



# INESEM

BUSINESS SCHOOL

## ***Máster en Auditoría Informática + Titulación Universitaria***

**+ Información Gratis**

titulación de formación continua bonificada expedida por el instituto europeo de estudios empresariales

# Máster en Auditoría Informática + Titulación Universitaria

**duración total:** 1.500 horas

**horas teleformación:** 750 horas

**precio:** 0 € \*

**modalidad:** Online

\* hasta 100 % bonificable para trabajadores.

## descripción

Este Master en Auditoría Informática le ofrece una formación especializada en la materia. Debemos saber que hoy en día la seguridad informática es un tema muy importante y sensible, que abarca un gran conjunto de aspectos en continuo cambio y constante evolución, que exige que los profesionales informáticos posean conocimientos totalmente actualizados. Con la realización del presente Master en Auditoría Informática el alumno aprenderá los conocimientos necesarios para auditar redes de comunicación y sistemas informáticos.



## *a quién va dirigido*

Todos aquellos trabajadores y profesionales en activo que deseen adquirir o perfeccionar sus conocimientos técnicos en este área.

## *objetivos*

- Analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático implantando aquellas que se adecuen a las especificaciones de seguridad informática.
- Aplicar procedimientos relativos al cumplimiento de la normativa legal vigente.
- Planificar y aplicar medidas de seguridad para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental.
- Dotar a los alumnos de los lineamientos básicos para la aplicación de la Norma ISO/IEC 27001 dentro de su organización.
- Ofrecer las pautas para implementar un sistema de gestión de seguridad de información basado en el estándar ISO/IEC 27001 siguiendo los controles recomendados por el estándar ISO/IEC 27002 en sus respectivas cláusulas.
- Exponer y explicar una serie de buenas prácticas para conseguir la seguridad de la información.
- Analizar los planes de implantación de la organización para identificar los elementos del sistema implicados y los niveles de seguridad a implementar.
- Analizar e implementar los mecanismos de acceso físicos y lógicos a los servidores según especificaciones de seguridad.
- Evaluar la función y necesidad de cada servicio en ejecución en el servidor según las especificaciones de seguridad.
- Instalar, configurar y administrar un cortafuegos de servidor con las características necesarias según especificaciones de seguridad.
- Planificar e implantar los sistemas de detección de intrusos según las normas de seguridad.
- Aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada.
- Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada.
- Evaluar las técnicas de cifrado existentes para escoger la necesaria en función de los requisitos de seguridad exigidos.
- Implantar servicios y técnicas criptográficas en aquellos servicios que lo requieran según especificaciones de seguridad informática.
- Utilizar sistemas de certificados digitales en aquellas comunicaciones que requieran integridad y confidencialidad según especificaciones de seguridad.
- Diseñar e implantar servicios de certificación digital según necesidades de explotación y de seguridad informática.
- Conocer la definición precisa de los diferentes tipos de hackers y de sus objetivos.
- Aprender sobre la metodología de un ataque y los medios para identificar las vulnerabilidades o fallos de seguridad a través de los que introducirse en un sistema.
- Conocer los fallos físicos, que permiten un acceso directo a ordenadores, y los fallos de red y Wi-Fi se presentan e ilustran cada uno con propuestas de contramedidas.
- Saber sobre el Cloud Computing (su historia, su funcionamiento) para dominar mejor la seguridad.
- Tener en cuenta la seguridad en la web y los fallos actuales identificados gracias a la ayuda de herramientas que el lector puede implantar fácilmente en sus propios sistemas.
- Identificar siempre los posibles fallos para establecer después la estrategia de protección adecuada.
- Conocer algunos ejemplos los fallos de sistemas en Windows o Linux y los fallos de aplicación, para familiarizarse con el lenguaje ensamblador y comprender mejor las posibilidades de ataque.

## *para qué te prepara*

Este Master en Auditoría Informática le prepara para analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático implantando aquellas que se adecuen a las especificaciones de seguridad informática, aplicar procedimientos relativos al cumplimiento de la normativa legal vigente y planificar y aplicar medidas de seguridad para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental.

## *salidas laborales*

Desarrolla su actividad profesional en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia.

