EUROINNOVA
INTERNATIONAL ONLINE EDUCATION

Máster Hackers + Titulación Universitaria

Elige aprender en la escuela
líder en formación online

ÍNDICE

Ver en la web

EUROINNOVA
INTERNATIONAL ONLINE EDUCATION

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

Ver en la web

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

Desde donde quieras y como quieras,

Elige Euroinnova

QS, sello de excelencia académica

Euroinnova: 5 estrellas en educación online

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.

QS WORLD UNIVERSITY RANKINGS

Ranking Educativo Innovatec

EUROPEAN EXCELLENCE EDUCATION

EL MUNDO

LOS MEJORES MASTERS EN CIBERSEGURIDAD ★ CyberEOP ★

MASTER

Ver en la web

ALIANZAS Y ACREDITACIONES

Ver en la web

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

oposiciones docentes

educaopen

enalde Alta Dirección Empresarial

EDUCA business school

ESIBE ESCUELA IBEROAMERICANA DE POSTGRADO

INNOVA SCHOOL OF MANAGEMENT

ceupe European Business School

Structuralia Engineering eLearning

UDAVINCI

Ver en la web

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

Ver en la web

EUROINNOVA
INTERNATIONAL ONLINE EDUCATION

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**

Solicitar información

MÉTODOS DE PAGO

Con la Garantía de:

educapay

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

mastercard maestro VISA PayPal

bizum amazon pay Pay G 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

Protección al Comprador

Ver en la web

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

Máster Hackers + Titulación Universitaria

DURACIÓN
1500 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

CREDITOS
5 ECTS

Titulación

Titulación Múltiple: - Titulación de Master Hackers 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 - 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.

Ver en la web

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con Número de Documento XXXXXXXXX ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación de EUROINNOVA en la convocatoria de XXX

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 (día) de (mes) del (año)

La Dirección General

NOMBRE DEL DIRECTOR ACADÉMICO

Sello

Firma del Alumno/a

NOMBRE DEL ALUMNO

Descripción

Con el presente Master Hackers recibirá una formación especializada en el campo del hacking. El hacking es altamente empleado para realizar auditorias de seguridad, comprometiendo y comprobando la seguridad de los sistemas informáticos, ya sean de redes WIFI, de páginas webs o de redes de área local. Con el presente Master Hackers recibirá la formación necesaria para poder abordar diferentes aspectos del hacking, ya sea mediante la búsqueda de exploit o usando herramientas especializadas para tal fin...

Objetivos

Los objetivos del máster de hackers son los siguientes: Conocer el Ethical Hacking. Aprender a realizar hacking wifi. Aprender a desarrollar exploits y a buscar vulnerabilidades. Conocer el Phishing y como los hackers lo emplean. Conocer el sistema de información UNEISO/IEC 27001:2017. Conocer el Big Data.

A quién va dirigido

El presente máster online está dirigido a todos los profesionales del mundo de la informática que quieran ampliar sus conocimientos y formarse en un mercado en continua evolución. Por lo que la formación adecuada y actualizada es indispensable para destacar en este mercado.

Ver en la web

EUROINNOVA
INTERNATIONAL ONLINE EDUCATION

Para qué te prepara

Este Master en Hackers te proporcionará los conocimientos necesarios para destacar en el mundo de la informática, especialmente en cuanto al hacking se refiere. Aprenderás y conocerás el ethical hacking, así como a realizar auditorias de seguridad a redes inalámbricas y conocer el desarrollo de exploits.

Salidas laborales

Los conocimientos adquiridos en esta formación te permiten aplicar tu aprendizaje, profesionalmente, en consultorías, así como en departamentos de informática de empresas de todos los sectores. Asimismo, te capacitan para desarrollar tu labor como jefe de proyectos, además de en las áreas de desarrollo y programación, ingeniería de software e ingeniería informática.

