

Máster en Administración de Sistemas CISCO + 60 Créditos ECTS





**Elige aprender en la escuela
líder en formación para profesionales**

ÍNDICE

1 | Somos INESEM

**4 | By EDUCA
EDTECH
Group**

**7 | Programa
Formativo**

2 | Rankings

**5 | Metodología
LXP**

8 | Temario

**3 | Alianzas y
acreditaciones**

**6 | Razones por las
que elegir
Inesem**

9 | Contacto

[Ver en la web](#)

SOMOS INESEM

INESEM es una **Business School online** especializada con un fuerte sentido transformacional. En un mundo cambiante donde la tecnología se desarrolla a un ritmo vertiginoso nosotros somos activos, evolucionamos y damos respuestas a estas situaciones.

Apostamos por **aplicar la innovación tecnológica a todos los niveles en los que se produce la transmisión de conocimiento**. Formamos a profesionales altamente capacitados para los trabajos más demandados en el mercado laboral; profesionales innovadores, emprendedores, analíticos, con habilidades directivas y con una capacidad de añadir valor, no solo a las empresas en las que estén trabajando, sino también a la sociedad. Y todo esto lo podemos realizar con una base sólida sostenida por nuestros objetivos y valores.

Más de
18
años de
experiencia

Más de
300k
estudiantes
formados

Más de un
90%
tasa de
empleabilidad

Hasta un
100%
de financiación

Hasta un
50%
de los estudiantes
repite

Hasta un
25%
de estudiantes
internacionales

[Ver en la web](#)



A way to learn, a way to grow
Elige Inesem



QS, sello de excelencia académica
Inesem: 5 estrellas en educación online

RANKINGS DE INESEM

INESEM Business School ha obtenido reconocimiento tanto a nivel nacional como internacional debido a su firme compromiso con la innovación y el cambio.

Para evaluar su posición en estos rankings, se consideran diversos indicadores que incluyen la percepción online y offline, la excelencia de la institución, su compromiso social, su enfoque en la innovación educativa y el perfil de su personal académico.



[Ver en la web](#)

ALIANZAS Y ACREDITACIONES

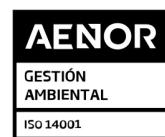
Relaciones institucionales



Relaciones internacionales



Acreditaciones y Certificaciones



[Ver en la web](#)

BY EDUCA EDTECH

Inesem 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.



ONLINE EDUCATION



[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 INESEM

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 Inesem.

2. Nuestro Equipo

En la actualidad, Inesem 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



Inesem 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](#)

4. Calidad AENOR

- ✓ Somos Agencia de Colaboración N°99000000169 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. 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**.

[Ver en la web](#)

Máster en Administración de Sistemas CISCO + 60 Créditos ECTS



DURACIÓN
1500 horas



MODALIDAD
ONLINE



ACOMPAÑAMIENTO
PERSONALIZADO



CREDITOS
60 ECTS

Titulación

Titulación de Máster de Formación Permanente en Administración de Sistemas CISCO con 1500 horas y 60 ECTS expedida por UTAMED - Universidad Tecnológica Atlántico Mediterráneo.



INESEM BUSINESS SCHOOL

como centro acreditado para la impartición de acciones formativas

expide el presente título propio

NOMBRE DEL ALUMNO/A

con número de documento XXXXXXXX ha superado los estudios correspondientes de

NOMBRE DEL CURSO

con una duración de XXX horas, perteneciente al Plan de Formación de Inesem Business School.

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

Con una calificación XXXXXXXXXXXXXXXXX.

Y para que conste expedido la presente titulación en Granada, a [día] de [mes] del [año].

Aviso legal | Condiciones de uso | Política de privacidad | Política de cookies | Aviso legal y condiciones de uso | Política de privacidad y cookies | Aviso legal y condiciones de uso | Política de privacidad y cookies

NOMBRE ALUMNO/A
Firma del Alumno/a

NOMBRE DE ÁREA MANAGER
La Dirección Académica



Con Estatuto Consultivo, Categoría Especial del Consejo Económico y Social de la UNESCO (Nº resolución 60/04)

Ver en la web

Descripción

En la actualidad, los sistemas CISCO y las redes son elementos fundamentales en el ámbito de las tecnologías de la información y las comunicaciones. El Master en Administración de Sistemas CISCO + Prácticas ofrece una formación completa y especializada en el área de administración de redes CISCO, combinando conocimientos teóricos y prácticos para capacitar a los profesionales en las habilidades necesarias para gestionar y mantener infraestructuras de red de manera eficiente. Una de las características distintivas de este programa es su enfoque en la formación online, lo que permite a los estudiantes acceder a los contenidos y recursos desde cualquier lugar y en cualquier momento. Y cuenta con un equipo de profesores especializados en el sector.