## titulación

Una vez finalizado el curso, el alumno recibirá por parte de INESEM vía correo postal, la Titulación Oficial que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/máster, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Instituto Europeo de Estudios Empresariales).



### INSTITUTO EUROPEO DE ESTUDIOS EMPRESARIALES

como centro de Formación acreditado para la impartición a nivel nacional de formación  
EXPIDE LA SIGUIENTE TITULACIÓN

#### NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXX ha superado los estudios correspondientes de

#### Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación INESEM en la convocatoria de XXXX  
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX- XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en  
Granada, a (día) de (mes) de (año)

La dirección General

MARIA MORENO HIDALGO

Firma del alumno/a

Sello



NOMBRE DEL ALUMNO/A



## forma de bonificación

- Mediante descuento directo en el TC1, a cargo de los seguros sociales que la empresa paga cada mes a la Seguridad Social.

## metodología

El alumno comienza su andadura en INESEM a través del Campus Virtual. Con nuestra metodología de aprendizaje online, el alumno debe avanzar a lo largo de las unidades didácticas del itinerario formativo, así como realizar las actividades y autoevaluaciones correspondientes. Al final del itinerario, el alumno se encontrará con el examen final, debiendo contestar correctamente un mínimo del 75% de las cuestiones planteadas para poder obtener el título.

Nuestro equipo docente y un tutor especializado harán un seguimiento exhaustivo, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

El alumno dispone de un espacio donde gestionar todos sus trámites administrativos, la Secretaría Virtual, y de un lugar de encuentro, Comunidad INESEM, donde fomentar su proceso de aprendizaje que enriquecerá su desarrollo profesional.

## materiales didácticos

- Manual teórico 'Gestión de Incidentes de Seguridad Informática'
- Manual teórico 'Sistemas Seguros de Acceso y Transmisión de Datos'
- Manual teórico 'Seguridad en Equipos Informáticos'
- Manual teórico 'Auditoría Informática'
- Manual teórico 'Sistema de Gestión de Seguridad de la Información UNE-ISO/IEC 27001:2017'



## profesorado y servicio de tutorías

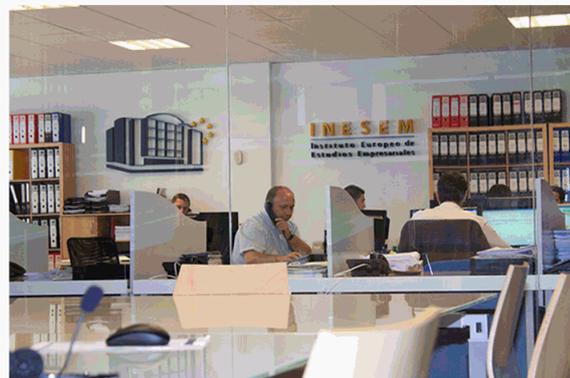
Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “Guía del Alumno” entregado junto al resto de materiales de estudio. Contamos con una extensa plantilla de profesores especializados en las distintas áreas formativas, con una amplia experiencia en el ámbito docente.

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas, así como solicitar información complementaria, fuentes bibliográficas y asesoramiento profesional. Podrá hacerlo de las siguientes formas:

- **Por e-mail:** El alumno podrá enviar sus dudas y consultas a cualquier hora y obtendrá respuesta en un plazo máximo de 48 horas.

- **Por teléfono:** Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.

- **A través del Campus Virtual:** El alumno/a puede contactar y enviar sus consultas a través del mismo, pudiendo tener acceso a Secretaría, agilizando cualquier proceso administrativo así como disponer de toda su documentación



### *plazo de finalización*

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la misma duración del curso. Existe por tanto un calendario formativo con una fecha de inicio y una fecha de fin.

### *campus virtual online*

especialmente dirigido a los alumnos matriculados en cursos de modalidad online, el campus virtual de inesem ofrece contenidos multimedia de alta calidad y ejercicios interactivos.

### *comunidad*

servicio gratuito que permitirá al alumno formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: becas, descuentos y promociones en formación, viajes al extranjero para aprender idiomas...

### *revista digital*

el alumno podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, etc.

