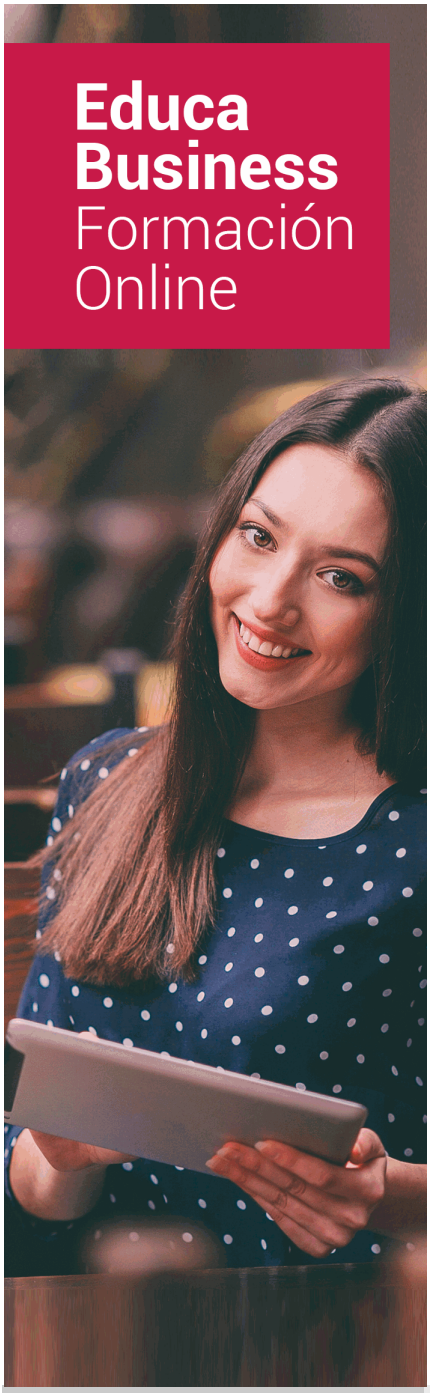


EDUCA BUSINESS SCHOOL

FORMACIÓN ONLINE

Titulación certificada por
EDUCA BUSINESS SCHOOL

Master En Seguridad Informática + Perito Informático Forense



SOBRE EDUCA

Educa Business School es una Escuela de Negocios Virtual, con reconocimiento oficial, acreditada para impartir formación superior de postgrado, (como formación complementaria y formación para el empleo), a través de cursos universitarios online y cursos / másteres online con título propio.

NOS COMPROMETEMOS CON LA CALIDAD

Educa Business School es miembro de pleno derecho en la Comisión Internacional de Educación a Distancia, (con estatuto consultivo de categoría especial del Consejo Económico y Social de NACIONES UNIDAS), y cuenta con **el Certificado de Calidad de la Asociación Española de Normalización y Certificación** (AENOR) de acuerdo a la normativa ISO 9001, mediante la cual se Certifican en Calidad todas las acciones

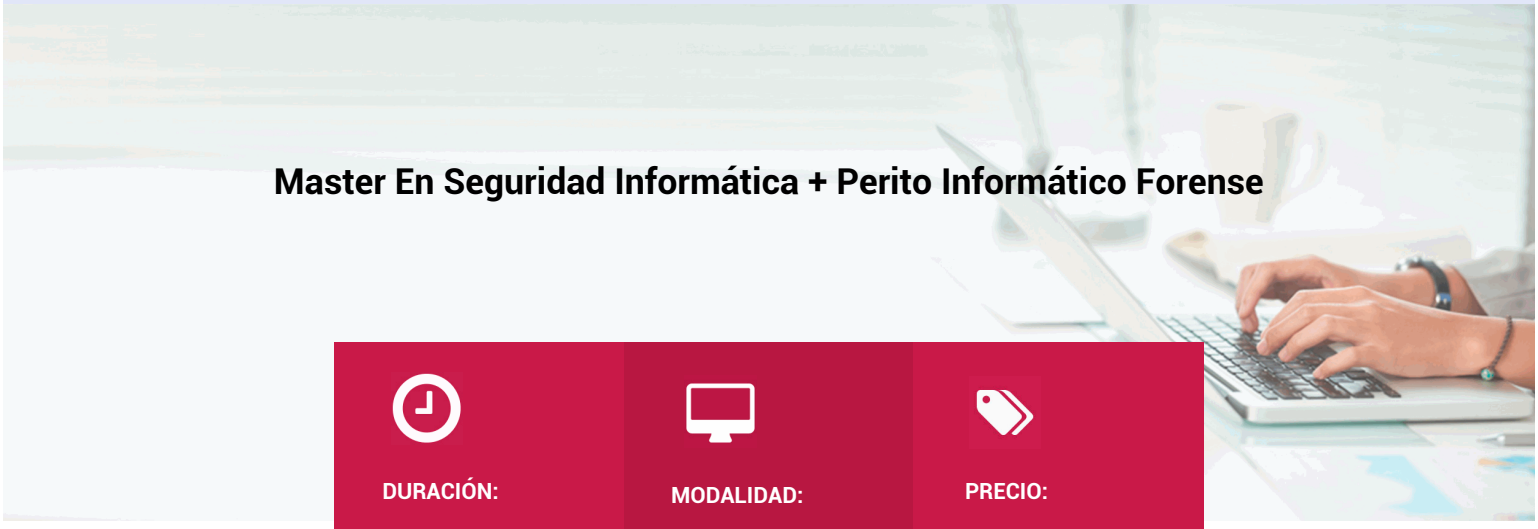
Los contenidos didácticos de Educa están elaborados, por tanto, bajo los parámetros de formación actual, teniendo en cuenta un sistema innovador con tutoría personalizada.