Objetivos

- Adquirir conocimientos sólidos en sistemas CISCO y redes.
- Dominar la instalación y configuración de routers CISCO.
- Desarrollar habilidades en la administración de sistemas microinformáticos y redes.
- Comprender y aplicar los sistemas operativos en red.
- Adquirir conocimientos en seguridad informática y protección de redes.
- Conocer los servicios de red y su implementación en entornos CISCO.
- Realizar prácticas profesionales para consolidar los conocimientos y obtener experiencia laboral.

Para qué te prepara

Este Master en Administración de Sistemas CISCO + Prácticas está dirigido a profesionales del ámbito de las tecnologías de la información y las comunicaciones que deseen especializarse en la administración de sistemas CISCO y redes. También es adecuado para aquellos que buscan actualizar sus conocimientos y adquirir nuevas habilidades en este campo en constante evolución.

A quién va dirigido

Este Master en Administración de Sistemas CISCO + Prácticas te prepara para asumir roles clave en la administración de sistemas CISCO y redes. Te brinda los conocimientos y habilidades necesarios para diseñar, implementar y mantener infraestructuras de red basadas en tecnología CISCO. Además, te capacita en la configuración y gestión de routers, así como en la seguridad informática y la protección de redes.

[Ver en la web](#)

Salidas laborales

Las salidas profesionales de este Master en Administración de Sistemas CISCO + Prácticas son administradores de redes, especialistas en sistemas CISCO, técnicos en sistemas microinformáticos y redes, consultores de seguridad informática, entre otros roles relacionados. También tendrán la oportunidad de desarrollar su carrera en empresas y organizaciones que utilizan tecnología CISCO.

[Ver en la web](#)

TEMARIO

MÓDULO 1. SISTEMAS MICROINFORMÁTICOS Y REDES

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN Y COMPONENTES DEL PC

1. Breve historia del PC
2. Componentes e interior del PC
3. Comprensión de los componentes del PC

UNIDAD DIDÁCTICA 2. ELEMENTOS NUCLEARES DEL PC

1. La placa base y la fuente de alimentación
2. La BIOS/SET-UP
3. El procesador
4. La memoria
5. El disco duro
6. Búsqueda a través de Internet de diferentes tipos de hardware, comparativas de precio, etc

UNIDAD DIDÁCTICA 3. ELEMENTOS DE CONEXIÓN Y TARJETAS

1. Las conexiones: Conexión USB, RDSI, ADSL, CABLE
2. Las diferentes tarjetas
3. Reflexión sobre los distintos elementos de conexión y las diferentes tarjetas compatibles con un PC

UNIDAD DIDÁCTICA 4. LOS PERIFÉRICOS Y PORTÁTILES

1. Los periféricos
2. El auge de los portátiles
3. Identificación de los periféricos y reflexión sobre la importancia de los portátiles
4. Búsqueda a través de Internet de periféricos, comparativas de precio, características, etc

UNIDAD DIDÁCTICA 5. INTRODUCCIÓN A LA RED

1. Elementos principales de una red
2. Tecnología de redes
3. Soporte para la continuidad de la actividad

UNIDAD DIDÁCTICA 6. ESTANDARIZACIÓN DE PROTOCOLOS

1. Modelo OSI
2. Enfoque pragmático del modelo de capas
3. Estándares y organismos

UNIDAD DIDÁCTICA 7. TRANSMISIÓN DE DATOS EN LA CAPA FÍSICA

1. Papel de una interfaz de red

[Ver en la web](#)

2. Opciones y parámetros de configuración
3. Arranque desde la red
4. Codificación de los datos
5. Conversión de las señales
6. Soportes de transmisión

UNIDAD DIDÁCTICA 8. SOFTWARE DE COMUNICACIÓN

1. Configuración de la tarjeta de red
2. Instalación y configuración del controlador de la tarjeta de red
3. Pila de protocolos
4. Detección de un problema de red

UNIDAD DIDÁCTICA 9. ARQUITECTURA DE RED E INTERCONEXIÓN

1. Topologías
2. Elección de la topología de red adaptada
3. Gestión de la comunicación
4. Interconexión de redes

UNIDAD DIDÁCTICA 10. CAPAS BAJAS DE LAS REDES PERSONALES Y LOCALES

1. Capas bajas e IEEE
2. Ethernet e IEEE 802.3
3. Token Ring e IEEE 802.5
4. Wi-Fi e IEEE 802.11
5. Bluetooth e IEEE 802.15
6. Otras tecnologías

