EUROINNOVA
INTERNATIONAL ONLINE EDUCATION

UDAVINCI

# Maestría en Seguridad Informática. Especialización en Ethical Hacking

Una **nueva forma** de ver el mundo

# ÍNDICE


1 | Conoce **Udavinci**

2 | **Alianzas**

3 | **Ranking**

4 | **Registros** y acreditaciones

5 | By **EDUCA EDTECH Group**

6 | **Modelo Educativo**

7 | **Razones** por las que elegir Udavinci

8 | **Becas y Financiamiento**

9 | Formas de **pago**

10 | **Programa** Formativo

11 | **Programas de Estudios**

12 | **Contacto**


Ver en la web

UDAVINCI

## CONOCE UDAVINCI

**UDAVINCI** es la primera universidad mexicana 100% en línea que cumple los estándares europeos con calidad. Con más de 19 años de experiencia en la formación virtual, nuestros programas académicos cuentan con el Reconocimiento de Validez Oficial de Estudios (RVOE) otorgado por la SEP.

| | | |
|---|---|---|
| Más de **19** años de experiencia | Más de **1k** alumnos al año | Hasta un **80%** tasa empleabilidad |
| Hasta un **100%** de financiación | Hasta un **50%** de los estudiantes repite | Hasta un **25%** de estudiantes internacionales |

Ver en la web

UDAVINCI

Universidad **100%**
**en línea** con calidad europea

## ALIANZAS

Compartir conocimientos, modelos y prácticas educativas es esencial para el desarrollo de una comunidad educativa próspera. Es por eso que a nuestra causa se incorpora una cantidad importante de universidades nacionales e internacionales con las que la **Universidad Da Vinci** tiene diversos tipos de alianzas, desde visitas, residencias, becas institucionales e intercambios académicos y de investigación.

Ver en la web

UDAVINCI

## RANKING

Contamos con excelencia académica, acreditada por: Ranking Educativo Innovatec, Ranking Financial Magazine y recientemente el Ranking Webometrics.

Ranking Educativo Innovatec

EUROPEAN EXCELLENCE EDUCATION

Webometrics RANKING WEB OF UNIVERSITIES

Ver en la web

UDAVINCI

# REGISTROS Y ACREDITACIONES

Para asegurar la calidad y la mejora continua de la institución, la universidad se somete a procesos que acreditan sus programas de estudio con diferentes organismos reconocidos por la comunidad educativa.
Entre los registros y acreditaciones con las que cuenta para la prestación de sus servicios educativos están:

- Autorización para expedir títulos profesionales por parte de la Dirección de Instituciones Particulares de Educación Superior (DIPES).
- Registro de Establecimiento Educativo Federal en CDMX: 09PSU0537M.
- Registro de Establecimiento Educativo Estatal en La Paz: 03PSU0022V.
- Registro Nacional de Instituciones y Empresas Científicas y Tecnológicas (RENIECYT) No. 1703521.
- Constancia de la Secretaría del Trabajo y Previsión Social: UDV-0400818- FQ8-0013.
- Registro Federal de Contribuyentes: UDV040818FQ8.

SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA

SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

RENIECYT
Registro Nacional de Instituciones y Empresas Científicas y Tecnológicas