Como centro autorizado para la impartición de formación continua para personal trabajador, l**os cursos de Educa pueden bonificarse, además de ofrecer un amplio catálogo de cursos homologados y baremables en Oposiciones**, dentro de la Administración Pública.Educa dirige parte de sus ingresos a la sostenibilidad ambiental y ciudadana, lo que la consolida como una Empresa Socialmente Responsable.

Las Titulaciones acreditadas por Educa Business School pueden **certificarse con la Apostilla de La Haya** (CERTIFICACIÓN OFICIAL DE CARÁCTER INTERNACIONAL que le da validez a las Titulaciones Oficiales en más de 160 países de todo el mundo).

Años de experiencia avalan el trabajo docente desarrollado en Educa, basándose en una metodología completamente a la vanguardia educativa

Desde Educa, hemos reinventado la formación online, de manera que nuestro alumnado pueda ir superando de forma flexible cada una de las acciones formativas con las que contamos, en todas las áreas del saber, mediante el apoyo incondicional de tutores/as con experiencia en cada materia, y la garantía de aprender los conceptos realmente demandados en el mercado laboral.



Master En Seguridad Informática + Perito Informático Forense

DURACIÓN:
900 horas

MODALIDAD:
Online

PRECIO:
1.200 €
Incluye materiales didácticos, titulación y gastos de envío.

CENTRO DE FORMACIÓN:
Educa Business School

Titulación

Titulación Expedida por EDUCA BUSINESS SCHOOL como Escuela de Negocios Acreditada para la Impartición de Formación Superior de Postgrado, con Validez Profesional a Nivel Internacional

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

Esta titulación incluirá el nombre del curso/master, 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 (Euroinnova Formación, Instituto Europeo de Estudios Empresariales y Comisión Internacional para la Formación a Distancia de la



EDUCA BUSINESS SCHOOL

como Escuela de Negocios de Formación Superior de Postgrado

EXPIDE EL PRESENTE TÍTULO PROPIO

NOMBRE DEL ALUMNO

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

Nombre de la Acción Formativa

de 600 horas, perteneciente al Plan de Formación EUROINNOVA en la convocatoria de 2015
Y para que surtan los efectos pertinentes queda registrado con Número de Expediente EURO/XXXX-XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en
Granada, a 1 de Diciembre de 2015

La Dirección General

JESÚS MORENO HIDALGO

SELLO

El/La Interesado/a

NOMBRE DEL ALUMNO/A

Descripción

Este Master en Seguridad Informática le ofrece una formación especializada en al materia. Este Master MBA en Seguridad Informática: IT Security Manager le ofrece una formación especializada en la materia. La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.
Este Perito Informático Forense le ofrece una formación especializada en al materia. 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 curso el alumno aprenderá los conocimientos necesarios para actuar como Perito Judicial en los ámbitos de Seguridad Informática. Este Curso de Perito Judicial contiene todo lo necesario para poder ejercer como Perito Judicial, desarrollando con éxito esta actividad, además una vez obtenido el diploma va a poder tramitar el alta en los Juzgados que el designe. Este curso de Perito Judicial incluye toda la legislación actual en el mundo del Peritaje.

Objetivos

- Conocer los ámbitos de actuación de un Perito Judicial en Seguridad Informática.
- Asegurar equipos informáticos
- Auditar redes de comunicación y sistemas informáticos
- Detectar y responder ante incidentes de seguridad.
- Diseñar e implementar sistemas seguros de acceso y transmisión de datos
- Gestionar servicios en el sistema informático
- Conocer el concepto y modelos de seguridad, los tipos de control de acceso, autentificación de datos y posibles ataques a los que pueden estar sometidos los sistemas informáticos.
- Clasificar los componentes que se utilizan en el montaje de los equipos microinformáticos, identificando sus parámetros funcionales y características, teniendo en cuenta sus especificaciones técnicas.
- Verificar los equipos microinformáticos montados y asegurar su funcionalidad, estabilidad, seguridad y rendimiento, de acuerdo a las especificaciones dadas.
- Llevar a cabo la instalación y configuración de redes domésticas y pequeñas redes de empresa.
- Clasificar los componentes que se utilizan en el montaje de los equipos microinformáticos, identificando sus parámetros funcionales y características, teniendo en cuenta sus especificaciones técnicas.
- Instalar los elementos que componen los equipos microinformáticos, aplicando criterios de calidad, eficiencia y seguridad, de acuerdo a especificaciones técnicas recibidas.
- Verificar los equipos microinformáticos montados y asegurar su funcionalidad, estabilidad, seguridad y rendimiento, de acuerdo a las especificaciones dadas.
- Ampliar equipos microinformáticos para añadir nuevas funcionalidades al sistema, de acuerdo a las especificaciones establecidas.
- Conocer los ámbitos de actuación de un Perito Judicial en Seguridad Informática.
- Asegurar equipos informáticos
- Auditar redes de comunicación y sistemas informáticos
- Detectar y responder ante incidentes de seguridad.
- Diseñar e implementar sistemas seguros de acceso y transmisión de datos
- Gestionar servicios en el sistema informático

