EDUCA business school

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

UNIVERSIDAD NEBRIJA

Máster en Ciencias de la Seguridad Informática + 60 Créditos ECTS

Elige aprender en la escuela
líder en formación online

ÍNDICE

SOMOS EUROINNOVA

Euroinnova International Online Education inicia su actividad hace más de 20 años. Con la premisa de revolucionar el sector de la educación online, esta escuela de formación crece con el objetivo de dar la oportunidad a sus estudiandes de experimentar un crecimiento personal y profesional con formación eminetemente práctica.

Nuestra visión es ser **una institución educativa online reconocida en territorio nacional e internacional** por ofrecer una educación competente y acorde con la realidad profesional en busca del reciclaje profesional. Abogamos por el aprendizaje significativo para la vida real como pilar de nuestra metodología, estrategia que pretende que los nuevos conocimientos se incorporen de forma sustantiva en la estructura cognitiva de los estudiantes.

Más de **19** 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

Desde donde quieras y como quieras,

Elige Euroinnova

ALIANZA EUROINNOVA Y UNIVERSIDAD DE NEBRIJA

Euroinnova International Online Education y la Universidad de Nebrija consolidan de forma exitosa una colaboración estratégica. De esta manera, la colaboración entre Euroinnova y la Universidad de Nebrija impulsa un enfoque colaborativo, innovador y accesible para el aprendizaje, adaptado a las necesidades individuales de los estudiantes.

Las dos instituciones priorizan una formación práctica y flexible, adaptada a las demandas del mundo laboral actual, y que promueva el desarrollo personal y profesional de cada estudiante. El propósito es asimilar nuevos conocimientos de manera dinámica y didáctica, lo que facilita su retención y contribuye a adquirir las habilidades necesarias para adaptarse a una sociedad en constante y rápida transformación.

Euroinnova y la Universidad de Nebrija se han fijado como objetivo principal la democratización de la educación, buscando llevarla incluso a las áreas más alejadas y aprovechando las últimas innovaciones tecnológicas. Además, cuentan con un equipo de docentes altamente especializados y plataformas de aprendizaje que incorporan tecnología educativa de vanguardia, asegurando así un seguimiento tutorizado a lo largo de todo el proceso educativo.

RANKINGS DE EUROINNOVA

Euroinnova International Online Education ha conseguido el reconocimiento de diferentes rankings a nivel nacional e internacional, gracias por su apuesta de **democratizar la educación** y apostar por la innovación educativa para **lograr la excelencia.**

Para la elaboración de estos rankings, se emplean **indicadores** como la reputación online y offline, la calidad de la institución, la responsabilidad social, la innovación educativa o el perfil de los profesionales.

ALIANZAS Y ACREDITACIONES

BY EDUCA EDTECH

Euroinnova 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.

Programas

PROPIOS UNIVERSITARIOS OFICIALES

RAZONES POR LAS QUE ELEGIR EUROINNOVA

1. Nuestra Experiencia

- ✓ Más de **18 años de experiencia.**
- ✓ Más de **300.000 alumnos** ya se han formado en nuestras aulas virtuales
- ✓ Alumnos de los 5 continentes.
- ✓ **25%** de alumnos internacionales.
- ✓ **97%** de satisfacción
- ✓ **100% lo recomiendan.**
- ✓ Más de la mitad ha vuelto a estudiar en Euroinnova.

2. Nuestro Equipo

En la actualidad, Euroinnova cuenta con un equipo humano formado por más **400 profesionales.** Nuestro personal se encuentra sólidamente enmarcado en una estructura que facilita la mayor calidad en la atención al alumnado.

3. Nuestra Metodología

100% ONLINE

Estudia cuando y desde donde quieras. Accede al campus virtual desde cualquier dispositivo.

APRENDIZAJE

Pretendemos que los nuevos conocimientos se incorporen de forma sustantiva en la estructura cognitiva

EQUIPO DOCENTE

Euroinnova cuenta con un equipo de profesionales que harán de tu estudio una experiencia de alta calidad educativa.

NO ESTARÁS SOLO

Acompañamiento por parte del equipo de tutorización durante toda tu experiencia como estudiante

4. Calidad AENOR

- ✓ Somos Agencia de Colaboración Nº99000000169 autorizada por el Ministerio de Empleo y Seguridad Social.
- ✓ Se llevan a cabo auditorías externas anuales que garantizan la máxima calidad AENOR.
- ✓ Nuestros procesos de enseñanza están certificados por **AENOR** por la ISO 9001.