STPS
SECRETARÍA DE TRABAJO Y PREVISIÓN SOCIAL

Copaes ACREDITACIÓN
CONSEJO PARA LA ACREDITACIÓN DE LA EDUCACIÓN SUPERIOR, A.C.®

Ver en la web

UDAVINCI

## BY EDUCA EDTECH

**Universidad Da Vinci** 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

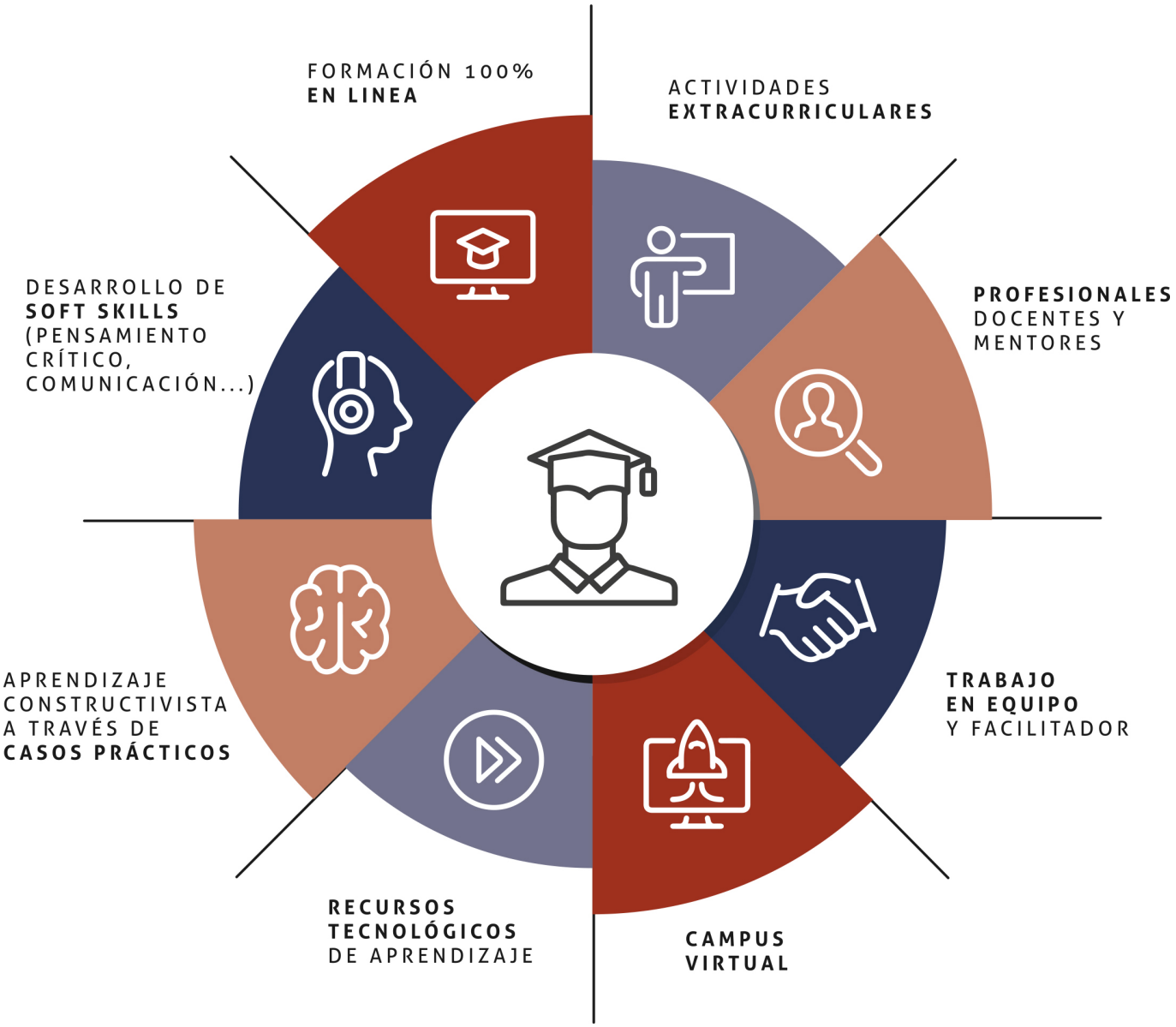
Structuralia Engineering eLearning

UDAVINCI

Ver en la web

# MODELO EDUCATIVO

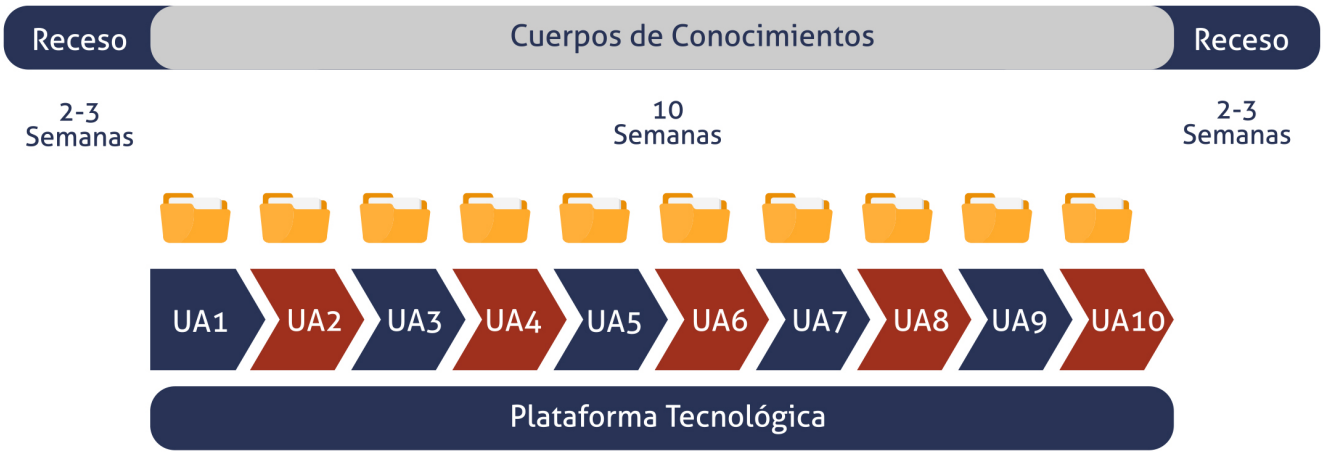
En UDAVINCI, adoptamos un enfoque constructivista que transforma al profesor en un facilitador del aprendizaje. De esta manera, los estudiantes desempeñan un papel activo en su proceso formativo, y es responsabilidad de nuestros docentes desarrollar estrategias didácticas que promuevan la autonomia e independencia del estudiante, involucrándolo plenamente en su desarollo académico.




Ver en la web

UDAVINCI

# ESTRUCTURA DE UNA ASIGNATURA




Cada asignatura tiene una duración de diez semanas, durante las cuales el estudiante accede a materiales organizados en Unidades de Aprendizaje consistentes y secuenciales. Esta estructura proporciona una distribución lógica de contenidos, lecturas, actividades, problemas, simulaciones y ejercicios, lo que ayuda al estudiante a gestionar su tiempo de manera eficiente.

Ver en la web

UDAVINCI

## RAZONES POR LAS QUE ELEGIR UDAVINCI

**1.** Primera universidad de **México 100%** online reconocida por la Secretaría de Educación Pública (SEP).

**2.** **Más de 19 años de experiencia y más de 6.000 estudiantes** de los cinco continentes.

**3.** **Excelencia académica**: Validez Oficial de Estudios (RVOE-SEP).

**4.** **Calidad Europea**: Modelo pedagógico europeo.

**5.** **Modelo constructivista**: Formación práctica y aplicada al entorno laboral.

Ver en la web

UDAVINCI

6. **Campus virtual** con la última tecnología en e-learning.

7. Elige entre nuestro amplio catálogo educativo de más de **500 programas.**

8. Alianzas y convenios con **instituciones de prestigio.**

9. **Profesorado especializado** que facilita el aprendizaje del alumnado.