### *secretaría*

Este sistema comunica al alumno directamente con nuestros asistentes, agilizando todo el proceso de matriculación, envío de documentación y solución de cualquier incidencia.

Además, a través de nuestro gestor documental, el alumno puede disponer de todos sus documentos, controlar las fechas de envío, finalización de sus acciones formativas y todo lo relacionado con la parte administrativa de sus cursos, teniendo la posibilidad de realizar un seguimiento personal de todos sus trámites con INESEM

**programa formativo**

# PARTE 1. AUDITORÍA INFORMÁTICA

## UNIDAD DIDÁCTICA 1. AUDITORÍA INFORMÁTICA

1. Código deontológico de la función de auditoría
2. Relación de los distintos tipos de auditoría en el marco de los sistemas de información
3. Criterios a seguir para la composición del equipo auditor
4. Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
5. Tipos de muestreo a aplicar durante el proceso de auditoría
6. Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
7. Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
8. Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
9. Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

## UNIDAD DIDÁCTICA 2. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

1. Principios generales de protección de datos de carácter personal
2. Normativa europea recogida en la directiva 95/46/CE
3. Normativa nacional recogida en el código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 4. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
4. Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 6. Guía para la realización de la auditoría bienal obligatoria de ley orgánica

## UNIDAD DIDÁCTICA 3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS INFORMÁTICOS.

1. Introducción al análisis de riesgos
2. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
3. Particularidades de los distintos tipos de código malicioso
4. Principales elementos del análisis de riesgos y sus modelos de relaciones
5. Metodologías cualitativas y cuantitativas de análisis de riesgos
6. Identificación de los activos involucrados en el análisis de riesgos y su valoración
7. Identificación de las amenazas que pueden afectar a los activos identificados previamente
8. Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
9. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
10. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y efecto sobre las vulnerabilidades y amenazas
11. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializar
12. Determinación de la probabilidad e impacto de materialización de los escenarios
13. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
14. Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
15. Relación de las distintas alternativas de gestión de riesgos
16. Guía para la elaboración del plan de gestión de riesgos
17. Exposición de la metodología NIST SP 18. Exposición de la metodología Magerit

## UNIDAD DIDÁCTICA 4. USO DE HERRAMIENTAS PARA LA AUDITORÍA INFORMÁTICA

1. Herramientas del sistema operativo tipo Ping, Traceroute, etc.
2. Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
3. Herramientas de análisis de vulnerabilidades tipo Nessus

4. Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.
5. Analizadores de páginas web tipo Acunetix, Sucuri, etc.
6. Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

#### **UNIDAD DIDÁCTICA 5. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS**

1. Principios generales de cortafuegos
2. Componentes de un cortafuegos de red
3. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
4. Arquitecturas de cortafuegos de red
5. Otras arquitecturas de cortafuegos de red

#### **UNIDAD DIDÁCTICA 6. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA INFORMÁTICA**

1. Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
2. Guía para la elaboración del plan de auditoría
3. Guía para las pruebas de auditoría
4. Guía para la elaboración del informe de auditoría

## **PARTE 2. GESTIÓN DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN ISO 27001**

#### **UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD Y SOCIEDAD DE LA INFORMACIÓN**

1. ¿Qué es la ciberseguridad?
2. La sociedad de la información
3. Diseño, desarrollo e implantación
4. Factores de éxito en la seguridad de la información
5. Soluciones de Ciberseguridad y Ciberinteligencia CCN-CERT

#### **UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)**

1. Estándares y Normas Internacionales sobre los SGSI. ISO 27001 e ISO 27002
2. Legislación: Leyes aplicables a los SGSI

#### **UNIDAD DIDÁCTICA 3. INTRODUCCIÓN A LA NIS2**

1. Historia y evolución de la NIS2
2. Objetivos y alcance de la NIS2
3. Diferencias entre NIS1 y NIS2
4. Sectores críticos afectados por la NIS2