5. Confianza

Contamos con el sello de **Confianza Online** y colaboramos con la Universidades más prestigiosas, Administraciones Públicas y Empresas Software a nivel Nacional e Internacional.

6. Somos distribuidores de formación

Como parte de su infraestructura y como muestra de su constante expansión Euroinnova incluye dentro de su organización una **editorial y una imprenta digital industrial.**

FINANCIACIÓN Y BECAS

Financia tu cursos o máster y disfruta de las becas disponibles. ¡Contacta con nuestro equipo experto para saber cuál se adapta más a tu perfil!

25% Beca **ALUMNI**

20% Beca **DESEMPLEO**

15% Beca **EMPRENDE**

15% Beca **RECOMIENDA**

15% Beca **GRUPO**

20% Beca **FAMILIA NUMEROSA**

20% Beca **DIVERSIDAD FUNCIONAL**

20% Beca **PARA PROFESIONALES, SANITARIOS, COLEGIADOS/AS**

MÉTODOS DE PAGO

Con la Garantía de:

innovapay

Fracciona el pago de tu curso en cómodos plazos de forma segura.

mastercard maestro VISA PayPal

bizum amazon pay Pay Pay

Nos adaptamos a todos los métodos de pago internacionales:

OXXO mercado pago DISCOVER efecty Diners Club INTERNATIONAL CMR Falabella

y muchos mas...

CONFIANZA ONLINE

TRUSTED SHOPS GUARANTEE

Protección al Comprador

Máster en Ciencias de la Seguridad Informática + 60 Créditos ECTS

DURACIÓN
1500 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

CREDITOS
60 ECTS

Titulación

Doble Titulación: - Titulación Universitaria en Máster de Formación Permanente en Ciencias de la Seguridad Informática expedida por la UNIVERSIDAD ANTONIO DE NEBRIJA con 60 Créditos Universitarios ECTS - Titulación de Máster de Formación Permanente en Ciencias de la Seguridad Informática con 1500 horas expedida por EUROINNOVA INTERNATIONAL ONLINE EDUCATION, miembro de la AEEN (Asociación Española de Escuelas de Negocios) y reconocido con la excelencia académica en educación online por QS World University Rankings

Descripción

Debemos saber que hoy en día la seguridad informática es un tema muy importante y sensible, que abarca un gran conjunto de aspectos en continuo cambio y constante evolución, que exige que los profesionales informáticos posean conocimientos totalmente actualizados. Con la realización del presente Master en Ciencias de la Seguridad Informática el alumno aprenderá los conocimientos necesarios para asegurar equipos informáticos, gestionar servicios en el sistema informático, auditar redes de comunicación y sistemas informáticos, detectar y responder ante incidentes de seguridad informática, conocer la instalación y configuración de los nodos de una red de área local y la verificación y resolución de incidencias en una red de área local... Este máster universitario que Euroinnova Business School pone a tu disposición cuenta con un programa de estudios completo y actualizado, que nace con el objetivo de dar respuesta a las necesidades reales de las empresas que participan de una forma u otra en el sector digital, un sector en el que la ciberseguridad cobra cada vez más relevancia. Si quieres desarrollar una carrera profesional como auditor o consultor en ciberseguridad, ya sea trabajando por cuenta ajena o montando tu propia empresa de consultoría, este máster puede ofrecerte todo lo que necesitas para alcanzar tus metas. Además, al finalizar tu formación recibirás una titulación propia expedida directamente por la universidad, con un gran reconocimiento a nivel empresarial y académico.

