EUROINNOVA BUSINESS SCHOOL

FORMACIÓN ONLINE

Titulación certificada por EUROINNOVA BUSINESS SCHOOL

Master MBA en Seguridad Informática: IT Security Manager + Titulación Universitaria + Perito Judicial Informático

EUROINNOVA FORMACIÓN

Especialistas en Formación Online

SOBRE EUROINNOVA BUSINESS SCHOOL

Bienvenidos/as a EUROINNOVA BUSINESS SCHOOL, una escuela de negocios apoyada por otras entidades de enorme prestigio a nivel internacional, que han visto el valor humano y personal con el que cuenta nuestra empresa; un valor que ha hecho que grandes instituciones de reconocimiento mundial se sumen a este proyecto.

EUROINNOVA BUSINESS SCHOOL es la mejor opción para formarse ya que contamos con años de experiencia y miles de alumnos/as, además del reconocimiento y apoyo de grandes instituciones a nivel internacional.

Como entidad acreditada para la organización e impartición de formación de postgrado, complementaria y para el empleo, Euroinnova es centro autorizado para ofrecer formación continua bonificada para personal trabajador, cursos homologados y baremables para Oposiciones dentro de la Administración Pública, y cursos y acciones formativas de máster online con título propio.

CERTIFICACIÓN EN CALIDAD

Euroinnova 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 formativas impartidas desde el centro.

DESCUBRE EUROINNOVA FORMACIÓN

Líderes en Formación Online

APOSTILLA DE LA HAYA

Además de disponer de formación avalada por universidades de reconocido prestigio y múltiples instituciones, Euroinnova posibilita certificar su formación con la Apostilla de La Haya, dotando a sus acciones formativas de Titulaciones Oficiales con validez internacional en más de 160 países de todo el mundo.

PROFESIONALES A TU DISPOSICION

La metodología virtual de la formación impartida en Euroinnova está completamente a la vanguardia educativa, facilitando el aprendizaje a su alumnado, que en todo momento puede contar con el apoyo tutorial de grandes profesionales, para alcanzar cómodamente sus objetivos.

DESCUBRE NUESTRAS METODOLOGÍAS

Desde Euroinnova se promueve una enseñanza multidisciplinar e integrada, desarrollando metodologías innovadoras de aprendizaje que permiten interiorizar los conocimientos impartidos con una aplicación eminentemente práctica, atendiendo a las demandas actuales del mercado laboral.

NUESTRA EXPERIENCIA NOS AVALA

Más de 15 años de experiencia avalan la trayectoria del equipo docente de Euroinnova Business School, que desde su nacimiento apuesta por superar los retos que deben afrontar los/las profesionales del futuro, lo que actualmente lo consolida como el centro líder en formación online.

Master MBA en Seguridad Informática: IT Security Manager + Titulación Universitaria + Perito Judicial Informático

DURACIÓN:
1.025 horas

MODALIDAD:
Online

PRECIO:
1.495 € *

CRÉDITOS:
5,00 ECTS

* Materiales didácticos, titulación y gastos de envío incluidos.

CENTRO DE FORMACIÓN:

Euroinnova Business School

TITULACIÓN

Titulación Múltiple: - Master MBA en Seguridad Informática: IT Security Manager con 600 horas expedida por EUROINNOVA INTERNATIONAL ONLINE EDUCATION, miembro de la AEEN (Asociación Española de Escuelas de Negocios) y CLADEA (Consejo Latinoamericano de Escuelas de Administración) - Titulación de Perito Judicial en Seguridad Informática con 300 horas expedida por EUROINNOVA INTERNATIONAL ONLINE EDUCATION, miembro de la AEEN (Asociación Española de Escuelas de Negocios) y CLADEA (Consejo Latinoamericano de Escuelas de Administración) - Titulación Universitaria en Consultor en Seguridad Informática IT: Ethical Hacking con 5 Créditos Universitarios ECTS. Formación Continua baremable en bolsas de trabajo y concursos oposición de la Administración Pública.

TITULACIÓN EXPEDIDA POR EUROINNOVA BUSINESS SCHOOL CENTRO DE ESTUDIOS DE POSTGRADO

3ª Mejor Escuela de Negocios España (RANKING EL ECONOMISTA)

Una vez finalizado el curso, el alumno recibirá por parte de Euroinnova Formación 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 UNESCO).