10. **Recursos interactivos para un aprendizaje efectivo.**

Ver en la web

UDAVINCI

## BECAS Y FINANCIAMIENTO

Disfruta de las becas disponibles y financia tu programa universitario en mensualidades. ¡Contacta con nuestro equipo experto para saber cuál se adapta más a tu perfil!

**20%** Beca **DEPORTISTA**

**40%** Beca **EXCELENCIA**

**20%** Beca **CAPACIDADES ESPECIALES**

**40%** Beca **HERMANOS/AMIGOS**

**30%** Beca **EMPRENDEDORES**

**40%** Beca **MAYOR DE +40 AÑOS**

**30%** Beca **DOCENTES**

**50%** Beca **EXA UDA**

**Solo se puede aplicar un tipo de beca.** Es necesario presentar los documentos que acrediten que son candidatos a cada tipo de beca. Las becas mencionadas estarán disponibles exclusivamente para las solicitudes realizadas desde el sitio web de **UDAVINCI**.

### ¿Existe posibilidad de fraccionar los pagos?

Sí, se puede diferir a pagos mensuales durante los estudios:

- **Doctorado** = 36 mensualidades.
- **Licenciatura** = 36 mensualidades.
- **Especialidad** = 15 mensualidades.
- **Maestría y Maestrías con Especialización** = 18 mensualidades.
- **Cursos, Diplomas y Especializaciones** = 3 mensualidades.

Solicitar información

# FORMAS DE PAGO

Con la Garantía de:

educapay

Puede realizar el pago a través de las siguientes vías
y fraccionar en diferentes cuotas sin intereses:

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...

7 ELEVEN · llegas, pagas y Yastás · CHEDRAUI · telecomm TELECOMUNICACIONES DE MÉXICO · DELSOL

CONFIANZA ONLINE · TRUSTED SHOPS GUARANTEE

Ver en la web

UDAVINCI

# Maestría en Seguridad Informática. Especialización en Ethical Hacking

**DURACIÓN**
1500 horas

**MODALIDAD**
**ONLINE**

**ACOMPAÑAMIENTO**
**PERSONALIZADO**

## Titulación

Doble Titulación: - Titulación de Master Europeo en Seguridad Informática. Especialización en Ethical Hacking con 1500 horas expedida por EUROINNOVA INTERNATIONAL ONLINE EDUCATION, miembro de la AEEN (Asociación Española de Escuelas de Negocios) y CLADEA (Consejo Latinoamericano de Escuelas de Administración) - Titulación Oficial de Maestría en Seguridad Informática por la Universidad DAVINCI con el Reconocimiento de Validez Oficial de Estudios (RVOE). Este plan de estudios se encuentra incorporado al Sistema Educativo Nacional (SEP) con número de acuerdo 2005202.

## Descripción

La importancia de la protección y recogida de datos en las empresas ha aumentado durante la última década convirtiéndose en una profesión esencial en la vida de las organizaciones. La Maestría en Seguridad Informática con Especialización en Ethical Hacking te enseñará las distintas técnicas para mantener la seguridad en los SGSI y a desarrollar los modelos de ciberseguridad aplicados al Cloud Computing. Profundizarás en el Black SEO y su aplicación a la ética hacker. En resumen, hackear sistemas analizando, detectando y explotando sus posibles vulnerabilidades. Desde la práctica, hackearemos varios dispositivos y sistemas para conocer sus debilidades, explotarlas y, posteriormente, poder ejercer buenas prácticas en seguridad.

## Objetivos

- Profundizar y conocer en la legislación vigente en materia de seguridad informática

Ver en la web

UDAVINCI

- Mantener la seguridad en los SGSI y sus requisitos legales aplicando las técnicas aprendidas
- Aprender las técnicas y herramientas del hacker ético.
- Conocer el concepto de Black SEO o CLoaking y su aplicación en la ética hacker
- Desarrollar modelos de ciberseguridad aplicados al Cloud Computing

## Campo Laboral

La Maestría en Seguridad Informática con Especialización en Ethical Hacking está dirigida a cualquier profesional que quiera especializarse y convertirse en un experto en la gestión tecnológica de la seguridad informática, y, de una manera más concreta, en Hacker ético, conociendo de forma más profunda las técnicas del hacker ético en un sector de alta demanda.

## Perfil de Egreso

Mediante la realización de esta Maestría en Seguridad Informática con Especialización en Ethical Hacking podrás abordar análisis y gestiones de riesgos de cualquier SGSI de manera efectiva, pudiendo establecer una adecuada política de seguridad frente a agentes maliciosos. Gestionarás las distintas fases del Hacking ético en diferentes ataques y descubrirás los principales aspectos del Black SEO o Cloaking así como la seguridad aplicable al Cloud Computing.

## Salidas laborales

Una vez realizada la Maestría en Seguridad Informática con Especialización en Ethical Hacking podrás desarrollarte profesionalmente en el sector de la ciberseguridad y el hacking ético, optando a trabajos tan demandados por las empresas como Auditor de sistemas SGSI, Especialista en Hacking ético, Pentester, Desarrollador de Sistemas de Ciberseguridad o Técnico de hacking ético.