A quién va dirigido

Este Master en Seguridad Informática está dirigido a todos aquellos profesionales de esta rama profesional. Además Este Master MBA en Seguridad Informática: IT Security Manager está dirigido a todas aquellas personas que quieran formarse en el mundo de la seguridad informática, conociendo los sistema de protección en los sistemas informáticos que garanticen desde la privacidad de los datos hasta la seguridad en las transacciones de información. No obstante tal y como establece la LEY de Enjuiciamiento Civil en su Artículo 340.1: Los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste. Si se tratare de materias que no estén comprendidas en títulos profesionales oficiales, habrán de ser nombrados entre personas entendidas en aquellas materias.

Para qué te prepara

Este Master en Seguridad Informática le prepara para conseguir una titulación profesional. Este Master MBA en Seguridad Informática: IT Security Manager le prepara para aprender el mundo de la seguridad informática, tanto el control de acceso, los protocolos de comunicación, las transferencias de datos, etc., que son procesos que deben ser estudiados y planificados por los usuarios para la definición de sus políticas de seguridad y la planificación.
Este Perito Informático Forense le prepara para conseguir una titulación profesional. El presente itinerario formativo dotará al alumno de las competencias profesionales necesarias para poder ejercer como Perito Judicial en Seguridad Informática en los diferentes procesos judiciales, además de garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior de la organización.La presente formación se ajusta al itinerario formativo del Certificado de Profesionalidad IFCT0109 Seguridad Informática, certificando el haber superado las distintas Unidades de Competencia en él incluidas, y va dirigido a la acreditación de las Competencias profesionales adquiridas a través de la experiencia laboral y de la formación no formal, vía por la que va a optar a la obtención del correspondiente Certificado de Profesionalidad, a través de las respectivas convocatorias que vayan publicando las distintas Comunidades Autónomas, así como el propio Ministerio de Trabajo (Real Decreto 1224/2009 de reconocimiento de las competencias profesionales adquiridas por experiencia laboral). Con este Curso de Perito Judicial podrás ejercer ante demandas de Particulares y Sociedades, Administración y Justicia. El alumno, al finalizar el curso, obtendrá un Diploma que le permitirá darse de Alta como Asociado Profesional en ASPEJURE y poder ejercer en los Juzgados y Tribunales. Es un curso apto para el acceso a las Listas de los Juzgados.

Salidas Laborales

Seguridad Informática / Peritaciones Judiciales
Derecho / Perito Judicial / Seguridad Informática.

- Manual teórico 'Perito Judicial'
- Manual teórico 'Seguridad Informática'
- Manual teórico 'Explotación de las Funcionalidades del Sistema Microinformático'
- Manual teórico 'Instalación y Actualización de Sistemas Operativos'
- Manual teórico 'Montaje y Verificación de Componentes'
- Manual teórico 'Instalación y Configuración de Periféricos Microinformáticos'
- Manual teórico 'Reparación y Ampliación de Equipos y Componentes Hardware Microinformáticos'

- Manual teórico 'Resolución de Averías Lógicas en Equipos Microinformáticos'
- Manual teórico 'Reparación de Impresoras'
- Manual teórico 'Elaboración de Informes Periciales'
- Manual teórico 'Ethical Hacking'

Formas de Pago

- Tarjeta
- Transferencia
- Paypal

Otros: PayU, Sofort, Western Union, SafetyPay
Fracciona tu pago en cómodos plazos sin intereses
+ Envío Gratis.

Llama gratis al teléfono (+34) 958 050 217 e infórmate de los pagos a plazos sin intereses que hay disponibles



Financiación

Facilidades económicas y financiación 100% sin intereses.
En Educa Business ofrecemos a nuestro alumnado facilidades económicas y financieras para la realización de pago de matrículas, todo ello 100% sin intereses.
30% Beca Desempleo: Para quienes atraviesen un periodo de inactividad laboral y decidan que es el momento para invertir en la mejora de sus posibilidades futuras.
10% Beca Alumnos: Como premio a la fidelidad y confianza ofrecemos una beca a todos aquellos que hayan cursado alguna de nuestras acciones formativas en el pasado.



Metodología y Tutorización

El modelo educativo por el que apuesta Euroinnova es el **aprendizaje colaborativo** con un método de enseñanza totalmente interactivo, lo que facilita el estudio y una mejor asimilación conceptual, sumando esfuerzos, talentos y competencias.
El alumnado cuenta con un **equipo docente** especializado en todas las áreas.
Proporcionamos varios medios que acercan la comunicación alumno tutor, adaptándonos a las circunstancias de cada usuario.
Ponemos a disposición una **plataforma web** en la que se encuentra todo el contenido de la acción formativa. A través de ella, podrá estudiar y comprender el temario mediante actividades prácticas, autoevaluaciones y una evaluación final, teniendo acceso al contenido las 24 horas del día.
Nuestro nivel de exigencia lo respalda un **acompañamiento personalizado.**



Redes Sociales

Síguenos en nuestras redes sociales y pasa a formar parte de nuestra gran **comunidad educativa,** donde podrás participar en foros de opinión, acceder a contenido de interés, compartir material didáctico e interactuar con otros/as alumnos/as, ex alumnos/as y profesores/as. Además, te enterarás antes que nadie de todas las promociones y becas mediante nuestras publicaciones, así como también podrás contactar directamente para obtener información o resolver tus dudas.



