EDUCA
business school

Master en Seguridad Informática

ÍNDICE

EDUCA business school

SOMOS EDUCA BUSINESS SCHOOL

EDUCA Business School es una institución de formación online especializada en negocios. Como miembro de la Comisión Internacional de Educación a Distancia y con el prestigioso Certificado de Calidad AENOR (normativa ISO 9001) nuestra institución se distingue por su compromiso con la excelencia educativa.

Nuestra **oferta formativa**, además de **satisfacer las demandas del mercado laboral** actual, puede bonificarse como formación continua para el personal trabajador, así como ser homologados en Oposiciones dentro de la Administración Pública. Las titulaciones de EDUCA Business School se pueden certificarse con la Apostilla de La Haya dotándolos de validez internacional en más de 160 países.

Más de **18** años de experiencia

Más de **300k** estudiantes formados

Hasta un **98%** tasa empleabilidad

Hasta un **100%** de financiación

Hasta un **50%** de los estudiantes repite

Hasta un **25%** de estudiantes internacionales

EDUCA business school

RANKINGS DE EDUCA BUSINESS SCHOOL

Educa Business School se engloba en el conjunto de EDUCA EDTECH Group, que ha sido reconocido por su trabajo en el campo de la formación online.

Todas las entidades bajo el sello EDUCA EDTECH comparten la misión de democratizar el acceso a la educación y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación. Gracias a ello ha conseguido el reconocimiento de diferentes rankings a nivel nacional e internacional.

QS STARS™ RATING SYSTEM
Online Learning

Ranking Educativo Innovatec

EUROPEAN EXCELLENCE EDUCATION

EL MUNDO

LOS MEJORES MASTERS EN CIBERSEGURIDAD
CyberEOP

MASTER

EDUCA business school

ALIANZAS Y ACREDITACIONES

EDUCA
business school

BY EDUCA EDTECH

Educa Business School es una marca avalada por **EDUCA EDTECH Group**, que está compuesto por un conjunto de experimentadas y reconocidas instituciones educativas de formación online. Todas las entidades que lo forman comparten la misión de democratizar el acceso a la educación y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación.

EDUCA EDTECH Group

ONLINE EDUCATION

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

inesem business school

INEAF BUSINESS SCHOOL

red educa.net

inesalud

EDU SPORT

EDUCA business school

ESIBE ESCUELA IBEROAMERICANA DE POSTGRADO

Educa.Pro

ceupe European Business School

UDAVINCI

CAPMAN testing solutions

Structuralia Engineering eLearning

UNIMIAMI International University of Miami

Educa PHAROS

METODOLOGÍA LXP

La metodología **EDUCA LXP** permite una experiencia mejorada de aprendizaje integrando la AI en los procesos de e-learning, a través de modelos predictivos altamente personalizados, derivados del estudio de necesidades detectadas en la interacción del alumnado con sus entornos virtuales.

EDUCA LXP es fruto de la **Transferencia de Resultados de Investigación** de varios proyectos multidisciplinares de I+D+i, con participación de distintas Universidades Internacionales que apuestan por la transferencia de conocimientos, desarrollo tecnológico e investigación.

1. Flexibilidad

Aprendizaje 100% online y flexible, que permite al alumnado estudiar donde, cuando y como quiera.

2. Accesibilidad

Cercanía y comprensión. Democratizando el acceso a la educación trabajando para que todas las personas tengan la oportunidad de seguir formándose.

3. Personalización

Itinerarios formativos individualizados y adaptados a las necesidades de cada estudiante.

4. Acompañamiento / Seguimiento docente

Orientación académica por parte de un equipo docente especialista en su área de conocimiento, que aboga por la calidad educativa adaptando los procesos a las necesidades del mercado laboral.

5. Innovación

Desarrollos tecnológicos en permanente evolución impulsados por la AI mediante Learning Experience Platform.

6. Excelencia educativa

Enfoque didáctico orientado al trabajo por competencias, que favorece un aprendizaje práctico y significativo, garantizando el desarrollo profesional.

RAZONES POR LAS QUE ELEGIR EDUCA BUSINESS SCHOOL

1. FORMACIÓN ONLINE ESPECIALIZADA

Nuestros alumnos acceden a un modelo pedagógico innovador **de más de 20 años de experiencia educativa con Calidad Europea.**

2. METODOLOGÍA DE EDUCACIÓN FLEXIBLE

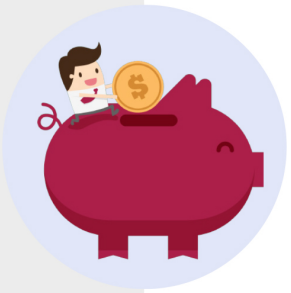
Con nuestra metodología estudiarán **100% online** y nuestros alumnos/as tendrán acceso los 365 días del año a la plataforma educativa.

3. CAMPUS VIRTUAL DE ÚLTIMA TECNOLOGÍA

Contamos con una **plataforma avanzada** con material adaptado a la realidad empresarial, que fomenta la participación, interacción y comunicación con alumnos de distintos países.

EDUCA business school

4. DOCENTES DE PRIMER NIVEL



Nuestros docentes están acreditados y formados en **Universidades de alto prestigio en Europa,** todos en activo y con una amplia experiencia profesional.

5. TUTORÍA PERMANENTE

Contamos con un **Centro de Atención al Estudiante CAE,** que brinda atención personalizada y acompañamiento durante todo el proceso formativo.

6. DOBLE MATRICULACIÓN

Algunas de nuestras acciones formativas cuentan con la llamada **Doble matriculación**, que te permite obtener dos formaciones, ya sean de masters o curso, al precio de una.

Master en Seguridad Informática

DURACIÓN
600 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

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

EDUCA business school

EDUCA BUSINESS SCHOOL

como centro acreditado para la impartición de acciones formativas
expide el presente título propio

NOMBRE DEL ALUMNO/A

con número de documento XXXXXXXX ha superado los estudios correspondientes de

Nombre del curso

con una duración de XXX horas, perteneciente al Plan de Formación de Educa Business School.
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX/XXXX-XXXX-XXXXXX.
Con una calificación XXXXXXXXXXXXXX.
Y para que conste expido la presente titulación en Granada, a (día) de (mes) del (año).

Firma del Alumno/a
NOMBRE ALUMNO/A

La Dirección Académica
NOMBRE DE AREA MANAGER

Con Estatuto Consultivo, Categoría Especial del Consejo Económico y Social de la UNESCO (Nom. Resolución 6049)

EDUCA business school

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.

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

Para qué te prepara

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.

A quién va dirigido

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.

Salidas laborales

Seguridad Informática / Peritaciones Judiciales

TEMARIO

PARTE 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.

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. 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


EDUCA
business school


By
EDUCA EDTECH
Group