# TEMARIO

MÓDULO 1. DATOS MASIVOS EN LAS ORGANIZACIONES

UNIDAD DIDÁCTICA 1. FUNDAMENTOS DE LOS DATOS MASIVOS

1. Evolución de la administración de los datos
2. Tipos de administración de los datos
3. Operaciones para el manejo de los datos masivos
4. Tipos de datos masivos

UNIDAD DIDÁCTICA 2. COMPUTACIÓN DISTRIBUIDA

1. Historia de la computación distribuida
2. Elementos de la computación distribuida
3. Uso de la computación distribuida

UNIDAD DIDÁCTICA 3. COMPONENTES TECNOLÓGICOS PARA EL USO DE DATOS MASIVOS

1. Pila de datos masivos
2. Capas para el manejo de los datos masivos
3. Tecnología para el uso de datos masivos

UNIDAD DIDÁCTICA 4. SERVICIOS Y ALMACENAMIENTO DE DATOS

1. Servicios de organización de datos
2. Herramientas para la organización de datos
3. Almacenamiento analítico de datos

UNIDAD DIDÁCTICA 5. FUNDAMENTOS DE LA VIRTUALIZACIÓN

1. Importancia de la virtualización en el uso de datos masivos
2. Servidor de virtualización
3. Aplicaciones de la virtualización
4. Manejo de la virtualización

UNIDAD DIDÁCTICA 6. USO DE LOS DATOS MASIVOS

1. Aplicación de los datos masivos
2. Manejo de datos masivos
3. Funciones en el uso de datos masivos

UNIDAD DIDÁCTICA 7. USO DE LA NUBE

1. Relación de la nube con los datos masivos
2. Modelos de despliegue y entrega en la nube

3. Manejo de la nube para la administración de datos masivos

UNIDAD DIDÁCTICA 8. SISTEMAS DE ALMACENAMIENTO MASIVO

1. Características de los sistemas de almacenamiento masivo
2. Elementos de los sistemas de almacenamiento masivo
3. Beneficios de los sistemas de almacenamiento masivo

UNIDAD DIDÁCTICA 9. MANEJO DE LOS SISTEMAS DE ALMACENAMIENTO MASIVO

1. Sistemas de archivos distribuidos
2. Uso de las funciones de reducción
3. Manejo de las funciones de mapeo

UNIDAD DIDÁCTICA 10. ADMINISTRACIÓN DE LOS SISTEMAS PARA EL ALMACENAMIENTO MASIVO

1. Manejo de recursos y aplicaciones
2. Almacenamiento de los datos masivos
3. Minería de datos masivos

MÓDULO 2. FUNDAMENTOS DE REDES

UNIDAD DIDÁCTICA 1. EXPLORANDO LA RED

1. Conectado globalmente
2. LANs, WANs e Internet
3. La red como plataforma
4. El entorno cambiante de la red

UNIDAD DIDÁCTICA 2. CONFIGURAR UN SISTEMA OPERATIVO DE RED

1. IOS Bootcamp
2. Configuración básica de dispositivos
3. Esquemas direccionales

UNIDAD DIDÁCTICA 3. PROTOCOLOS DE RED Y COMUNICACIONES

1. Normas de comunicación
2. Protocolos y estándares de la red
3. Transferencia de datos en la red

UNIDAD DIDÁCTICA 4. ACCESO A LA RED

1. Protocolos de capa física
2. Medios de la red
3. Protocolos de capa de enlace de datos
4. Control de acceso a medios

UNIDAD DIDÁCTICA 5. ETHERNET

1. Protocolo Ethernet
2. Switches LAN
3. Protocolo de resolución de direcciones

UNIDAD DIDÁCTICA 6. CAPA DE RED

1. Protocolos de capa de red
2. Enrutamiento
3. Routers
4. Configurar un router Cisco

UNIDAD DIDÁCTICA 7. DIRECCIONAMIENTO IP

1. Direcciones de red IPv4
2. Direcciones de red IPv6
3. Verificación de conectividad

UNIDAD DIDÁCTICA 8. REDES DE SUBNETEO IP

1. Subredes de una red IPv4
2. Esquemas de direccionamiento
3. Consideraciones de diseño para IPv6

UNIDAD DIDÁCTICA 9. CAPA DE TRANSPORTE Y APLICACIÓN

1. Protocolos de capa de transporte
2. TCP y UDP
3. Protocolos de capa de aplicación
4. Protocolos y servicios de capa de aplicación bien conocidos

UNIDAD DIDÁCTICA 10. CONSTRUIR UNA RED PEQUEÑA

1. Diseño de red
2. Seguridad de la red
3. Rendimiento básico de la red
4. Solución de problemas de red

MÓDULO 3. GESTIÓN DE LA SEGURIDAD Y DELITOS INFORMÁTICOS

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL DERECHO

1. Conceptos y propósitos del derecho
2. Normas jurídicas, morales y sociales
3. Fuentes y clasificación del derecho

UNIDAD DIDÁCTICA 2. LA SOCIEDAD DE LA INFORMACIÓN

1. Derecho informático
2. Orígenes, concepto y clasificación del derecho informático
3. Informática jurídica

UNIDAD DIDÁCTICA 3. DERECHO DE LA INFORMACIÓN

1. El derecho de la información
2. Los problemas de su sistematización
3. Las telecomunicaciones

UNIDAD DIDÁCTICA 4. DERECHO A LOS DATOS PERSONALES

1. El régimen jurídico de la información en México
2. Libertad de expresión
3. Derecho de petición

UNIDAD DIDÁCTICA 5. EL DERECHO DE LA PROPIEDAD INTELECTUAL

1. Protección jurídica de los programas de computo
2. Implicaciones
3. Criptografía

UNIDAD DIDÁCTICA 6. PROPIEDAD INTELECTUAL Y DERECHOS DE AUTOR

1. Mascas, patentes y modelos de utilidad
2. Copyriht y Copyleft

UNIDAD DIDÁCTICA 7. CONTRATOS INFORMÁTICOS

1. Partes de los contratos informáticos
2. Fraudes en la comercialización de tecnologías de información y comunicación

UNIDAD DIDÁCTICA 8. DELITOS INFORMÁTICOS

1. Conceptos y características
2. Clasificación de delitos informáticos

UNIDAD DIDÁCTICA 9. NORMATIVIDAD

1. Normatividad nacional
2. Normatividad internacional

UNIDAD DIDÁCTICA 10. SITUACIÓN INTERNACIONAL DE LOS DELITOS INFORMÁTICOS

1. Países de primer mundo
2. Países en desarrollo
3. Otros países

MÓDULO 4. FUNDAMENTOS DE RUTEO Y SWITCHEO

UNIDAD DIDÁCTICA 1. CONCEPTOS DE ROUTING

1. Configuración inicial del router
2. Decisiones de routing
3. Funcionamiento del router

UNIDAD DIDÁCTICA 2. ROUTING ESTÁTICO

1. Implementación de rutas estáticas
2. Configuración de rutas estáticas y predeterminadas
3. Resolución de problemas de rutas estáticas y predeterminadas