EUROINNOVA FORMACIÓN

EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXXX que presta sus servicios en la empresa LABORATORIO ELECTROTECNICO, S.C.C.L. con C.I.F. XXXXXXXXX ha cursado la acción formativa

Nombre de la Acción Formativa

perteneciente al Plan de Formación Continua impartido por EUROINNOVA con Nº Exp.XXXXXXXXX dentro del marco de la Fundación Estatal para la Formación en el empleo dirigido a trabajadores de todos los sectores en la convocatoria del 2019.

Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX/XXXX-XXXX-XXXXXX

Con un nivel de aprovechamiento ALTO

Y para que conste expido la presente TITULACIÓN en Granada, a 11 de Noviembre de 2019

La Dirección General

JESÚS MORENO HIDALGO

Sello

Firma del Alumno/a

VÍCTOR LUIS LLORENTE

DESCRIPCIÓN

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.

OBJETIVOS

- 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 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

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.

SALIDAS LABORALES

Seguridad Informática, Peritaciones Judiciales

MATERIALES DIDÁCTICOS

- Maletín porta documentos
- 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'

- Subcarpeta portafolios

- Dossier completo Oferta Formativa

- Carta de presentación

- Guía del alumno

- Bolígrafo

FORMAS DE PAGO

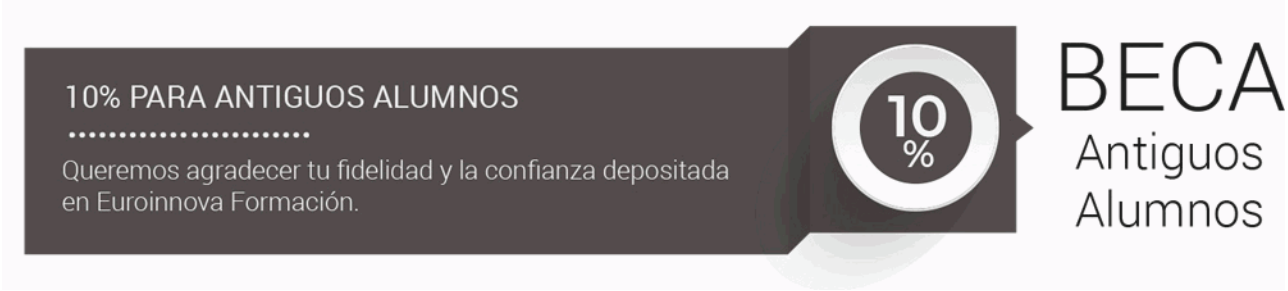
Contrareembolso / Transferencia / Tarjeta de Crédito / Paypal
Tarjeta de Crédito / PayPal Eligiendo esta opción de pago, podrá abonar el importe correspondiente, cómodamente en este mismo instante, a través de nuestra pasarela de pago segura concertada con Paypal Transferencia Bancaria
Eligiendo esta opción de pago, deberá abonar el importe correspondiente mediante una transferencia bancaria. No será aceptado el ingreso de cheques o similares en ninguna de nuestras cuentas bancarias.
Contrareembolso Podrá pagar sus compras directamente al transportista cuando reciba el pedido en su casa . Eligiendo esta opción de pago, recibirá mediante mensajería postal, en la dirección facilitada
Otras: PayU, Sofort, Western Union / SafetyPay
Fracciona tu pago en cómodos Plazos sin Intereses + Envío

Llama gratis al 900 831 200 e infórmate de nuestras facilidades de pago.