Reinventamos la Formación Online

Más de 150 cursos Universitarios

Contamos con más de 150 cursos avalados por distintas Universidades de reconocido prestigio.

Campus 100% Online

Impartimos nuestros programas formativos mediante un campus online adaptado a cualquier tipo de dispositivo.

Amplio Catálogo

Nuestro alumnado tiene a su disposición un amplio catálogo formativo de diversas áreas de conocimiento.

Claustro Docente

Contamos con un equipo de docentes especializados/as que realizan un seguimiento personalizado durante el itinerario formativo del alumno/a.

Nuestro Aval AEC y AECA

Nos avala la Asociación Española de Calidad (AEC) estableciendo los máximos criterios de calidad en la formación y formamos parte de la Asociación Española de Contabilidad y Administración de Empresas (AECA), dedicada a la investigación de vanguardia en gestión empresarial.

Club de Alumnos/as

Servicio Gratuito que permite a nuestro alumnado formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: beca, descuentos y promociones en formación. En este, se puede establecer relación con alumnos/as que cursen la misma área de conocimiento, compartir opiniones, documentos, prácticas y un sinfín de intereses comunitarios.

Bolsa de Prácticas

Facilitamos la realización de prácticas de empresa, gestionando las ofertas profesionales dirigidas a nuestro alumnado. Ofrecemos la posibilidad de practicar en entidades relacionadas con la formación que se ha estado recibiendo en nuestra escuela.

Revista Digital

El alumnado puede 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, y otros recursos actualizados de interés.

Innovación y Calidad

Ofrecemos el contenido más actual y novedoso, respondiendo a la realidad empresarial y al entorno cambiante, con una alta rigurosidad académica combinada con formación práctica.

Acreditaciones y Reconocimientos

Temario

1.CURSO 1: MASTER EN SEGURIDAD INFORMÁTICA

PARTE 1. MONTAJE DE EQUIPOS MICROINFORMÁTICOS

MÓDULO 1. MONTAJE Y VERIFICACIÓN DE COMPONENTES.

UNIDAD DIDÁCTICA 1. APLICACIÓN DE MEDIDAS DE SEGURIDAD CONTRA EL RIESGO ELÉCTRICO.

1.Seguridad eléctrica.
2.Medidas de prevención de riesgos eléctricos.
3.Daños producidos por descarga eléctrica.
4.Seguridad en el uso de componentes eléctricos.
5.Seguridad en el uso de herramientas manuales.

UNIDAD DIDÁCTICA 2. HERRAMIENTAS Y COMPONENTES ELECTRÓNICOS.

1.Electricidad estática. Descargas electrostáticas (ESD).
2.Estándares de la industria relacionados con la electrostática.

UNIDAD DIDÁCTICA 3. INTERPRETACIÓN DE LA SIMBOLOGÍA APLICADA A LOS COMPONENTES MICROINFORMÁTICOS.

1.Simbología estándar de los componentes.
2.Simbología de homologaciones nacionales e internacionales.

UNIDAD DIDÁCTICA 4. COMPONENTES INTERNOS DE UN EQUIPO MICROINFORMÁTICO.

1.Arquitectura de un sistema microinformático.
2.Componentes de un equipo informático, tipos, características y tecnologías.
3.El procesador.
4.Componentes OEM y RETAIL

UNIDAD DIDÁCTICA 5. ENSAMBLADO DE EQUIPOS Y MONTAJE DE PERIFÉRICOS BÁSICOS

1.El puesto de montaje.
2.Guías de montaje.
3.Elementos de fijación, tipos de tornillos.
4.El proceso de ensamblado de un equipo microinformático.
5.El ensamblado fuera del chasis.
6.Descripción de dispositivos periféricos básicos.
7.Instalación y prueba de periféricos básicos.
8.Instalación y configuración de periféricos básicos.
9.Instalación y configuración de la tarjeta gráfica.
10.Instalación de controladores y utilidades software.
11.Realización de pruebas funcionales y operativas.

UNIDAD DIDÁCTICA 6. PUESTA EN MARCHA Y VERIFICACIÓN DE EQUIPOS INFORMÁTICOS.

1.El proceso de verificación de equipos microinformáticos.
2.Proceso de arranque de un ordenador.
3.Herramientas de diagnóstico y/o verificación de los sistemas operativos.
4.Pruebas y mensajes con sistemas operativos en almacenamiento extraíble.
5.Pruebas con software de diagnóstico.
6.Pruebas de integridad y estabilidad en condiciones extremas.
7.Pruebas de rendimiento.

UNIDAD DIDÁCTICA 7. CONFIGURACIÓN DE LA BIOS.

1.El SETUP. Versiones más utilizadas.
2.El menú principal de configuración de la BIOS.

UNIDAD DIDÁCTICA 8. NORMA Y REGLAMENTOS SOBRE PREVENCIÓN DE RIESGOS LABORALES Y ERGONOMÍA.

1.Marco legal general.
2.Marco legal específico.