Objetivos

Este máster universitario en ciberseguridad ofrece al alumnado un programa de estudios orientado a desarrollar, entre otras, las siguientes competencias profesionales: - Analizar los planes de implantación de la organización para identificar los elementos del sistema implicados y los niveles de seguridad a implementar. - Analizar e implementar los mecanismos de acceso físicos y lógicos a los servidores según especificaciones de seguridad. - Evaluar la función y necesidad de cada servicio en

ejecución en el servidor según las especificaciones de seguridad. - Instalar, configurar y administrar un cortafuegos de servidor con las características necesarias según especificaciones de seguridad. - Analizar los procesos del sistema con objeto de asegurar un rendimiento adecuado a los parámetros especificados en el plan de explotación. - Aplicar procedimientos de administración a dispositivos de almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, seguro y disponible - Administrar el acceso al sistema y a los recursos para verificar el uso adecuado y seguro de los mismos. - Evaluar el uso y rendimiento de los servicios de comunicaciones para mantenerlos dentro de los parámetros especificados. - Analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático implantando aquellas que se adecuen a las especificaciones de seguridad informática. - Aplicar procedimientos relativos al cumplimiento de la normativa legal vigente. - Planificar y aplicar medidas de seguridad para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental. - Planificar e implantar los sistemas de detección de intrusos según las normas de seguridad. - Aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada. - Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada. - Clasificar los elementos de comunicaciones que conforman una red local, para identificar los componentes que constituyen el mapa físico. - Aplicar los procedimientos de instalación y configuración de los nodos de la red local, así como los gestores de protocolos y otros programas que soportan servicios de comunicaciones. - Establecer la configuración de los parámetros de los protocolos de comunicaciones en los nodos de la red, para su integración en la propia red, siguiendo unos procedimientos dados. - Aplicar los procedimientos de prueba y verificación de los elementos de conectividad de la red y las herramientas para estos procesos. - Atender las incidencias de los elementos de comunicaciones de la red local, y proceder a su solución siguiendo unas especificaciones dadas.

Para qué te prepara

El presente Master en Ciencias de la Seguridad Informática va dirigido a todas aquellas personas que quieran orientar su futuro laboral en el mundo de la informática, desempeñando tareas de audítoria, configuración y temas relacionado con la seguridad informática, así como para aquellas personas que quieran ampliar sus conocimientos profesionales sobre esta área. De igual forma, se dirige a estudiantes y profesionales de este ámbito que tengan interés en actualizar o ampliar sus conocimientos en materia de ciberseguridad, para desarrollar su carrera profesional en uno de los sectores con mayor demanda de personal cualificado en la actualidad por parte de todo tipo de empresas con presencia en el mundo digital. Finalmente, también se dirige a todas aquellas personas que quiera completar o actualizar sus estudios en esta disciplina, consiguiendo un título de máster propio expedido por la universidad, muy valorado tanto en el ámbito de la empresa como el académico.

A quién va dirigido

Este Master en Ciencias de la Seguridad Informática le prepara para adquirir los conocimientos necesarios para asegurar equipos informáticos, gestionar servicios en el sistema informático, auditar redes de comunicación y sistemas informáticos, detectar y responder ante incidentes de seguridad informática, conocer la instalación y configuración de los nodos de una red de área local y la

verificación y resolución de incidencias en una red de área local. Con este máster universitario podrás desarrollar una carrera profesional tanto por cuenta propia montando tu propia empresa, como por cuenta ajena realizando funciones de consultoría y auditoría en materia de ciberseguridad a todo tipo de empresas que tengan presencia en el mundo digital o que utilicen sistemas y equipamientos informáticos como parte de su actividad productiva.

Salidas laborales

Gracias a los conocimientos incluidos en el programa de estudios del presente máster universitario, el alumnado podrá adquirir las competencias profesionales adecuadas para desarrollar su actividad profesional en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia.

TEMARIO

MÓDULO 1. SEGURIDAD EN EQUIPOS INFORMÁTICOS

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

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

UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO

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

UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS

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

UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD

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

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

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

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

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

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS

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

UNIDAD DIDÁCTICA 8. ROBUSTECIMIENTO DE SISTEMAS

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

UNIDAD DIDÁCTICA 9. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

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

MÓDULO 2. GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

UNIDAD DIDÁCTICA 1. GESTIÓN DE LA SEGURIDAD Y NORMATIVAS

1. Norma ISO 27002 Código de buenas practicas para la gestión de la seguridad de la información
2. Metodología ITIL Librería de infraestructuras de las tecnologías de la información
3. Ley orgánica de protección de datos de carácter personal.
4. Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

UNIDAD DIDÁCTICA 2. ANÁLISIS DE LOS PROCESOS DE SISTEMAS

1. Identificación de procesos de negocio soportados por sistemas de información
2. Características fundamentales de los procesos electrónicos
3. Estados de un proceso,
4. Manejo de señales, su administración y los cambios en las prioridades
5. Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
6. Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
7. Técnicas utilizadas para la gestión del consumo de recursos