UNIDAD DIDÁCTICA 11. REDES MAN Y WAN, PROTOCOLOS

1. Interconexión de la red local
2. Acceso remoto y redes privadas virtuales

UNIDAD DIDÁCTICA 12. PROTOCOLOS DE CAPAS MEDIAS Y ALTAS

1. Principales familias de protocolos
2. Protocolo IP versión 4
3. Protocolo IP versión 6
4. Otros protocolos de capa Internet
5. Voz sobre IP (VoIP)
6. Protocolos de transporte TCP y UDP
7. Capa de aplicación TCP/IP

UNIDAD DIDÁCTICA 13. PROTECCIÓN DE UNA RED

1. Comprensión de la necesidad de la seguridad
2. Herramientas y tipos de ataque
3. Conceptos de protección en la red local
4. Protección de la interconexión de redes

[Ver en la web](#)

UNIDAD DIDÁCTICA 14. REPARACIÓN DE RED

1. Introducción a la reparación de red
2. Diagnóstico en capas bajas
3. Utilización de herramientas TCP/IP adaptadas
4. Herramientas de análisis de capas altas

UNIDAD DIDÁCTICA 15. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1. Seguridad a Nivel Físico
2. Seguridad a Nivel de Enlace
3. Seguridad a Nivel de Red
4. Seguridad a Nivel de Transporte
5. Seguridad a Nivel de Aplicación

MÓDULO 2. CISCO: EXPERTO EN INSTALACIÓN Y CONFIGURACIÓN DE ROUTER

UNIDAD DIDÁCTICA 1. PRESENTACIÓN

1. Conceptos básicos
2. Dispositivos de una Red
3. Servidores de Aplicaciones
4. Descripción y conceptualización de los mecanismos de comunicación de equipo a equipo en una red
5. Redes de Área Local y Redes de Área Amplia (LAN y WAN)

UNIDAD DIDÁCTICA 2. SEGURIDAD DE RED

1. Seguridad de red
2. Amenazas
3. Defensas

UNIDAD DIDÁCTICA 3. CONTROL DE ACCESO

1. Control de acceso

UNIDAD DIDÁCTICA 4. SOFTWARE CISCO PACKET TRACER

1. Cisco - Packet Tracer
2. Configuración de Equipos

UNIDAD DIDÁCTICA 5. AJUSTES

1. Ajustes AAA
2. Configuración AAA

UNIDAD DIDÁCTICA 6. ROUTERS

1. Routers

[Ver en la web](#)

UNIDAD DIDÁCTICA 7. REGISTROS Y MENSAJES

1. Registros y Mensajes

UNIDAD DIDÁCTICA 8. LISTAS DE ACCESO (ACL)

1. Listas De Acceso (ACL)
2. Práctica ACL
3. ACL's continuación

UNIDAD DIDÁCTICA 9. CORTAFUEGOS

1. Firewalls
2. Cortafuegos CBAC
3. Práctica CBAC
4. Cortafuegos basados en zonas
5. Ejercicios ZBF

UNIDAD DIDÁCTICA 10. SISTEMAS DE PREVENCIÓN DE INTRUSIONES(IPS)

1. Seguridad
2. Seguridad en capa 2
3. Consideraciones
4. Puertos
5. Funciones avanzadas
6. VPN, ASA, Wireless, VOIP
7. Acceso Remoto
8. Autoevaluación

MÓDULO 3. SISTEMAS OPERATIVOS EN RED

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LOS SISTEMAS OPERATIVOS EN RED

1. Definición de NOS
2. Componentes
3. Diferencias entre un sistema operativo en red y uno distribuido
4. NOS más utilizados

UNIDAD DIDÁCTICA 2. WINDOWS SERVER

1. ¿Qué es Windows Server? Versiones
2. Active Directory
3. Instalación de directorio activo
4. Creación de usuarios en Active Directory
5. Conexión al directorio activo

UNIDAD DIDÁCTICA 3. LINUX SERVER

1. ¿Qué es Linux?
2. Mejores distribuciones Linux para servidores

[Ver en la web](#)

3. OpenLDAP
4. Instalar OpenLDAP en Linux
5. Configuración inicial OpenLDAP
6. Creación de grupos y usuarios en OpenLDAP
7. Conexión a OpenLDAP