UNIDAD DIDÁCTICA 9. NORMAS DE PROTECCIÓN DEL MEDIO AMBIENTE.

1.Ley 10/1998, de Residuos. Definiciones. Categorías de residuos.
2.Ley 11/1997, de Envases y Residuos de Envases y su desarrollo. Definiciones.
3.R.D. 208/2005, sobre aparatos eléctricos y electrónicos y la gestión de sus residuos.
4.Objeto, ámbito de aplicación y definiciones.
5.Tratamiento de residuos.
6.Operaciones de tratamiento: reutilización, reciclado, valorización energética y eliminación.
7.Categorías de aparatos eléctricos o electrónicos.
8.Tratamiento selectivo de materiales y componentes.
9.Lugares de reciclaje y eliminación de residuos informáticos. Símbolo de recogida selectiva.
10.R.D. 106/2008, sobre pilas y acumuladores y la gestión ambiental de sus residuos.
11.Objeto, ámbito de aplicación, y definiciones.

12.Tipos de pilas y acumuladores.
13.Recogida, tratamiento y reciclaje.
14.Símbolo de recogida selectiva.
15.Normas sobre manipulación y almacenaje de productos contaminantes, tóxicos y combustibles. Las Fichas de Datos de Seguridad.
16.Identificación de las sustancias o preparados.

MÓDULO 2. INSTALACIONES Y CONFIGURACIÓN DE PERIFÉRICOS MICROINFORMÁTICOS.

UNIDAD DIDÁCTICA 1. DESCRIPCIÓN DE DISPOSITIVOS PERIFÉRICOS.

1.Tipos de dispositivos periféricos.
2.Características técnicas y funcionales.
3.Parámetros de configuración.
4.Recomendaciones de uso.
5.Especificaciones técnicas.

UNIDAD DIDÁCTICA 2. INSTALACIÓN Y PRUEBA DE PERIFÉRICOS.

1.Procedimientos para el montaje de periféricos.
2.Identificación de los requisitos de instalación.
3.Instalación y configuración de periféricos.
4.Instalación y configuración de tarjetas.
5.Instalación de controladores y utilidades software.
6.Realización de pruebas funcionales y operativas.

PARTE 2. INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS OPERATIVOS

MÓDULO 1. INSTALACIÓN Y ACTUALIZACIÓN DE SISTEMAS OPERATIVOS

UNIDAD DIDÁCTICA 1. ARQUITECTURAS DE UN SISTEMA MICROINFORMÁTICO.

1.Esquema funcional de un ordenador.
2.La unidad central de proceso y sus elementos.
3.Buses.
4.Correspondencia entre los Subsistemas físicos y lógicos.

UNIDAD DIDÁCTICA 2. FUNCIONES DEL SISTEMA OPERATIVO INFORMÁTICO.

1.Conceptos básicos.
2.Funciones.

UNIDAD DIDÁCTICA 3. ELEMENTOS DE UN SISTEMA OPERATIVO INFORMÁTICO.

1.Gestión de procesos.

2.Gestión de memoria.
3.El sistema de Entrada y Salida.
4.Sistema de archivos.
5.Sistema de protección.
6.Sistema de comunicaciones.
7.Sistema de interpretación de órdenes.
8.Programas del sistema.

UNIDAD DIDÁCTICA 4. SISTEMAS OPERATIVOS INFORMÁTICOS ACTUALES.

1.Clasificación de los sistemas operativos.
2.Software libre.
3.Características y utilización.
4.Diferencias.
5.Versiones y distribuciones.

UNIDAD DIDÁCTICA 5. INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS OPERATIVOS INFORMÁTICOS.

1.Requisitos para la instalación. Compatibilidad hardware y software.
2.Fases de instalación.
3.Tipos de instalación.
4.Verificación de la instalación. Pruebas de arranque y parada.
5.Documentación de la instalación y configuración.

UNIDAD DIDÁCTICA 6. REPLICACIÓN FÍSICA DE PARTICIONES Y DISCOS DUROS.

1.Programas de copia de seguridad.
2.Clonación.
3.Funcionalidad y objetivos del proceso de replicación.
4.Seguridad y prevención en el proceso de replicación.
5.Particiones de discos.
6.Herramientas de creación e implantación de imágenes y réplicas de sistemas:

UNIDAD DIDÁCTICA 7. ACTUALIZACIÓN DEL SISTEMA OPERATIVO INFORMÁTICO.

1.Clasificación de las fuentes de actualización.
2.Actualización automática.
3.Los centros de soporte y ayuda.
4.Procedimientos de actualización.
5.Actualización de sistemas operativos.
6.Actualización de componentes software.
7.Verificación de la actualización.
8.Documentación de la actualización.

MÓDULO 2. EXPLOTACIÓN DE LAS FUNCIONALIDADES DEL SISTEMA MICROINFORMATICO

UNIDAD DIDÁCTICA 1. UTILIDADES DEL SISTEMA OPERATIVO.

1.Características y funciones.
2.Configuración del entorno de trabajo.
3.Administración y gestión de los sistemas de archivo.
4.Gestión de procesos y recursos.
5.Gestión y edición de archivos.

UNIDAD DIDÁCTICA 2. ORGANIZACIÓN DEL DISCO Y SISTEMA DE ARCHIVOS.