UNIDAD DIDÁCTICA 3. DEMOSTRACIÓN DE SISTEMAS DE ALMACENAMIENTO

1. Tipos de dispositivos de almacenamiento más frecuentes
2. Características de los sistemas de archivo disponibles
3. Organización y estructura general de almacenamiento
4. Herramientas del sistema para gestión de dispositivos de almacenamiento

UNIDAD DIDÁCTICA 4. UTILIZACIÓN DE MÉTRICAS E INDICADORES DE MONITORIZACIÓN DE RENDIMIENTO DE SISTEMAS

1. Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información
2. Identificación de los objetos para los cuales es necesario obtener indicadores
3. Aspectos a definir para la selección y definición de indicadores
4. Establecimiento de los umbrales de rendimiento de los sistemas de información
5. Recolección y análisis de los datos aportados por los indicadores
6. Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

UNIDAD DIDÁCTICA 5. CONFECCIÓN DEL PROCESO DE MONITORIZACIÓN DE SISTEMAS Y COMUNICACIONES

1. Identificación de los dispositivos de comunicaciones
2. Análisis de los protocolos y servicios de comunicaciones
3. Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
4. Procesos de monitorización y respuesta
5. Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
6. Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
7. Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
8. Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

UNIDAD DIDÁCTICA 6. SELECCIÓN DEL SISTEMA DE REGISTRO DE EN FUNCIÓN DE LOS REQUERIMIENTOS DE LA ORGANIZACIÓN

1. Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
2. Análisis de los requerimientos legales en referencia al registro
3. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
4. Asignación de responsabilidades para la gestión del registro
5. Alternativas de almacenamiento para los registros del sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
6. Guía para la selección del sistema de almacenamiento y custodia de registros

UNIDAD DIDÁCTICA 7. ADMINISTRACIÓN DEL CONTROL DE ACCESOS ADECUADOS DE LOS SISTEMAS DE INFORMACIÓN

1. Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
2. Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
3. Requerimientos legales en referencia al control de accesos y asignación de privilegios
4. Perfiles de de acceso en relación con los roles funcionales del personal de la organización
5. Herramientas de directorio activo y servidores LDAP en general
6. Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
7. Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

MÓDULO 3. AUDITORÍA INFORMÁTICA

UNIDAD DIDÁCTICA 1. AUDITORÍA INFORMÁTICA

1. Código deontológico de la función de auditoría
2. Relación de los distintos tipos de auditoría en el marco de los sistemas de información
3. Criterios a seguir para la composición del equipo auditor
4. Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
5. Tipos de muestreo a aplicar durante el proceso de auditoría
6. Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)

7. Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
8. Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
9. Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

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

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

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

1. Introducción al análisis de riesgos
2. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
3. Particularidades de los distintos tipos de código malicioso
4. Principales elementos del análisis de riesgos y sus modelos de relaciones
5. Metodologías cualitativas y cuantitativas de análisis de riesgos
6. Identificación de los activos involucrados en el análisis de riesgos y su valoración
7. Identificación de las amenazas que pueden afectar a los activos identificados previamente
8. Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
9. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
10. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y 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 18. Exposición de la metodología Magerit

UNIDAD DIDÁCTICA 4. USO DE HERRAMIENTAS PARA LA AUDITORÍA INFORMÁTICA

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

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

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

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

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

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

MÓDULO 4. GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

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

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

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

1. Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio.
2. Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3. Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
4. Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 3. CONTROL DE CÓDIGO MALICIOSO

1. Sistemas de detección y contención de código malicioso
2. Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar
3. Criterios de seguridad para la configuración de las herramientas de protección frente a código

malicioso
4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
5. Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso
7. Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

UNIDAD DIDÁCTICA 4. RESPUESTA ANTE INCIDENTES DE SEGURIDAD

1. Procedimiento de recolección de información relacionada con incidentes de seguridad
2. Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
3. Proceso de verificación de la intrusión
4. Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

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

1. Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
2. Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
3. Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente
4. Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
5. Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo
6. Establecimiento del nivel de intervención requerido en función del impacto previsible
7. Guía para la investigación y diagnostico del incidente de intento de intrusión o infecciones
8. Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección
9. Proceso para la comunicación del incidente a terceros, si procede
10. Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE INFORMÁTICO