UNIDAD DIDÁCTICA 3. ROUTING DINÁMICO

1. Protocolos de routing dinámico
2. RIPv2
3. La tabla de routing

UNIDAD DIDÁCTICA 4. REDES CONMUTADAS

1. Redes conmutadas
2. Diseño de la LAN
3. El entorno conmutado

UNIDAD DIDÁCTICA 5. CONFIGURACIÓN DEL SWITCH

1. Configuración de parámetros iniciales de un switch
2. Configuración de puertos de un switch
3. Acceso remoto seguro
4. Seguridad de puertos de switch

UNIDAD DIDÁCTICA 6. VLAN

1. Segmentación de VLAN
2. Implementaciones de VLAN
3. Routing entre VLAN con routers

UNIDAD DIDÁCTICA 7. LISTAS DE CONTROL DE ACCESO

1. Funcionamiento de las ACL
2. ACL de IPv4 estándar
3. Solución de problemas de ACL
4. Solución de problemas de red

UNIDAD DIDÁCTICA 8. DHCP

1. Funcionamiento de DHCPv4
2. Configuración de un servidor de DHCPv4 básico

3. Configuración de cliente DHCPv4
4. Resolución de problemas de DHCPv4
5. SLAAC y DHCPv6
6. DHCPv6 sin estado
7. Servidor de DHCPv6 con estado
8. Resolución de problemas de DHCPv6

UNIDAD DIDÁCTICA 9. NAT PARA IPV4

1. Funcionamiento de NAT
2. Configurar NAT
3. Resolver problemas de NAT

UNIDAD DIDÁCTICA 10. DETECCIÓN, ADMINISTRACIÓN Y MANTENIMIENTO DE DISPOSITIVOS

1. Detección de dispositivos
2. Administración de dispositivos
3. Mantenimiento de dispositivos
4. Solución de problemas de red

MÓDULO 5. SEGURIDAD EN LA NUBE Y REDES SOCIALES

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LAS REDES SOCIALES

1. Historia de las redes sociales
2. Tipos de Redes sociales
3. Ética y las redes sociales

UNIDAD DIDÁCTICA 2. FACEBOOK

1. Facebook como herramienta personal
2. Facebook como herramienta empresarial
3. Herramientas y seguridad en las páginas de Facebook

UNIDAD DIDÁCTICA 3. TWITTER

1. Filosofías de uso
2. Twitter como herramienta empresarial
3. Herramientas y seguridad en Twitter

UNIDAD DIDÁCTICA 4. LINKEDIN

1. Diferencia entre Linkedin con otras redes sociales
2. Herramientas en Linkedin
3. Seguridad en Linkedin

UNIDAD DIDÁCTICA 5. BLOG

1. Diferencias entre blogs personales y profesionales
2. Proveedores de blogspot
3. Casos de éxito

UNIDAD DIDÁCTICA 6. OTRAS REDES SOCIALES

1. Instagram
2. Slideshare
3. Google+

UNIDAD DIDÁCTICA 7. LA NUBE

1. Beneficios y riesgos
2. Roles existentes
3. Modelos de implementación

UNIDAD DIDÁCTICA 8. ARQUITECTURA DE LA NUBE

1. Herramientas de gestión
2. Administración de la nube
3. Implementación de nubes privadas

UNIDAD DIDÁCTICA 9. SEGURIDAD EN LA NUBE

1. Conflictos con la privacidad
2. Modelos de servicios

UNIDAD DIDÁCTICA 10. DESARROLLO DE APLICACIONES EN LA NUBE

1. Desarrollo de software en la Nube vs Desarrollo tradicional
2. Consideraciones para el análisis, diseño y desarrollo en la Nube
3. Herramientas de desarrollo

MÓDULO 6. ESCALAMIENTO DE REDES

UNIDAD DIDÁCTICA 1. DISEÑO DE LAN

1. Diseños validados Cisco
2. Expansión de la red
3. Hardware del switch
4. Hardware de routers
5. Administración de dispositivos

UNIDAD DIDÁCTICA 2. ESCALAMIENTO DE VLAN

1. VTP, VLAN extendidas y DTP
2. Solución de problemas de VLAN múltiple
3. Conmutación de Capa 3

UNIDAD DIDÁCTICA 3. STP

1. Conceptos de árbol de expansión
2. Variedades de protocolos de árbol de expansión
3. Configuración de árbol de expansión

UNIDAD DIDÁCTICA 4. ETHERCHANNEL Y HSRP

1. Conceptos de agregación de enlaces
2. Configuración de la agregación de enlaces
3. Protocolos de redundancia de primer salto

UNIDAD DIDÁCTICA 5. ROUTING DINÁMICO

1. Protocolos de routing dinámico
2. Routing dinámico vector distancia
3. Routing dinámico de estado de enlace

UNIDAD DIDÁCTICA 6. EIGRP

1. Características del protocolo EIGRP
2. Implementar el protocolo EIGRP para IPv4
3. Funcionamiento del protocolo EIGRP
4. Implementar el protocolo EIGRP para IPv6