1.El sistema de archivos.
2.Unidades lógicas de almacenamiento.
3.Estructuración de los datos.
4.Tipos de ficheros.
5.Carpetas y archivos del sistema.
6.Estructura y configuración del explorador de archivos.
7.Operaciones con archivos.
8.Búsqueda de archivos.

UNIDAD DIDÁCTICA 3. CONFIGURACIÓN DE LAS OPCIONES DE ACCESIBILIDAD.

1.Opciones para facilitar la visualización de pantalla.
2.Uso de narradores.
3.Opciones para hacer más fácil el uso del teclado o del ratón.
4.Reconocimiento de voz.
5.Uso de alternativas visuales y de texto para personas con dificultades auditivas.

UNIDAD DIDÁCTICA 4. CONFIGURACIÓN DEL SISTEMA INFORMÁTICO.

1.Configuración del entorno de trabajo.
2.Administrador de impresión.
3.Administrador de dispositivos.
4.Protección del sistema.
5.Configuración avanzada del sistema.

UNIDAD DIDÁCTICA 5. UTILIZACIÓN DE LAS HERRAMIENTAS DEL SISTEMA.

1.Desfragmentado de disco.
2.Copias de seguridad.
3.Liberación de espacio.
4.Programación de tareas.
5.Restauración del sistema.

UNIDAD DIDÁCTICA 6. GESTIÓN DE PROCESOS Y RECURSOS.

1.Mensajes y avisos del sistema.
2.Eventos del sistema.
3.Rendimiento del sistema.
4.Administrador de tareas.
5.Editor del registro del sistema.

PARTE 3. REPARACIÓN DE EQUIPAMIENTO MICROINFORMÁTICO

MÓDULO 1. REPARACIÓN DE EQUIPAMIENTO MICROINFORMÁTICO

UNIDAD DIDÁCTICA 1. INSTRUMENTACIÓN BÁSICA APLICADA A LA REPARACIÓN DE EQUIPOS MICROINFORMÁTICOS.

1.Conceptos de electricidad y electrónica aplicada a la reparación de equipos microinformáticos.
2.Magnitudes eléctricas y su medida.
3.Señales analógicas y digitales.
4.Componentes analógicos.
5.Electrónica digital
6.Instrumentación básica.

UNIDAD DIDÁCTICA 2. FUNCIONAMIENTO DE LOS DISPOSITIVOS DE UN SISTEMA INFORMÁTICO.

1.Esquemas funcionales de los dispositivos y periféricos en equipos informáticos.
2.Componentes eléctricos. Funciones.
3.Componentes electrónicos. Funciones.
4.Componentes electromecánicos. Funciones.
5.Los soportes de almacenamiento magnético.

UNIDAD DIDÁCTICA 3. TIPOS DE AVERÍAS EN EQUIPOS MICROINFORMÁTICOS.

1.Tipología de las averías.
2.Averías típicas.

UNIDAD DIDÁCTICA 4. DIAGNÓSTICO Y LOCALIZACIÓN DE AVERÍAS EN EQUIPOS INFORMÁTICOS.

1.Organigramas y procedimientos para la localización de averías.
2.El diagnóstico.
3.Herramientas software de diagnóstico.
4.Herramientas hardware de diagnóstico.
5.Conectividad de los equipos informáticos
6.Medidas de señales de las interfases, buses y conectores de los diversos componentes.
7.El conexionado externo e interno de los equipos informáticos.
8.Técnicas de realización de diverso cableado.

UNIDAD DIDÁCTICA 5. REPARACIÓN DEL HARDWARE DE LA UNIDAD CENTRAL.

1.El puesto de reparación.
2.El presupuesto de la reparación.
3.El procedimiento de reparación.
4.Reparación de averías del hardware.

UNIDAD DIDÁCTICA 6. AMPLIACIÓN DE UN EQUIPO INFORMÁTICO.

1.Componentes actualizables.

2.El procedimiento de ampliación.
3.Ampliaciones típicas de equipos informáticos lógicas y físicas.

MÓDULO 2. RESOLUCIÓN DE AVERÍAS LÓGICAS EN EQUIPOS MICROINFORMÁTICOS.

UNIDAD DIDÁCTICA 1. EL ADMINISTRADOR DE TAREAS Y HERRAMIENTAS DE RECUPERACIÓN DE DATOS.

1.El administrador de tareas.
2.Instalación y utilización de herramientas de recuperación de datos.

UNIDAD DIDÁCTICA 2. RESOLUCIÓN DE AVERÍAS LÓGICAS.

1.El Master Boot Record (MBR), particiones y partición activa.
2.Archivos de inicio del sistema.
3.Archivos de configuración del sistema.
4.Optimización del sistema.
5.Copia de seguridad.
6.Restablecimiento por clonación.
7.Reinstalación, configuración y actualización de componentes de componentes software.

UNIDAD DIDÁCTICA 3. INSTALACIÓN Y CONFIGURACIÓN DEL SOFTWARE ANTIVIRUS.

1.Virus informáticos.
2.Definición de software antivirus.
3.Componentes activos de los antivirus.
4.Características generales de los paquetes de software antivirus.
5.Instalación de software antivirus.
6.La ventana principal.

MÓDULO 3. REPARACIÓN DE IMPRESORAS.

UNIDAD DIDÁCTICA 1. LAS IMPRESORAS.