#### **UNIDAD DIDÁCTICA 4. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS**

1. Plan de implantación del SGSI
2. Análisis de riesgos
3. Gestión de riesgos

#### **UNIDAD DIDÁCTICA 5. IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD EN LA ORGANIZACIÓN**

1. Contexto
2. Liderazgo
3. Planificación
4. Soporte 213

#### **UNIDAD DIDÁCTICA 6. SEGUIMIENTO DE LA IMPLANTACIÓN DEL SISTEMA**

1. Operación
2. Evaluación del desempeño
3. Mejora

#### **UNIDAD DIDÁCTICA 7. AUDITORÍA DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN POR LA DIRECCIÓN**

1. El porqué de la auditoría
2. La auditoría interna

3.El proceso de certificación

### **UNIDAD DIDÁCTICA 8. REVISIÓN POR LA DIRECCIÓN Y MEJORA DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN**

- 1.Revisión del sistema de gestión de la información por la dirección
- 2.Mejora del sistema de gestión de la seguridad de la información

### **UNIDAD DIDÁCTICA 9. GUÍAS DE SEGURIDAD: NORMATIVAS Y BUENAS PRÁCTICAS**

- 1.Introducción a las guías de seguridad CCN-STIC
- 2.CCN-STIC-800 Glosario de términos y abreviaturas del ENS
- 3.CCN-STIC-801 Responsabilidades y funciones en el ENS
- 4.CCN-STIC-802 Auditoría del ENS
- 5.CCN-STIC-803 Valoración de Sistemas en el ENS
- 6.CCN-STIC-804 Medidas de implantación del ENS
- 7.CCN-STIC-805 Política de seguridad de la información
- 8.CCN-STIC-806 Plan de adecuación al ENS
- 9.CCN-STIC-807 Criptología de empleo en el ENS
- 10.CCN-STIC-808 Verificación del cumplimiento del ENS

## **PARTE 3. SEGURIDAD EN EQUIPOS INFORMÁTICOS**

### **UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS**

- 1.Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
- 2.Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
- 3.Salvaguardas y tecnologías de seguridad más habituales
- 4.La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

### **UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO**

- 1.Identificación de procesos de negocio soportados por sistemas de información
- 2.Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
- 3.Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

### **UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS**

- 1.Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
- 2 Metodologías comúnmente aceptadas de identificación y análisis de riesgos
- 3.Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

### **UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD**

- 1.Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.
- 2.Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
- 3.Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

### **UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

- 1.Principios generales de protección de datos de carácter personal
- 2.Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
- 3.Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- 4.Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

### **UNIDAD DIDÁCTICA 6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS**

- 1.Determinación de los perímetros de seguridad física
- 2.Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
- 3.Criterios de seguridad para el emplazamiento físico de los sistemas informáticos

- 4.Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
- 5.Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
- 6.Elaboración de la normativa de seguridad física e industrial para la organización
- 7.Sistemas de ficheros más frecuentemente utilizados
- 8.Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
- 9.Configuración de políticas y directivas del directorio de usuarios
- 10.Establecimiento de las listas de control de acceso (ACLs) a ficheros
- 11.Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
- 12.Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
- 13.Sistemas de autenticación de usuarios débiles, fuertes y biométricos
- 14.Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
- 15.Elaboración de la normativa de control de accesos a los sistemas informáticos

#### **UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS**

- 1.Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
- 2.Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
- 3.Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

#### **UNIDAD DIDÁCTICA 8. ROBUSTECIMIENTO DE SISTEMAS**

- 1.Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información
- 2.Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
- 3.Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
- 4.Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
- 5.Actualización de parches de seguridad de los sistemas informáticos
- 6.Protección de los sistemas de información frente a código malicioso
- 7.Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
- 8.Monitorización de la seguridad y el uso adecuado de los sistemas de información

#### **UNIDAD DIDÁCTICA 9. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS**

- 1.Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- 2.Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
- 3.Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
- 4.Definición de reglas de corte en los cortafuegos
- 5.Relación de los registros de auditoría del cortafuegos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
- 6.Establecimiento de la monitorización y pruebas del cortafuegos

## **PARTE 4. GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA**

#### **UNIDAD DIDÁCTICA 1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)**

- 1.Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
- 2.Identificación y caracterización de los datos de funcionamiento del sistema
- 3.Arquitecturas más frecuentes de los sistemas de detección de intrusos
- 4.Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
- 5.Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

#### **UNIDAD DIDÁCTICA 2. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS**

- 1.Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio.
- 2.Definición de políticas de corte de intentos de intrusión en los IDS/IPS

3. Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS

4. Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión

5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

#### **UNIDAD DIDÁCTICA 3. CONTROL DE CÓDIGO MALICIOSO**

1. Sistemas de detección y contención de código malicioso

2. Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar

3. Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso

4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso

5. Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso

7. Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

#### **UNIDAD DIDÁCTICA 4. RESPUESTA ANTE INCIDENTES DE SEGURIDAD**

1. Procedimiento de recolección de información relacionada con incidentes de seguridad

2. Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad

3. Proceso de verificación de la intrusión

4. Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

#### **UNIDAD DIDÁCTICA 5. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN**

1. Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones

2. Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial

3. Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente

4. Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones

5. Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo

6. Establecimiento del nivel de intervención requerido en función del impacto previsible

7. Guía para la investigación y diagnóstico del incidente de intento de intrusión o infecciones

8. Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección

9. Proceso para la comunicación del incidente a terceros, si procede

10. Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

#### **UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE INFORMÁTICO**

1. Conceptos generales y objetivos del análisis forense

2. Exposición del Principio de Lockard

3. Guía para la recogida de evidencias electrónicas:

4. Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios oculta información oculta del sistema y la recuperación de ficheros borrados

5. Guía para la selección de las herramientas de análisis forense

## **PARTE 5. SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS**

#### **UNIDAD DIDÁCTICA 1. CRIPTOGRAFÍA**

1. Perspectiva histórica y objetivos de la criptografía

2. Teoría de la información

3. Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos
4. Elementos fundamentales de la criptografía de clave privada y de clave pública
5. Características y atributos de los certificados digitales
6. Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente
7. Algoritmos criptográficos más frecuentemente utilizados
8. Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización
9. Elementos fundamentales de las funciones resumen y los criterios para su utilización
10. Requerimientos legales incluidos en la ley 59/2003, de 19 de diciembre, de firma electrónica
11. Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización
12. Criterios para la utilización de técnicas de cifrado de flujo y de bloque
13. Protocolos de intercambio de claves
14. Uso de herramientas de cifrado tipo PGP, GPG o CryptoLoop

#### **UNIDAD DIDÁCTICA 2. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)**

1. Identificación de los componentes de una PKI y su modelo de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructura de gestión de privilegios (PMI)
7. Campos de certificados de atributos, incluyen la descripción de sus usos habituales y la relación con los certificados digitales
8. Aplicaciones que se apoyan en la existencia de una PKI

#### **UNIDAD DIDÁCTICA 3. COMUNICACIONES SEGURAS**

1. Definición, finalidad y funcionalidad de redes privadas virtuales
2. Protocolo IPsec
3. Protocolos SSL y SSH
4. Sistemas SSL VPN
5. Túneles cifrados
6. Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN

## **PARTE 6. ETHICAL HACKING**

#### **UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LOS ATAQUES Y AL HACKING ÉTICO**

1. Introducción a la seguridad informática
2. El hacking ético
3. La importancia del conocimiento del enemigo
4. Seleccionar a la víctima
5. El ataque informático
6. Acceso a los sistemas y su seguridad
7. Análisis del ataque y seguridad

#### **UNIDAD DIDÁCTICA 2. SOCIAL ENGINEERING**

1. Introducción e historia del Social Engineering
2. La importancia de la Ingeniería social
3. Defensa ante la Ingeniería social

#### **UNIDAD DIDÁCTICA 3. LOS FALLOS FÍSICOS EN EL ETHICAL HACKING Y LAS PRUEBAS DEL ATAQUE**

1. Introducción
2. Ataque de Acceso físico directo al ordenador
3. El hacking ético
4. Lectura de logs de acceso y recopilación de información

#### **UNIDAD DIDÁCTICA 4. LA SEGURIDAD EN LA RED INFORMÁTICA**

- 1.Introducción a la seguridad en redes
- 2.Protocolo TCP/IP
- 3.IPv6
- 4.Herramientas prácticas para el análisis del tráfico en la red
- 5.Ataques Sniffing
- 6.Ataques DoS y DDoS
- 7.Ataques Robo de sesión TCP (HIJACKING) y Spoofing de IP
- 8.Ataques Man In The Middle (MITM).
- 9.Seguridad Wi-Fi
- 10.IP over DNS
- 11.La telefonía IP