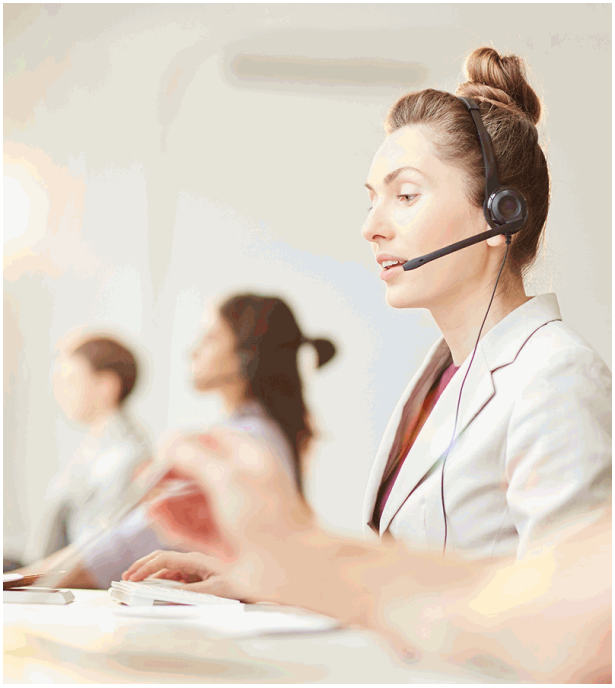
FINANCIACIÓN Y BECAS

Facilidades económicas y financiación 100% sin intereses

En EUROINNOVA, ofrecemos a nuestros alumnos facilidades económicas y financieras para la realización de pago de matrículas, todo ello 100% sin intereses.
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

CARÁCTER OFICIAL DE LA FORMACIÓN

La presente formación no está incluida dentro del ámbito de la formación oficial reglada (Educación Infantil, Educación Primaria, Educación Secundaria, Formación Profesional Oficial FP, Bachillerato, Grado Universitario, Master Oficial Universitario y Doctorado). Se trata por tanto de una formación complementaria y/o de especialización, dirigida a la adquisición de determinadas competencias, habilidades o aptitudes de índole profesional, pudiendo ser baremable como mérito en bolsas de trabajo y/o concursos oposición, siempre dentro del apartado de Formación Complementaria y/o Formación Continua siendo siempre

imprescindible la revisión de los requisitos específicos de baremación de las bolsa de trabajo público en concreto a la que deseemos presentarnos.

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 alumnos, ex alumnos y profesores.

Además serás el primero en enterarte de todas las promociones y becas mediante nuestras publicaciones, así como también podrás contactar directamente para obtener información o resolver tus dudas.

LÍDERES EN FORMACION ONLINE

Somos Diferentes

Amplio Catálogo Format

Nuestro catálogo está formado por más de 18.000 cursos de múltiples áreas de conocimiento, adaptándonos a las necesidades formativas de nuestro alumnado.

Confianza

Contamos con el Sello de Confianza Online que podrás encontrar en tus webs de confianza. Además colaboramos con las más prestigiosas Universidades, Administraciones Públicas y Empresas de Software a nivel

Campus Online

Nuestro alumnado puede acceder al campus virtual desde cualquier dispositivo, contando con acceso ilimitado a los contenidos de su programa formativo.

Profesores/as Especialis

Contamos con un equipo formado por más de 50 docentes con especialización y más de 1.000 colaboradores externos a la entera disposición de nuestro alumnado.

Bolsa de Empleo

Disponemos de una bolsa de empleo propia con diferentes ofertas de trabajo correspondientes a los distintos cursos y masters. Somos agencia de colaboración Nº 9900000169 autorizada por el Ministerio de Empleo y Seguridad Social.

Garantía de Satisfacción

Más de 15 años de experiencia con un récord del 96% de satisfacción en atención al alumnado y miles de opiniones de personas satisfechas nos avalan.

Precios Competitivos

Garantizamos la mejor relación calidad/precio en todo nuestro catálogo formativo.

Calidad AENOR

Todos los procesos de enseñanza aprendizaje siguen los más rigurososcontroles de calidad extremos, estando certificados por AENOR conforme a la ISO 9001, llevando a cabo auditorías externas que garantizan la máxima calidad.

Club de Alumnos/as

Servicio Gratuito que permitirá al alumnado formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: beca, descuentos y promociones en formación. En esta, el alumnado podrá relacionarse con personas que estudian la misma área de conocimiento, compartir opiniones, documentos, prácticas y un sinfín de

Bolsa de Prácticas

Facilitamos la realización de prácticas de empresa gestionando las ofertas profesionales dirigidas a nuestro alumnado, para realizar prácticas relacionadas con la formación que ha estado recibiendo

Revista Digital

El alumnado 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, y otros recursos

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

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

18.Exposición de la metodología Magerit

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