1. Conceptos generales y objetivos del análisis forense
2. Exposición del Principio de Lockard
3. Guía para la recogida de evidencias electrónicas:
4. Evidencias volátiles y no volátiles
5. Etiquetado de evidencias
6. Cadena de custodia
7. Ficheros y directorios ocultos

8. Información oculta del sistema
9. Recuperación de ficheros borrados
10. Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta del sistema y la recuperación de ficheros borrados
11. Guía para la selección de las herramientas de análisis forense

MÓDULO 5. INSTALACIÓN Y CONFIGURACIÓN DE LOS NODOS DE UNA RED DE AREA LOCAL

UNIDAD DIDÁCTICA 1. ARQUITECTURA DE REDES DE ÁREA LOCAL.

1. Clasificación de las redes en función del territorio que abarcan.
2. Características de una red local.
3. Arquitectura de redes de área local.
    1. - Topologías básicas.
    2. - Topología lógica y física.
    3. - Método de acceso al cable.
    4. - Protocolos de comunicaciones.
    5. - Arquitecturas de redes de área local más usadas.
4. Normativa.
    1. - Comités de estandarización.
    2. - Estándares de redes de área local.
    3. - Infraestructuras Comunes de Telecomunicación.

UNIDAD DIDÁCTICA 2. ELEMENTOS DE UNA RED DE ÁREA LOCAL.

1. Características y funciones.
2. Estaciones de trabajo.
3. Servidores.
4. Tarjetas de red.
5. Equipos de conectividad.
    1. - Repetidores.
    2. - Concentradores (Hubs).
    3. - Conmutadores (Switches).
    4. - Encaminadores (Routers).
    5. - Pasarelas (Gateways).
    6. - Puentes (Bridges).
    7. - Dispositivos inalámbricos.
6. Sistemas operativos de red.
7. Medios de transmisión.
    1. - Medios de cobre: Cables de para trenzado y coaxial.
    2. - Medios ópticos: Cables de fibra óptica.
    3. - Comunicaciones inalámbricas.
8. El cableado estructurado.
    1. - Subsistemas de cableado estructurado.
    2. - Estándares TIA/EIA sobre cableado estructurado.
    3. - Estándares de Cable UTP/STP.
9. El mapa físico y lógico de una red de área local.

UNIDAD DIDÁCTICA 3. PROTOCOLOS DE UNA RED DE ÁREA LOCAL.

1. Introducción a los protocolos.
2. Modelo de Interconexión de Sistemas Abiertos (OSI).
3. El nivel físico.
4. Protocolos del nivel de enlace.
    1. - Protocolos de control de enlace lógico (LLC).
    2. - Protocolos de control de acceso al medio (MAC).
        1. * Protocolos de contienda.
        2. * Protocolos de paso de testigo.
        3. * Otros.
5. Ethernet.
    1. - Introducción a Ethernet.
    2. - Ethernet y el modelo OSI.
    3. - Direccionamiento MAC.
    4. - Trama Ethernet.
    5. - Tecnologías Ethernet.
6. Otros protocolos de nivel de enlace: Token Ring, FDDI, etc.
7. Protocolos de nivel de red.
    1. - Protocolo de Internet (IP).
8. *Introducción a IP
    1. * Dirección IP.
    2. * Asignación de direcciones.
    3. * Enrutamiento
    1. - Otros Protocolos de nivel de red (IPX, etc)
9. Direcciones físicas y lógicas.

UNIDAD DIDÁCTICA 4. INSTALACIÓN Y CONFIGURACIÓN DE LOS NODOS DE LA RED DE ÁREA LOCAL.

1. El armario de comunicaciones.
    1. - Elementos del armario de comunicaciones.
    2. - Representación en el armario de la tomas de red de los nodos.
2. Instalación de adaptadores de red y controladores.
3. Instalación y configuración de protocolos de red más habituales.
    1. - Parámetros característicos.
    2. - Configuración del protocolo TCP/IP.
        1. * Elementos de configuración de TCP/IP.
        2. * Dirección IP.
        3. * Mascara de subred.
        4. * Puerta de enlace.
        5. * Servidor DNS.
        6. * Servidor WINS.
        7. * Configuración de NetBIOS.
        8. * Asignación a un grupo de trabajo.
    3. - Procedimiento de configuración de otros protocolos: SPX/IPX, etc.
    4. - Configuración de la seguridad
        1. * Autenticación de identidad.
        2. * Cifrado de datos.
    5. - Procedimientos sistemáticos de configuración.
4. Instalación y configuración de servicios de red.
    1. - Servicios de acceso a la red.