TEMARIO

PARTE 1. 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

PARTE 2. HACKING WIFI

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN: HACKING

1. Introducción
2. Historia del hacking
3. Tipos de hacking
4. Tipos de hacker

UNIDAD DIDÁCTICA 2. HARDWARE NECESARIO PREVIO AL HACK WIFI

1. Introducción
2. Hardware

UNIDAD DIDÁCTICA 3. TIPOS DE REDES WIFI Y CIFRADOS

1. Introducción
2. Estándares wifi

3. Cifrados wifi

UNIDAD DIDÁCTICA 4. DISTRIBUCIONES LINUX PARA EL HACK WIFI

1. Introducción
2. Sistemas operativos linux
3. Sistemas operativos utilizados en hacking wifi
    1. - Kali linux
    2. - Parrot
    3. - Wifislax

UNIDAD DIDÁCTICA 5. SOFTWARE UTILIZADO PARA EL HACK WIFI

1. Introducción
2. Herramientas de wifislax
3. Aircrack
4. Cain & Abel

UNIDAD DIDÁCTICA 6. PROCESO PRÁCTICO DE HACKEO DE RED WIFI

1. Introducción al caso práctico
2. Desarrollo del caso práctico
3. Resultados del caso práctico

UNIDAD DIDÁCTICA 7. CONSEJOS DE SEGURIDAD

1. Introducción
2. Recomendaciones

UNIDAD DIDÁCTICA 8. LEGISLACIÓN

1. Introducción
2. Leyes anti piratería

PARTE 3. DESAROLLO DE EXPLOITS Y BÚSQUEDA DE VULNERABILIDADES

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN EXPLOITS

1. Historia de los exploits
2. Definición de exploit y cómo funciona
3. Tipología de exploits
4. Uso común de los exploits y medidas de protección

UNIDAD DIDÁCTICA 2. METAEXPLOIT Y CREACIÓN DE EXPLOIT

1. Introducción a metaexploit
2. Creando nuestro primer exploit
3. Post-Explotación
4. Meterpreter

UNIDAD DIDÁCTICA 3. TIPOS DE EXPLOITS

1. Code injection
2. Cross-site request forgery
3. Cross-site scripting
4. SQL injection
5. Buffer overflow
6. Heap overflow
7. Stack buffer overflow
8. Integer overflow
9. Return-to-libc attack
10. Format string attack

UNIDAD DIDÁCTICA 4. UTILIZANDO ARMITAGE

1. Introducción Armitage
2. Atacando con Armitage
3. Post-Explotación Armitage
4. Facilidades Armitage

UNIDAD DIDÁCTICA 5. INTRODUCCIÓN VULNERABILIDADES

1. Qué es una vulnerabilidad
2. Vulnerabilidad vs Amenaza
3. Análisis de vulnerabilidades
4. Evitar vulnerabilidades

UNIDAD DIDÁCTICA 6. TIPOS DE VULNERABILIDADES

1. Gravedad de las vulnerabilidades
2. Vulnerabilidades del sistema
3. Vulnerabilidades web

UNIDAD DIDÁCTICA 7. DESCUBRIR VULNERABILIDADES

1. Utilizar metasploit para descubrir vulnerabilidades
2. Prueba de penetración
3. Herramientas para escanear vulnerabilidades

UNIDAD DIDÁCTICA 8. UTILIZANDO VULNERABILIDADES JUNTO A EXPLOITS

1. Vulnerabilidades en Linux
2. Vulnerabilidades en Windows
3. Vulnerabilidades en Android

UNIDAD DIDÁCTICA 9. RECOMENDACIONES FRENTE A EXPLOITS Y VULNERABILIDADES

1. Recomendaciones de seguridad frente a exploits
2. Recomendaciones de seguridad frente a vulnerabilidades
3. Herramientas de seguridad

UNIDAD DIDÁCTICA 10. CASO PRÁCTICO

1. Introducción
2. Objetivos
3. Realización

PARTE 4. INGENIERIA SOCIAL, PHISHING Y HACKING WEB

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA INGENIERÍA SOCIAL

1. Definición ingeniería social
2. Como evitar la ingeniería
3. Formación de empleados
4. Victimas mas frecuentes de los ataques

UNIDAD DIDÁCTICA 2. RECOPILAR INFORMACIÓN

1. OSINT
2. Doxing
3. Metadatos
4. Buscar información en la web

UNIDAD DIDÁCTICA 3. HERRAMIENTAS INGENIERÍA SOCIAL

1. FOCA
2. MALTEGO
3. GOOGLE HACKING
4. THEHARVESTER
5. SET

UNIDAD DIDÁCTICA 4. TECNICAS DE ATAQUES

1. Clasificación de ataques
2. Scareware
3. Utilizar dominios con erratas
4. USB olvidado y Piggyback
5. Caso practico

UNIDAD DIDÁCTICA 5. PREVENCION DE ATAQUES

1. Informar de los ataque comunes
2. Comprobar la seguridad antes ataques
3. Planear un sistema de contigencia
4. Lo que nunca te van a pedir
5. Pensar antes de actuar