UNIDAD DIDÁCTICA 7. AJUSTES Y SOLUCIÓN DE PROBLEMAS DEL PROTOCOLO EIGRP

1. Ajustes del protocolo EIGRP
2. Componentes de la solución de problemas de EIGRP
3. Solucionar problemas de vecinos EIGRP
4. Solucionar problemas de la tabla de routing de EIGRP

UNIDAD DIDÁCTICA 8. OSPF DE ÁREA ÚNICA

1. Características del protocolo OSPF
2. Protocolo OSPFv2 de área única
3. OSPFv3 de área única

UNIDAD DIDÁCTICA 9. OSPF MULTIÁREA

1. ¿Por qué OSPF multiárea?
2. Tipos de LSA de OSPF
3. Tabla de routing y tipos de rutas de OSPF
4. Configuración de OSPF multiárea

UNIDAD DIDÁCTICA 10. AJUSTES Y SOLUCIÓN DE PROBLEMAS DEL PROTOCOLO OSPF

1. Configuraciones avanzadas de OSPF de área única

2. Ajuste de las interfaces OSPF
3. Resolución de problemas de implementaciones de OSPF de área única

MÓDULO 7. AMENAZAS Y VULNERABILIDADES

UNIDAD DIDÁCTICA 1. CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

1. Concepto de Amenaza
2. Concepto de vulnerabilidad
3. Concepto de riesgo

UNIDAD DIDÁCTICA 2. INTRODUCCIÓN AL ANÁLISIS DE VULNERABILIDADES

1. Vulnerabilidades Físicas
2. Vulnerabilidades lógicas
3. Escáneres de vulnerabilidades

UNIDAD DIDÁCTICA 3. CARACTERÍSTICAS DE LAS VULNERABILIDADES

1. Tipos de vulnerabilidades
2. Detección de vulnerabilidades
3. Métodos de escaneo de vulnerabilidades

UNIDAD DIDÁCTICA 4. REMEDIACIÓN DE VULNERABILIDADES

1. Análisis y clasificación de activos
2. Identificación de vulnerabilidades
3. Clasificación y priorización de riesgos
4. Propuesta para mitigar riesgo

UNIDAD DIDÁCTICA 5. METODOLOGÍAS, MÉTODOS Y TÉCNICAS PARA EL ANÁLISIS DE VULNERABILIDADES

1. Establecimiento de reglas, políticas y procedimientos
2. Recolección de información
3. Análisis interior y exterior

UNIDAD DIDÁCTICA 6. HERRAMIENTAS PARA EL ANÁLISIS DE VULNERABILIDADES

1. Escáner de vulnerabilidades en puertos
2. Escáner de vulnerabilidades en páginas web
3. Escáner de vulnerabilidades en sistemas operativos
4. Escáner de seguridad de red y administración de parches

UNIDAD DIDÁCTICA 7. MECANISMOS DE SEGURIDAD INFORMÁTICA

1. Preventivos
2. Correctivos

3. Detectivos

UNIDAD DIDÁCTICA 8. HACKERS

1. Definición
2. Tipos de Hackers
3. Script kiddie

UNIDAD DIDÁCTICA 9. TIPOS DE AMENAZAS

1. Exploits
2. Malware
3. Ingeniería social
4. Ataque DDoS
5. Phishing
6. Otros tipos de amenazas

UNIDAD DIDÁCTICA 10. ATAQUES DIRIGIDOS EN LA HISTORIA

1. Stuxnet
2. Sony Picture
3. Zeus
4. Otros ataques

MÓDULO 8. SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. FUNDAMENTOS DE LA SEGURIDAD EN REDES

1. Introducción a la seguridad en redes
2. Vulnerabilidades de las redes
3. Metodología de un ataque

UNIDAD DIDÁCTICA 2. SEGURIDAD EN ROUTERS

1. Construyendo la seguridad en un router
2. Configuración de contraseñas
3. Configuración de Roles
4. Protección de archivos del router y sus contraseñas

UNIDAD DIDÁCTICA 3. ADMINISTRACIÓN DE LA SEGURIDAD EN LA RED

1. Reportes y administración
2. Auditoria de seguridad

UNIDAD DIDÁCTICA 4. AAA (AUTHENTICATION, AUTHORIZATION, ACCOUNTING)

1. Introducción a AAA
2. Configuración local de AAA

3. Autenticación de AAA basada en servidores
4. Configuración de autenticación basada en servidor TACACS y RADIUS
5. Resolución de fallos de AAA

UNIDAD DIDÁCTICA 5. SEGURIDAD EN CAPA 2

1. Seguridad de la LAN
2. Ataques de CAPA 2
3. Seguridad en Puertos de CAPA 2
4. Control de tormentas
5. Protección de la topología STP
6. Seguridad en VLAN

UNIDAD DIDÁCTICA 6. LISTAS DE CONTROL DE ACCESO

1. Introducción a las ACLs
2. Ubicación de las ACLs
3. Recomendaciones en el diseño de las ACLs

UNIDAD DIDÁCTICA 7. CONFIGURACIÓN DE LAS ACLS

1. Configuración de las ACLs Numeradas
2. Configuración de las ACLs Nombradas
3. Otros tipos de ACLs

UNIDAD DIDÁCTICA 8. FIREWALLS

1. Características de los Firewalls
2. Control de acceso basado en el contexto
3. Firewall basado en zonas
4. Cisco ASA
5. Configuración avanzada del Firewall Cisco ASA

UNIDAD DIDÁCTICA 9. IPS (INTRUSION PREVENTION SYSTEM)