1.Las impresoras.
2.Tipos de impresoras. Características y diferencias.
3.Marcas y modelos más usuales.

UNIDAD DIDÁCTICA 2. MANIPULACIÓN Y SUSTITUCIÓN DE ELEMENTOS CONSUMIBLES.

1.Tipos y características.
2.Conservación de elementos consumibles.
3.Procedimientos de sustitución de elementos consumibles.
4.Seguridad en procedimientos de manipulación y sustitución de elementos consumibles.

UNIDAD DIDÁCTICA 3. REPARACIÓN DE IMPRESORAS MATRICIALES.

1.Impresoras matriciales. Funcionamiento y detalles técnicos.
2.Seguridad en el manejo de impresoras matriciales.
3.Piezas de una impresora matricial.

4.Especificaciones mecánicas, electrónicas, eléctricas y ambientales.
5.Bloques funcionales y funcionamiento de sus componentes.
6.Consumibles.
7.Transporte de la impresora.

UNIDAD DIDÁCTICA 4. REPARACIÓN DE IMPRESORAS DE INYECCIÓN DE TINTA.

1.Seguridad en el manejo de impresoras de inyección de tinta.
2.Piezas de una impresora de inyección de tinta.
3.Especificaciones mecánicas, electrónicas, eléctricas y ambientales.
4.Bloques funcionales y funcionamiento de sus componentes.
5.Limpieza de la impresora.
6.Lubricación.
7.Consumibles.
8.Revisión de los inyectores.
9.Limpieza del cabezal de inyección.
10.Alineación del cabezal de inyección.
11.Limpieza de la impresora.
12.Resolución de problemas.
13.Transporte de la impresora.

UNIDAD DIDÁCTICA 5. REPARACIÓN DE IMPRESORAS LÁSER.

1.Seguridad en el manejo de impresoras láser.
2.Piezas de una impresora láser.
3.Especificaciones mecánicas, electrónicas, eléctricas y ambientales.
4.Bloques funcionales y funcionamiento de sus componentes.
5.Consumibles.
6.Mantenimiento preventivo y correctivo.
7.Transporte de la impresora.

PARTE 4. PERITO JUDICIAL EN SEGURIDAD INFORMÁTICA

MÓDULO 1. PERITO JUDICIAL

UNIDAD DIDÁCTICA 1. PERITACIÓN Y TASACIÓN

1.Delimitación de los términos peritaje y tasación
2.La peritación
3.La tasación pericial

UNIDAD DIDÁCTICA 2. NORMATIVA BÁSICA NACIONAL

1.Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
2.Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil

3.Ley de Enjuiciamiento Criminal, de 1882
4.Ley 1/1996, de 10 de enero, de Asistencia Jurídica Gratuita

UNIDAD DIDÁCTICA 3. LOS PERITOS

1.Concepto
2.Clases de perito judicial
3.Procedimiento para la designación de peritos
4.Condiciones que debe reunir un perito
5.Control de la imparcialidad de peritos
6.Honorarios de los peritos

UNIDAD DIDÁCTICA 4. EL RECONOCIMIENTO PERICIAL

1.El reconocimiento pericial
2.El examen pericial
3.Los dictámenes e informes periciales judiciales
4.Valoración de la prueba pericial
5.Actuación de los peritos en el juicio o vista

UNIDAD DIDÁCTICA 5. LEGISLACIÓN REFERENTE A LA PRÁCTICA DE LA PROFESIÓN EN LOS TRIBUNALES

1.Funcionamiento y legislación
2.El código deontológico del Perito Judicial

UNIDAD DIDÁCTICA 6. LA RESPONSABILIDAD

1.La responsabilidad
2.Distintos tipos de responsabilidad
  1.- Responsabilidad civil
  2.- Responsabilidad penal
  3.- Responsabilidad disciplinaria
3.El seguro de responsabilidad civil

UNIDAD DIDÁCTICA 7. PERITACIONES

1.La peritación médico-legal
  1.- Daño corporal
  2.- Secuelas
2.Peritaciones psicológicas
  1.- Informe pericial del peritaje psicológico
3.Peritajes informáticos
4.Peritaciones inmobiliarias

MÓDULO 2. ELABORACIÓN DE INFORMES PERICIALES

UNIDAD DIDÁCTICA 1. PERITO, INFORME PERICIAL Y ATESTADO POLICIAL

1.Concepto de perito
2.Atestado policial

3.Informe pericial

UNIDAD DIDÁCTICA 2. TIPOS DE INFORMES PERICIALES

1.Informes periciales por cláusulas de suelo
2.Informes periciales para justificación de despidos

UNIDAD DIDÁCTICA 3. TIPOS DE INFORMES PERICIALES

1.Informes periciales de carácter económico, contable y financiero
2.Informes especiales de carácter pericial

UNIDAD DIDÁCTICA 4. LAS PRUEBAS JUDICIALES Y EXTRAJUDICIALES

1.Concepto de prueba
2.Medios de prueba
3.Clases de pruebas
4.Principales ámbitos de actuación
5.Momento en que se solicita la prueba pericial
6.Práctica de la prueba

UNIDAD DIDÁCTICA 5. ELABORACIÓN DEL INFORME TÉCNICO

1.¿Qué es el informe técnico?
2.Diferencia entre informe técnico y dictamen pericial
3.Objetivos del informe pericial
4.Estructura del informe técnico