UNIDAD DIDÁCTICA 6. INTRODUCCION PHISHING

1. ¿Que es el phishing?
2. Historia del phishing

3. Técnicas de phishing
4. Identificar un email falso y que hacer con el

UNIDAD DIDÁCTICA 7. PHISHING

1. Como funciona el phishing
2. Anti-phishing
3. Objetivos del phishing
4. Casos prácticos ataques

UNIDAD DIDÁCTICA 8. MAN IN THE MIDDLE

1. Introduccion Man In The Middle
2. Protegernos de ataques Man In The Middle
3. Lugares comunes ataques Man In The Middle
4. Caso practico

UNIDAD DIDÁCTICA 9. HACKING WEB

1. Descubriendo subdominios
2. Escaneando servidores web
3. Escaneando huella digital servidor web
4. Hackeando un sitio Wordpress con WPScan
5. Securizar nuestro sitio web

PARTE 5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN UNE-ISO/IEC 27001:2017

UNIDAD DIDÁCTICA 1. NATURALEZA Y DESARROLLO DE LA SEGURIDAD DE LA INFORMACIÓN

1. La sociedad de la información
2. ¿Qué es la seguridad de la información?
3. Importancia de la seguridad de la información
4. Principios básicos de seguridad de la información: confidencialidad, integridad y disponibilidad
5. Descripción de los riesgos de la seguridad
6. Selección de controles
7. Factores de éxito en la seguridad de la información

UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE SEGURIDAD DE LA INFORMACIÓN

1. Marco legal y jurídico de la seguridad de la información
2. Normativa comunitaria sobre seguridad de la información
3. Normas sobre gestión de la seguridad de la información: Familia de Normas ISO 27000
4. Legislación española sobre seguridad de la información

UNIDAD DIDÁCTICA 3. BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN: NORMA ISO/IEC 27002

1. Aproximación a la norma ISO/IEC 27002
2. Alcance de la Norma ISO/IEC 27002
3. Estructura de la Norma ISO/IEC 27002

4. Evaluación y tratamiento de los riesgos de seguridad

UNIDAD DIDÁCTICA 4. POLÍTICA DE SEGURIDAD, ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE ACTIVOS

1. Política de seguridad de la información
2. Organización de la seguridad de la información
3. Organización interna de la seguridad de la información
4. Grupos o personas externas: el control de acceso a terceros
5. Clasificación y control de activos de seguridad de la información
6. Responsabilidad por los activos de seguridad de la información
7. Clasificación de la información

UNIDAD DIDÁCTICA 5. SEGURIDAD FÍSICA, AMBIENTAL Y DE LOS RECURSOS HUMANOS

1. Seguridad de la información ligada a los recursos humanos
2. Medidas de seguridad de la información antes del empleo
3. Medidas de seguridad de la información durante el empleo
4. Seguridad de la información en la finalización de la relación laboral o cambio de puesto de trabajo
5. Seguridad de la información ligada a la seguridad física y ambiental o del entorno
6. Las áreas seguras
7. Los equipos de seguridad

UNIDAD DIDÁCTICA 6. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

1. Aproximación a la gestión de las comunicaciones y operaciones
2. Procedimientos y responsabilidades operacionales
3. Gestión de la prestación de servicios de terceras partes
4. Planificación y aceptación del sistema
5. Protección contra códigos maliciosos y móviles
6. Copias de seguridad de la información
7. Gestión de la seguridad de la red
8. Gestión de medios
9. El intercambio de información
10. Los servicios de comercio electrónico
11. Supervisión para la detección de actividades no autorizadas

UNIDAD DIDÁCTICA 7. EL CONTROL DE ACCESOS A LA INFORMACIÓN

1. El control de accesos: generalidades, alcance y objetivos
2. Requisitos de negocio para el control de accesos
3. Gestión de acceso de usuario
4. Responsabilidades del usuario
5. Control de acceso a la red
6. Control de acceso al sistema operativo
7. Control de acceso a las aplicaciones y a la información
8. Informática móvil y teletrabajo

