EDUCA
business school

Máster en Ciberseguridad Avanzada + Titulación universitaria

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

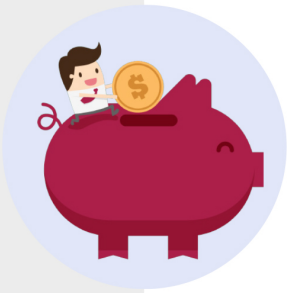
Con nuestra metodología estudiarán **100% online** y nuestros alumnos/as tendrán acceso los 365 días del año a la plataforma educativa.

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.

Máster en Ciberseguridad Avanzada + Titulación universitaria

DURACIÓN
1500 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

CREDITOS
8 ECTS

Titulación

Doble Titulación: - Titulación de Máster en Ciberseguridad Avanzada con 1500 horas expedida por EDUCA BUSINESS SCHOOL como Escuela de Negocios Acreditada para la Impartición de Formación Superior de Postgrado, con Validez Profesional a Nivel Internacional - Titulación de Curso en Consultor en Seguridad Informática IT: Ethical Hacking con 200 horas y 8 ECTS expedida por UTAMED - Universidad Tecnológica Atlántico Mediterráneo.

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 XXXXXXXXX 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 (Núm. Resolución 6049)

Descripción

El Máster en Ciberseguridad Avanzada es tu puerta de entrada al vibrante mundo de la seguridad digital, un sector en constante crecimiento con una demanda laboral insaciable. En un entorno donde las amenazas digitales evolucionan vertiginosamente, dominar habilidades como el Ethical Hacking, el análisis de vulnerabilidades y la protección de datos en la nube no solo es relevante, sino imprescindible. Este máster te capacitará para identificar y mitigar riesgos, desarrollar exploits efectivos y entender la ingeniería social y el phishing. Además, te familiarizarás con normativas cruciales como la UNE-ISO/IEC 27001:2017, que son esenciales para cualquier organización comprometida con la seguridad de la información. Al elegir este máster, te posicionas como un experto listo para afrontar los desafíos de la ciberseguridad y liderar el cambio en un mundo cada vez más interconectado.

Objetivos

'- Identificar vulnerabilidades en sistemas y redes para mejorar la seguridad informática. - Analizar y aplicar técnicas avanzadas de hacking ético para detectar fallos de seguridad. - Implementar medidas de protección contra ataques de ingeniería social y phishing. - Desarrollar y probar exploits para evaluar la seguridad en aplicaciones y sistemas. - Configurar sistemas de gestión de seguridad basados en la norma ISO/IEC 27001. - Utilizar herramientas de análisis de Big Data para mejorar la inteligencia de negocio. - Auditar sistemas de seguridad en la nube y asegurar el cumplimiento normativo.

EDUCA business school

Para qué te prepara

El Máster en Ciberseguridad Avanzada está dirigido a profesionales y titulados del sector tecnológico que desean profundizar en áreas críticas como el ethical hacking, la seguridad en la nube y el desarrollo de exploits. Este programa avanzado es ideal para quienes buscan mejorar sus habilidades en la protección de sistemas, implementación de SGSI y gestión de proyectos de Big Data.

A quién va dirigido

El Máster en Ciberseguridad Avanzada te capacita para identificar y mitigar amenazas en redes y sistemas operativos, utilizando técnicas de ethical hacking y fortaleciendo la seguridad en la nube. Aprenderás a evaluar vulnerabilidades, implementar medidas de protección efectivas y gestionar sistemas de seguridad de la información conforme a la normativa vigente. Además, desarrollarás habilidades en la prevención de ataques de ingeniería social y phishing, asegurando un entorno digital robusto y fiable.