UNIDAD DIDÁCTICA 6. ELABORACIÓN DEL DICTAMEN PERICIAL

1.Características generales y estructura básica
2.Las exigencias del dictamen pericial
3.Orientaciones para la presentación del dictamen pericial

UNIDAD DIDÁCTICA 7. VALORACIÓN DE LA PRUEBA PERICIAL

1.Valoración de la prueba judicial
2.Valoración de la prueba pericial por Jueces y Tribunales

MÓDULO 3. SEGURIDAD INFORMÁTICA

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. 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 necesario para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6.Establecimiento de la monitorización y pruebas de los cortafuegos

UNIDAD DIDÁCTICA 9. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

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 su efecto sobre las vulnerabilidades y amenazas
11.Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
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 800-30
18.Exposición de la metodología Magerit versión 2

UNIDAD DIDÁCTICA 10. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

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, Dirb, Parosproxy, etc.
6.Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

UNIDAD DIDÁCTICA 11. 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 12. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

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 5. 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
6.CURSO 2: PERITO INFORMÁTICO FORENSE

MÓDULO 1. PERITO JUDICIAL

UNIDAD DIDÁCTICA 1. PERITACIÓN Y TASACIÓN

1.Delimitación de los términos peritaje y tasación
2.La peritación
3.La tasación pericial

UNIDAD DIDÁCTICA 2. NORMATIVA BÁSICA NACIONAL

1.Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
2.Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
3.Ley de Enjuiciamiento Criminal, de 1882
4.Ley 1/1996, de 10 de enero, de Asistencia Jurídica Gratuita

UNIDAD DIDÁCTICA 3. LOS PERITOS

1.Concepto
2.Clases de perito judicial
3.Procedimiento para la designación de peritos
4.Condiciones que debe reunir un perito
5.Control de la imparcialidad de peritos
6.Honorarios de los peritos

UNIDAD DIDÁCTICA 4. EL RECONOCIMIENTO PERICIAL

1.El reconocimiento pericial
2.El examen pericial
3.Los dictámenes e informes periciales judiciales
4.Valoración de la prueba pericial
5.Actuación de los peritos en el juicio o vista

UNIDAD DIDÁCTICA 5. LEGISLACIÓN REFERENTE A LA PRÁCTICA DE LA PROFESIÓN EN LOS TRIBUNALES

1.Funcionamiento y legislación
2.El código deontológico del Perito Judicial

UNIDAD DIDÁCTICA 6. LA RESPONSABILIDAD

1.La responsabilidad
2.Distintos tipos de responsabilidad
1.- Responsabilidad civil

2.- Responsabilidad penal
3.- Responsabilidad disciplinaria
3.El seguro de responsabilidad civil

UNIDAD DIDÁCTICA 7. PERITACIONES

1.La peritación médico-legal
1.- Daño corporal
2.- Secuelas
2.Peritaciones psicológicas
1.- Informe pericial del peritaje psicológico
3.Peritajes informáticos
4.Peritaciones inmobiliarias

MÓDULO 2. ELABORACIÓN DE INFORMES PERICIALES

UNIDAD DIDÁCTICA 1. PERITO, INFORME PERICIAL Y ATESTADO POLICIAL

1.Concepto de perito
2.Atestado policial
3.Informe pericial

UNIDAD DIDÁCTICA 2. TIPOS DE INFORMES PERICIALES

1.Informes periciales por cláusulas de suelo
2.Informes periciales para justificación de despidos

UNIDAD DIDÁCTICA 3. TIPOS DE INFORMES PERICIALES

1.Informes periciales de carácter económico, contable y financiero
2.Informes especiales de carácter pericial

UNIDAD DIDÁCTICA 4. LAS PRUEBAS JUDICIALES Y EXTRAJUDICIALES

1.Concepto de prueba
2.Medios de prueba
3.Clases de pruebas
4.Principales ámbitos de actuación
5.Momento en que se solicita la prueba pericial
6.Práctica de la prueba

UNIDAD DIDÁCTICA 5. ELABORACIÓN DEL INFORME TÉCNICO

1.¿Qué es el informe técnico?
2.Diferencia entre informe técnico y dictamen pericial
3.Objetivos del informe pericial
4.Estructura del informe técnico

UNIDAD DIDÁCTICA 6. ELABORACIÓN DEL DICTAMEN PERICIAL

1.Características generales y estructura básica
2.Las exigencias del dictamen pericial
3.Orientaciones para la presentación del dictamen pericial

UNIDAD DIDÁCTICA 7. VALORACIÓN DE LA PRUEBA PERICIAL

1.Valoración de la prueba judicial

2.Valoración de la prueba pericial por Jueces y Tribunales

MÓDULO 3. SEGURIDAD INFORMATICA

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. 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 necesario para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6.Establecimiento de la monitorización y pruebas de los cortafuegos

UNIDAD DIDÁCTICA 9. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

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 su efecto sobre las vulnerabilidades y amenazas
11.Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
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 800-30
18.Exposición de la metodología Magerit versión 2

UNIDAD DIDÁCTICA 10. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

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, Dirb, Parosproxy, etc.
6.Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

UNIDAD DIDÁCTICA 11. 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 12. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

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

MÓDULO 4. LEGISLACIÓN NACIONAL APLICABLE AL SECTOR DEL PERITAJE