UNIDAD DIDÁCTICA 8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

1. Objetivos del desarrollo y mantenimiento de sistemas de información
2. Requisitos de seguridad de los sistemas de información
3. Tratamiento correcto de la información en las aplicaciones
4. Controles criptográficos
5. Seguridad de los archivos del sistema
6. Seguridad de los procesos de desarrollo y soporte
7. Gestión de la vulnerabilidad técnica

UNIDAD DIDÁCTICA 9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN Y DE LA CONTINUIDAD DEL NEGOCIO

1. La gestión de incidentes en la seguridad de la información
2. Notificación de eventos y puntos débiles en la seguridad de la información
3. Gestión de incidentes y mejoras en la seguridad de la información
4. Gestión de la continuidad del negocio
5. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

UNIDAD DIDÁCTICA 10. CUMPLIMIENTO DE LAS PREVISIONES LEGALES Y TÉCNICAS

1. Cumplimiento de los requisitos legales
2. Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico
3. Consideraciones de la auditoría de los sistemas de información

UNIDAD DIDÁCTICA 11. LA NORMA UNE-EN-ISO/IEC 27001:2017

1. Objeto y ámbito de aplicación
2. Relación con la Norma ISO/IEC 27002:2022
3. Definiciones y términos de referencia
4. Beneficios aportados por un sistema de seguridad de la información
5. Introducción a los sistemas de gestión de seguridad de la información

UNIDAD DIDÁCTICA 12. IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD EN LA ORGANIZACIÓN

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

UNIDAD DIDÁCTICA 13. SEGUIMIENTO DE LA IMPLANTACIÓN DEL SISTEMA

1. Operación
2. Evaluación del desempeño
3. Mejora

PARTE 6. BIG DATA

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL BIG DATA

1. ¿Qué es Big Data?
2. La era de las grandes cantidades de información: historia del big data
3. La importancia de almacenar y extraer información
4. Big Data enfocado a los negocios
5. Open Data
6. Información pública
7. IoT (Internet of Things-Internet de las cosas)

UNIDAD DIDÁCTICA 2. FASES DE UN PROYECTO DE BIG DATA

1. Diagnóstico inicial
2. Diseño del proyecto
3. Proceso de implementación
4. Monitorización y control del proyecto
5. Responsable y recursos disponibles
6. Calendarización
7. Alcance y valoración económica del proyecto

UNIDAD DIDÁCTICA 3. BIG DATA Y MARKETING

1. Apoyo del Big Data en el proceso de toma de decisiones
2. Toma de decisiones operativas
3. Marketing estratégico y Big Data
4. Nuevas tendencias en management

UNIDAD DIDÁCTICA 4. INTELIGENCIA DE NEGOCIO Y HERRAMIENTAS DE ANALÍTICA

1. Tipo de herramientas BI
2. Productos comerciales para BI
3. Productos Open Source para BI
4. Beneficios de las herramientas de BI

UNIDAD DIDÁCTICA 5. PRINCIPALES PRODUCTOS DE BUSINESS INTELLIGENCE

1. Cuadros de Mando Integrales (CMI)
2. Sistemas de Soporte a la Decisión (DSS)
3. Sistemas de Información Ejecutiva (EIS)

UNIDAD DIDÁCTICA 6: DEL BIG DATA AL LINKED OPEN DATA

1. Concepto de web semántica
2. Linked Data Vs Big Data
3. Lenguaje de consulta SPARQL

¿Te ha parecido interesante esta información?

Si aún tienes dudas, nuestro equipo de asesoramiento académico estará encantado de resolverlas.

Pregúntanos sobre nuestro método de formación, nuestros profesores, las becas o incluso simplemente conócenos.

Solicita información sin compromiso

¡Matricularme ya!

¡Encuéntranos aquí!

Edificio Educa Edtech

Camino de la Torrecilla N.º 30 EDIFICIO EDUCA EDTECH, C.P. 18.200, Maracena (Granada)

900 831 200

formacion@euroinnova.com

www.euroinnova.edu.es

Horario atención al cliente

Lunes a viernes: 9:00 a 20:00h Horario España

¡Síguenos para estar al tanto de todas nuestras novedades!

Ver en la web

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

EUROINNOVA

INTERNATIONAL ONLINE EDUCATION

By
EDUCA EDTECH
Group