1. Características de los IDS e IPS
2. Firmas IPS
3. Configuración de Cisco IOS IPS

UNIDAD DIDÁCTICA 10. TECNOLOGÍAS VPN

1. Introducción a las VPN
2. Túneles GRE
3. Protocolos de IPSEC
4. Internet Key Exchange
5. Algoritmos de encriptación
6. Configuración de VPN SITE to SITE
7. Configuración de IPSEC con CCP

8. VPN de acceso remoto

MÓDULO 9. ADMINISTRACIÓN DE RIESGOS

UNIDAD DIDÁCTICA 1. FILOSOFÍAS DE ANÁLISIS DE RIESGOS EN TECNOLOGÍAS DE LA INFORMACIÓN

1. Disponibilidad
2. Integridad
3. Confidencialidad

UNIDAD DIDÁCTICA 2. ACTIVOS DE INFORMACIÓN

1. Identificación de activos de información de la empresa
2. Clasificación de activos de información de la empresa
3. Identificación de responsables del activo de información

UNIDAD DIDÁCTICA 3. FLUJOS DE INFORMACIÓN

1. Identificación de los flujos información de la empresa
2. Clasificación de flujos de información de la empresa
3. Identificación de responsables del flujo de información

UNIDAD DIDÁCTICA 4. VULNERABILIDADES

1. Identificación de vulnerabilidades por cada activo de información
2. Clasificación de vulnerabilidades
3. Evaluación del grado de vulnerabilidad

UNIDAD DIDÁCTICA 5. AMENAZAS

1. Identificación de posibles amenazas por cada vulnerabilidad
2. Clasificación de la amenaza
3. Evaluación de posibles responsables

UNIDAD DIDÁCTICA 6. IMPACTOS

1. Identificación del impacto por cada amenaza materializada
2. Clasificación del impacto
3. Evaluación del grado de impacto

UNIDAD DIDÁCTICA 7. ANÁLISIS DE RIESGOS

1. Determinar el grado de la probabilidad de ocurrencia
2. Determinación del riesgo
3. Elección de acciones a tomar por parte de los dueños

UNIDAD DIDÁCTICA 8. CONTROLES

1. Identificar los controles por cada amenaza

2. Determinar el tipo de control

UNIDAD DIDÁCTICA 9. SIMULACIÓN DE PROSPECTIVA

1. Revisión de los nuevos impactos
2. Revisión de la nueva probabilidad de ocurrencia
3. Determinación del nuevo Riesgo

UNIDAD DIDÁCTICA 10. ANÁLISIS COSTO-BENEFICIO

1. Generación de presupuesto
2. Revisión de los beneficios & la inversión

MÓDULO 10. CRIPTOGRAFÍA Y MECANISMOS DE SEGURIDAD

UNIDAD DIDÁCTICA 1. ATACANTES Y DEFENSORES

1. El peligro
2. Combatiendo la Ciberdelincuencia

UNIDAD DIDÁCTICA 2. SISTEMAS OPERATIVOS

1. Sistema Operativo Windows
2. Descripción de Linux

UNIDAD DIDÁCTICA 3. FUNDAMENTOS DE REDES

1. Protocolos de Red
2. Protocolo IP y Ethernet
3. Protocolo ICMP
4. Protocolo ARP
5. Capa de Transporte
6. Servicios de Red

UNIDAD DIDÁCTICA 4. INFRAESTRUCTURA DE RED

1. Dispositivos de Comunicación por Redes
2. Infraestructura de Seguridad de Redes

UNIDAD DIDÁCTICA 5. AMENAZAS Y ATAQUES

1. Los Atacantes y sus Herramientas
2. Amenazas y Ataques Comunes
3. Monitoreo de Red y Herramientas
4. PDUs y sus Vulnerabilidades
5. Ataques a los Servicios de Red

UNIDAD DIDÁCTICA 6. DEFENSA DE LA RED

1. ¿Qué es la defensa?
2. Control de acceso AAA
3. Inteligencia contra amenazas

UNIDAD DIDÁCTICA 7. CRIPTOGRAFÍA Y PROTECCIÓN DE TERMINALES

1. Criptografía
2. Protección de terminales (Hosts)
3. Vulnerabilidades de terminales (Hosts)

UNIDAD DIDÁCTICA 8. PROTOCOLOS Y REGISTROS

1. Protocolos de red para monitoreo
2. Datos de seguridad de la red

UNIDAD DIDÁCTICA 9. ANÁLISIS DE DATOS DE SEGURIDAD

1. Evaluación de alertas
2. Datos de seguridad de la red
3. Análisis y respuestas a incidentes e información forense digital

UNIDAD DIDÁCTICA 10. EVALUACIONES FINALES

1. Teórico y práctico

MÓDULO 11. IMPACTOS, CONTROLES Y ANÁLISIS DE RIESGOS

UNIDAD DIDÁCTICA 1. IMPACTOS EN EL NEGOCIO

1. Concepto de impacto
2. Tipos de impacto
3. Impactos en las organizaciones

UNIDAD DIDÁCTICA 2. TIPOS DE IMPACTOS

1. Financieros
2. Legales
3. Imagen
4. Productivos
5. Salud

UNIDAD DIDÁCTICA 3. ANÁLISIS DE IMPACTO DE NEGOCIO

1. Identificación de procesos de negocio soportados por sistemas de información
2. Valoración de requerimientos de confidencialidad, integridad y disponibilidad
3. Requerimientos de seguridad