#### **UNIDAD DIDÁCTICA 5. LOS FALLOS EN LOS SISTEMAS OPERATIVOS Y WEB**

- 1.Usuarios, grupos y permisos
- 2.Contraseñas
- 3.Virtualización de sistemas operativos
- 4.Procesos del sistema operativo
- 5.El arranque
- 6.Hibernación
- 7.Las RPC
- 8.Logs, actualizaciones y copias de seguridad
- 9.Tecnología WEB Cliente - Servidor
- 10.Seguridad WEB
- 11.SQL Injection
- 12.Seguridad CAPTCHA
- 13.Seguridad Akismet
- 14.Consejos de seguridad WEB

#### **UNIDAD DIDÁCTICA 6. ASPECTOS INTRODUCTORIOS DEL CLOUD COMPUTING**

- 1.Orígenes del cloud computing
- 2.Qué es cloud computing
  - 1.- Definición de cloud computing
- 3.Características del cloud computing
- 4.La nube y los negocios
  - 1.- Beneficios específicos
- 5.Modelos básicos en la nube

#### **UNIDAD DIDÁCTICA 7. CONCEPTOS AVANZADOS Y ALTA SEGURIDAD DE CLOUD COMPUTING**

- 1.Interoperabilidad en la nube
  - 1.- Recomendaciones para garantizar la interoperabilidad en la nube
- 2.Centro de procesamiento de datos y operaciones
- 3.Cifrado y gestión de claves
- 4.Gestión de identidades

#### **UNIDAD DIDÁCTICA 8. SEGURIDAD, AUDITORÍA Y CUMPLIMIENTO EN LA NUBE**

- 1.Introducción
- 2.Gestión de riesgos en el negocio
  - 1.- Recomendaciones para el gobierno
  - 2.- Recomendaciones para una correcta gestión de riesgos
- 3.Cuestiones legales básicas. eDiscovery
- 4.Las auditorías de seguridad y calidad en cloud computing
- 5.El ciclo de vida de la información
  - 1.- Recomendaciones sobre seguridad en el ciclo de vida de la información

#### **UNIDAD DIDÁCTICA 9. CARACTERÍSTICAS DE SEGURIDAD EN LA PUBLICACIÓN DE PÁGINAS WEB**

- 1.Seguridad en distintos sistemas de archivos.

- 1.- Sistema operativo Linux.
  - 2.- Sistema operativo Windows.
  - 3.- Otros sistemas operativos.
2. Permisos de acceso.
- 1.- Tipos de accesos
  - 2.- Elección del tipo de acceso
  - 3.- Implementación de accesos
3. Órdenes de creación, modificación y borrado.
- 1.- Descripción de órdenes en distintos sistemas
  - 2.- Implementación y comprobación de las distintas órdenes.

#### **UNIDAD DIDÁCTICA 10. PRUEBAS Y VERIFICACIÓN DE PÁGINAS WEB**

1. Técnicas de verificación.
- 1.- Verificar en base a criterios de calidad.
  - 2.- Verificar en base a criterios de usabilidad.
2. Herramientas de depuración para distintos navegadores.
- 1.- Herramientas para Mozilla.
  - 2.- Herramientas para Internet Explorer.
  - 3.- Herramientas para Opera.
  - 4.- Creación y utilización de funciones de depuración.
  - 5.- Otras herramientas.
3. Navegadores: tipos y «plug-ins».
- 1.- Descripción de complementos.
  - 2.- Complementos para imágenes.
  - 3.- Complementos para música.
  - 4.- Complementos para vídeo.
  - 5.- Complementos para contenidos.
  - 6.- Máquinas virtuales.

#### **UNIDAD DIDÁCTICA 11. LOS FALLOS DE APLICACIÓN**

1. Introducción en los fallos de aplicación
2. Los conceptos de código ensamblador y su seguridad y estabilidad
3. La mejora y el concepto de shellcodes
4. Buffer overflow
5. Fallos de seguridad en Windows