Salidas laborales

'- Consultor de ciberseguridad - Analista de vulnerabilidades - Ingeniero de seguridad en redes - Especialista en seguridad en la nube - Auditor de sistemas de gestión de seguridad - Desarrollador de exploits - Experto en hacking ético - Profesional en big data aplicado a la ciberseguridad - Especialista en prevención de ataques de ingeniería social y phishing

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. CIBERSEGURIDAD Y SOCIEDAD DE LA INFORMACIÓN

1. ¿Qué es la ciberseguridad?
2. La sociedad de la información
3. Diseño, desarrollo e implantación
4. Factores de éxito en la seguridad de la información
5. Soluciones de Ciberseguridad y Ciberinteligencia CCN-CERT

UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. Estándares y Normas Internacionales sobre los SGSI. ISO 27001 e ISO 27002
2. Legislación: Leyes aplicables a los SGSI

UNIDAD DIDÁCTICA 3. INTRODUCCIÓN A LA NIS2

1. Historia y evolución de la NIS2
2. Objetivos y alcance de la NIS2
3. Diferencias entre NIS1 y NIS2
4. Sectores críticos afectados por la NIS2

UNIDAD DIDÁCTICA 4. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1. Plan de implantación del SGSI
2. Análisis de riesgos
3. Gestión de riesgos

UNIDAD DIDÁCTICA 5. IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD EN LA ORGANIZACIÓN

1. Contexto
2. Liderazgo
3. Planificación
4. Soporte 213

UNIDAD DIDÁCTICA 6. SEGUIMIENTO DE LA IMPLANTACIÓN DEL SISTEMA

1. Operación
2. Evaluación del desempeño
3. Mejora

UNIDAD DIDÁCTICA 7. AUDITORÍA DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN POR LA DIRECCIÓN

1. El porqué de la auditoría
2. La auditoría interna
3. El proceso de certificación

UNIDAD DIDÁCTICA 8. REVISIÓN POR LA DIRECCIÓN Y MEJORA DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN

1. Revisión del sistema de gestión de la información por la dirección
2. Mejora del sistema de gestión de la seguridad de la información

UNIDAD DIDÁCTICA 9. GUÍAS DE SEGURIDAD: NORMATIVAS Y BUENAS PRÁCTICAS

1. Introducción a las guías de seguridad CCN-STIC
2. CCN-STIC-800 Glosario de términos y abreviaturas del ENS
3. CCN-STIC-801 Responsabilidades y funciones en el ENS
4. CCN-STIC-802 Auditoría del ENS
5. CCN-STIC-803 Valoración de Sistemas en el ENS
6. CCN-STIC-804 Medidas de implantación del ENS
7. CCN-STIC-805 Política de seguridad de la información
8. CCN-STIC-806 Plan de adecuación al ENS
9. CCN-STIC-807 Criptología de empleo en el ENS
10. CCN-STIC-808 Verificación del cumplimiento del ENS

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. FUENTES DE DATOS

1. Definición y relevancia de la selección de las fuentes de datos
2. Naturaleza de las fuentes de datos Big Data

UNIDAD DIDÁCTICA 3. OPEN DATA

1. Definición, Beneficios y Características
2. Ejemplo de uso de Open Data

UNIDAD DIDÁCTICA 4. 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 5. BUSINESS INTELLIGENCE Y LA SOCIEDAD DE LA INFORMACIÓN

1. Definiendo el concepto de Business Intelligence y sociedad de la información
2. Arquitectura de una solución de Business Intelligence
3. Business Intelligence en los departamentos de la empresa
4. Conceptos de Plan Director, Plan Estratégico y Plan de Operativa Anual
5. Sistemas operacionales y Procesos ETL en un sistema de BI
6. Ventajas y Factores de Riesgos del Business Intelligence

UNIDAD DIDÁCTICA 6. 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 7. 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 8. DEL BIG DATA AL LINKED OPEN DATA

1. Concepto de web semántica

2. Linked Data Vs Big Data
3. Lenguaje de consulta SPARQL

UNIDAD DIDÁCTICA 9. INTERNET DE LAS COSAS

1. Contexto Internet de las Cosas (IoT)
2. ¿Qué es IoT?
3. Elementos que componen el ecosistema IoT
4. Arquitectura IoT
5. Dispositivos y elementos empleados
6. Ejemplos de uso
7. Retos y líneas de trabajo futuras


EDUCA
business school


By
EDUCA EDTECH
Group