
-Escala de privilegios
-Evaluación de objetivos
-Metástasis de una intrusión
•Herramientas
-Análisis: anonimizadores, escáneres
-Explotación: exploits, web, contraseñas
-Gestión: rootkits, troyanos.
•Buffer overforws, exploits y shellcodes
•Análisis de aplicaciones web
•Eliminación y análisis de rastros

Seguridad de aplicaciones. Programación segura
• Principios de Seguridad
•Gestión de la Seguridad en el ciclo de vida del desarrollo del software (SSDLC, Secure Software Development Life Cycle).
-Integración de las vulnerabilidades de la gestión de errores.
-Quality Assurance.
-Auditoria.
•Técnicas de Programación Segura
-Autentificación, autorización, validación de datos, motes canónicos, criptografía, conexiones con bases de datos, registro de operaciones, control de sesiones y cookies, objetos compilados, control de errores y excepciones.

• **Vulnerabilidades en las aplicaciones.**
•Errores comunes en la programación, inyección de comandos, desbordamientos, revelación de información, condiciones de carrera, denegación de servicio, bugs o errores de formato
•Vulnerabilidades en las aplicaciones. Caso Web.
-Revelación información, directory traversal, secuestro de sesiones, cross site scripting, inyección SQL, inyección de comandos, HTTP Splitting, manipulación de: variables, cookies y campos ocultos, denegación de servicio y desbordamientos de búfer
•Seguridad en la parte cliente
•Vulnerabilidades en Web Services
•Vulnerabilidades en Ajax

Mecanismos de protección
•NAT, DMZ
•Firewall: de paquete, de aplicación, proxies
•Productos comerciales
•Linux/Iptables
•VPN
•Alta disponibilidad

Mecanismos de detección
•Intrusión Detection Systems
•HIDS: trypwire
•NIDS: Snort
•Honeypots
•Gestión de logotipos
•Antivirus
•Computer forensics
-La delincuencia en la sociedad de la información
-El sistema judicial
-Los peritos: forenses digitales
-La prueba pericial y la cadena de custodia
-Las formas de actuar
-El examen pericial: el detective forense

Planificación de la seguridad informática
•Análisis de riesgos
•Política de seguridad
•UNE/ISO 17799
•Planes de contingencia
•Auditoria

Legislación
•Nuevas tecnologías: ámbito legal
•Legislación nacional y europea
-LOPD
-Comercio electrónico
-Propiedad intelectual
-Firma electrónica
-LSSIce
-Derecho laboral
-Civil/Mercantil: identidades, nombres de dominio
Penal: ciberdelitos
•Implicaciones legales para la empresa
•Riesgos de no-adaptación a la legislación
•Acciones legales

Proyecto de seguridad

"La demanda en el mercado laboral de profesionales con formación específica en seguridad informática sigue una fuerte tendencia al alza"

escert.upc.edu

Master en Tecnologías de Seguridad Informática 6 edición

CALENDARIO

L, X, V
18:30 – 21:30

22 de octubre al
27 de junio

IMPORTE DE LA MATRÍCULA

5.400 euros

Información y admisiones

Las sesiones informativas sirven para exponer, de una manera directa, los contenidos y la aplicación de cada módulo.
Para acceder al curso hace falta presentar la solicitud de admisión y, si fuera necesario, mantener una entrevista personal con el coordinador del Master

Próximas sesiones informativas:

Miércoles 19 de septiembre a las 19:00 horas

Miércoles 26 de septiembre a las 19:00 horas

Información

Para más información pueden dirigir las consultas sobre el programa, el proceso de admisión y confirmar la asistencia a las sesiones informativas al coordinador del master a:
esCert UPC
Gran Capitán 2-4,
08034 Barcelona
TEL. 93 230 35 00

De lunes a viernes
De 9:00 a 14:00 horas y
de 16:00 a 19:00

O bien por correo electrónico a la dirección:

master@escert.upc.edu

A principios de la década de los noventa surge en Europa una iniciativa para la creación de Equipos de Respuestas a Incidentes de Seguridad en Redes de ordenadores.

A finales del 1994, se crea EsCERT-UPC (Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas) como primer centro español dedicado a asesorar, prevenir y resolver incidencias de seguridad en entornos telemáticos y especialmente en:
•Informar sobre vulnerabilidades de seguridad y amenazas.
•Divulgar y poner a disposición de la sociedad de la información información que permita prevenir y resolver incidentes de seguridad.
•Educar a la comunidad en general sobre temas de seguridad.

escert.upc.edu