2. - Servicio de ficheros.
3. - Servicios de impresión.
4. - Servicio de correos.
5. - Otros servicios.

5. Procedimiento de aplicación de configuraciones a routers y switches.
    1. - Las aplicaciones de emulación de terminal.
    2. - Configuración de las aplicaciones de emulación de terminal.
    3. - Aplicación de configuraciones a routers y switches.

MÓDULO 6. VERIFICACIÓN Y RESOLUCIÓN DE INCIDENCIAS EN UNA RED DE ÁREA LOCAL

UNIDAD DIDÁCTICA 1. VERIFICACIÓN Y PRUEBA DE ELEMENTOS DE CONECTIVIDAD DE REDES DE ÁREA LOCAL.

1. Herramientas de verificación y prueba.
    1. - Herramientas de verificación y prueba de los sistemas operativos.
    2. - Comandos TCP/IP.
    3. - Obtención de la Configuración IP.
    4. - Realización de pruebas de conexión.
    5. - Interpretación de respuestas.
2. Procedimientos sistemáticos de verificación y prueba de elementos de conectividad de redes locales.

UNIDAD DIDÁCTICA 2. TIPOS DE INCIDENCIAS QUE SE PUEDEN PRODUCIR EN UNA RED DE ÁREA LOCAL.

1. Incidencias a nivel de conectividad del enlace.
2. Incidencias a nivel de red.

UNIDAD DIDÁCTICA 3. DETECCIÓN Y DIAGNÓSTICO DE INCIDENCIAS EN REDES DE ÁREA LOCAL.

1. Herramientas de diagnóstico de dispositivos de comunicaciones en redes locales.
2. Procesos de gestión de incidencias en redes locales.

UNIDAD DIDÁCTICA 4. COMPROBACIÓN DE CABLES DE PAR TRENZADO Y COAXIAL.

1. Categorías de herramientas de comprobación de cableado.
2. Analizadores o comprobadores de cable.
    1. - Características.
    2. - Procedimiento de comprobación de cables de par trenzado.
        1. * Circuito abierto.
        2. * Cortocircuito.
        3. * Hilos cruzados.
        4. * Pares cruzados.
        5. * Par dividido.
        6. * Detección de voltajes telefónicos.
        7. * Derivación en puente.
        8. * Detección de puertos Ethernet.
    3. - Procedimiento de comprobación de cables coaxiales.

4. - Procedimiento de detección de alimentación por Ethernet.
5. - Procedimientos de localización de cables utilizando tonos.

UNIDAD DIDÁCTICA 5. COMPROBACIÓN Y SOLUCIÓN DE INCIDENCIAS A NIVEL DE RED.

1. Herramientas de comprobación.
2. Detección de problemas relacionados con:
    1. - Tramas largas y cortas.
    2. - Tráfico excesivo.
    3. - Netware.
    4. - TCP/IP.
    5. - Configuración del Host.
    6. - Resolución de nombres.
    7. - NetBIOS.
    8. - Conexión al servidor http o proxy.
    9. - Conexión al servidor de correos.
    10. - Conexión al servidor de impresión.
    11. - Otros.

MÓDULO 7. 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

MÓDULO 8. GESTIÓN DE SEGURIDAD INFORMÁTICA EN ENTORNOS MÓVILES Y SISTEMAS DE CONTROL INDUSTRIAL

UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD EN ENTORNOS MÓVILES

1. Aplicaciones seguras en Cloud
2. Protección de ataques en entornos de red móvil
3. Plataformas de administración de la movilidad empresarial (EMM)
4. Redes WiFi seguras

UNIDAD DIDÁCTICA 2. CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL (IC)

1. Introducción
2. Amenazas y riesgos en los entornos IC
3. Mecanismo de defensa frente a ataques en entornos IC

MÓDULO 9. PROYECTO FIN DE MÁSTER

EUROINNOVA

INTERNATIONAL ONLINE EDUCATION

By
EDUCA EDTECH
Group