UNIDAD DIDÁCTICA 4. SEGURIDAD EN SISTEMAS OPERATIVOS EN RED

1. Seguridad informática
2. Amenazas comunes
3. Medidas de seguridad para proteger nuestro servidor

MÓDULO 4. REDES LOCALES

UNIDAD DIDÁCTICA 1. CONCEPTOS DE UNA RED DE ÁREA LOCAL

1. Redes de área local
2. Equipos de conectividad
3. Sistemas operativos de red
4. Medios de transmisión

UNIDAD DIDÁCTICA 2. PROTOCOLOS DE UNA RED DE ÁREA LOCAL

1. Introducción a los protocolos
2. Modelo de Interconexión de Sistemas Abiertos (OSI)
3. Modelo TCP/IP

UNIDAD DIDÁCTICA 3. RESOLUCIÓN DE PROBLEMAS CON EL CABLEADO

1. Armario de comunicaciones
2. Comprobaciones de la instalación de red
3. Analizadores o comprobadores de cable

UNIDAD DIDÁCTICA 4. DIAGNÓSTICO EN REDES LOCALES

1. Herramientas de diagnóstico
2. Análisis especializado
3. Herramientas de gestión de red

UNIDAD DIDÁCTICA 5. MONITORIZACIÓN DE RED

1. Tipos de información de monitorización
2. Acceso a la información de gestión
3. Mecanismos de monitorización: sondeo y notificaciones
4. Gestión de prestaciones
5. Métricas

MÓDULO 5. SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE

[Ver en la web](#)

LOS EQUIPOS INFORMÁTICOS

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

UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO

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

UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS

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

UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD

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

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

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

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

1. Determinación de los perímetros de seguridad física
2. Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
3. Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
4. Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro

[Ver en la web](#)

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

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS

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

UNIDAD DIDÁCTICA 8. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

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

UNIDAD DIDÁCTICA 9. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

- 1. Introducción al análisis de riesgos
- 2. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
- 3. Particularidades de los distintos tipos de código malicioso
- 4. Principales elementos del análisis de riesgos y sus modelos de relaciones
- 5. Metodologías cualitativas y cuantitativas de análisis de riesgos
- 6. Identificación de los activos involucrados en el análisis de riesgos y su valoración
- 7. Identificación de las amenazas que pueden afectar a los activos identificados previamente
- 8. Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja

- blanca y de caja negra
- 9. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
 - 10. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
 - 11. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
 - 12. Determinación de la probabilidad e impacto de materialización de los escenarios
 - 13. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
 - 14. Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
 - 15. Relación de las distintas alternativas de gestión de riesgos
 - 16. Guía para la elaboración del plan de gestión de riesgos
 - 17. Exposición de la metodología NIST SP 800
 - 18. Exposición de la metodología Magerit

UNIDAD DIDÁCTICA 10. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

- 1. Herramientas del sistema operativo tipo Ping, Traceroute, etc
- 2. Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc
- 3. Herramientas de análisis de vulnerabilidades tipo Nessus
- 4. Analizadores de protocolos tipo Wireshark, DSniff, Cain & Abel, etc
- 5. Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc
- 6. Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc

UNIDAD DIDÁCTICA 11. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS

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

UNIDAD DIDÁCTICA 12. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

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

MÓDULO 6. SERVICIOS DE RED

UNIDAD DIDÁCTICA 1. SERVICIOS EN LA RED

- 1. ¿Qué son los servicios de red?
- 2. Partes de una red
- 3. Componentes de una red

[Ver en la web](#)

4. Topología de red
5. Topología de anillo
6. Topología de árbol
7. Topología de bus
8. Topología de estrella
9. Topología de malla
10. Topología híbrida

UNIDAD DIDÁCTICA 2. TIPOS DE SERVICIOS DE UNA RED

1. Protocolo de configuración dinámica de host (DHCP)
2. Protocolo simple de Administración de red (SNMP)
3. Correo electrónico
4. Protocolo de transferencia de archivos (FTP)
5. Domain Name System (DNS)
6. Telnet y SSH

UNIDAD DIDÁCTICA 3. INSTALAR SERVIDOR DHCP

1. ¿Qué es DHCP?
2. Instalación del servidor DHCP en Linux
3. Conectar un cliente Linux
4. Instalación del servidor DHCP en Windows Server
5. Conectar un cliente Windows

UNIDAD DIDÁCTICA 4. INSTALADOR SERVIDOR DNS

1. ¿Qué es DNS?
2. Instalación del servidor DNS en Linux
3. Conectar un cliente Linux
4. Instalación del servidor DNS en Windows Server
5. Conectar un cliente Windows

UNIDAD DIDÁCTICA 5. SERVIDORES VIRTUALES

1. ¿Qué es un servidor virtual?
2. Características
3. Cloud vs VPS
4. Tipos de virtualización de servidores

MÓDULO 7. PROYECTO FIN DE MASTER

[Ver en la web](#)

Solicita información sin compromiso

¡Matricularme ya!

Teléfonos de contacto

 +34 958 050 240

¡Encuéntranos aquí!

Edificio Educa Edtech

Camino de la Torrecilla N.º 30 EDIFICIO EDUCA EDTECH,
Oficina 34, C.P. 18200, Maracena (Granada)

 formacion.continua@inesem.es

 www.formacioncontinua.eu

Horario atención al cliente

Lunes a Jueves: 09:00 a 20:00

Viernes: 9:00 a 14:00

[Ver en la web](#)