UNIDAD DIDÁCTICA 4. IMPACTOS EN LA HISTORIA

1. PlayStation
2. Stuxnet
3. eBay
4. Otros impactos

UNIDAD DIDÁCTICA 5. CONCEPTOS BÁSICOS DE CONTROLES

1. Definición
2. Tipos de controles (lógicos, físicos y humanos)
3. Identificación de controles

UNIDAD DIDÁCTICA 6. DISEÑO Y DEFINICIÓN DE LOS OBJETIVOS DE CONTROL

1. Contexto de riesgos
2. Estándares y buenas prácticas
3. Objetivos de Control

UNIDAD DIDÁCTICA 7. AUDITORÍA Y ENTORNO DE CONTROLES

1. Entendimiento de TI
2. Mapa de sistemas TI
3. Evaluación Implementación y efectividad de Controles de TI

UNIDAD DIDÁCTICA 8. MECANISMOS DE SEGURIDAD INFORMÁTICA

1. Controles preventivos
2. Controles Correctivos
3. Controles Detectivos

UNIDAD DIDÁCTICA 9. RIESGOS

1. Conceptos generales
2. Riesgos de TI
3. Análisis y gestión de riesgos

UNIDAD DIDÁCTICA 10. ESTÁNDARES DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA

1. La organización ISO y la familia de normas ISO
2. Normas ISO/IEC 27000
3. Otros estándares de gestión (ITIL, COBIT)

MÓDULO 12. METODOLOGÍA DE LA INVESTIGACIÓN

UNIDAD DIDÁCTICA 1. ENFOQUE CUANTITATIVO Y CUALITATIVO

1. Elementos de la investigación
2. Características del enfoque cuantitativo
3. Características del enfoque cualitativo

4. Diferencias entre los enfoques de investigación
5. Ventajas de los enfoques de investigación

UNIDAD DIDÁCTICA 2. PROYECTO DE INVESTIGACIÓN

1. Tipos de proyectos de investigación
2. Proyecto de investigación cuantitativa
3. Proyecto de investigación cualitativa
4. Fuentes de ideas para la investigación
5. Antecedentes de la investigación

UNIDAD DIDÁCTICA 3. PLANTEAMIENTO DEL PROBLEMA CUANTITATIVO

1. Planteamiento del problema de investigación
2. Enfoque cuantitativo
3. Criterios para plantear el problema
4. Elementos para el planteamiento del problema de investigación
5. Objetivos, preguntas y justificación de la investigación

UNIDAD DIDÁCTICA 4. REVISIÓN DE LA LITERATURA Y CONSTRUCCIÓN DEL MARCO TEÓRICO

1. Desarrollo de la perspectiva teórica
2. Etapas para el desarrollo de la perspectiva teórica
3. Elementos para la revisión de la literatura
4. Elementos del marco teórico
5. Construcción del marco teórico

UNIDAD DIDÁCTICA 5. ALCANCE DE LA INVESTIGACIÓN

1. Estudio exploratorio
2. Estudio descriptivo
3. Estudio correlacional
4. Estudio explicativo
5. Selección del tipo de estudio

UNIDAD DIDÁCTICA 6. FORMULACIÓN DE HIPÓTESIS

1. Elementos de las hipótesis
2. Características de las variables
3. Tipos de hipótesis
4. Hipótesis nulas
5. Hipótesis alternativas

UNIDAD DIDÁCTICA 7. DISEÑOS DE INVESTIGACIÓN

1. Características del diseño en la investigación
2. Diseño experimentales
3. Experimentos puros

4. Diseños no experimentales
5. Diseños transeccionales descriptivos

UNIDAD DIDÁCTICA 8. SELECCIÓN DE LA MUESTRA

1. Delimitación de la población
2. Selección de muestra
3. Tipos de muestra
4. Muestra probabilística
5. Muestra no probabilística

UNIDAD DIDÁCTICA 9. RECOLECCIÓN Y ANÁLISIS DE LOS DATOS CUANTITATIVOS

1. Características para la recolección de datos
2. Instrumento de medición
3. Análisis de los datos cuantitativos
4. Proceso para el análisis de los datos cuantitativos
5. Pruebas de hipótesis

UNIDAD DIDÁCTICA 10. REPORTE DE RESULTADOS DEL PROCESO CUANTITATIVO

1. Características del reporte
2. Elementos del reporte
3. Recursos para la elaboración del reporte
4. Criterios para la elaboración del reporte
5. Protocolo de investigación

MÓDULO 13. NORMAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA LAS EMPRESAS

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LAS NORMAS Y LOS ESTÁNDARES

1. Definiciones
2. Entidades desarrolladoras
3. Las normas y estándares en las empresas

UNIDAD DIDÁCTICA 2. NORMAS ISO

1. Definición de normas ISO
2. Tipos de normas
3. ISO/IEC 27000

UNIDAD DIDÁCTICA 3. ISO/IEC 27001 E ISO/IEC 27002

1. Interesados
2. Puntos clave
3. Requisitos, prerrequisitos y métodos de obtención

UNIDAD DIDÁCTICA 4. ISO/IEC 27003 E ISO/IEC 27004

1. Interesados
2. Puntos clave
3. Requisitos, prerrequisitos y métodos de obtención

UNIDAD DIDÁCTICA 5. ISO/IEC 27005 E ISO/IEC 27006

1. Interesados
2. Puntos clave
3. Requisitos, prerrequisitos y métodos de obtención

UNIDAD DIDÁCTICA 6. ISO/IEC 27007

1. Interesados
2. Puntos clave
3. Requisitos, prerrequisitos y métodos de obtención

UNIDAD DIDÁCTICA 7. EL RFC 2196

1. Interesados
2. Puntos clave
3. Requisitos, prerrequisitos y métodos de obtención

UNIDAD DIDÁCTICA 8. ESTÁNDAR ISA/IEC 62443

1. Interesados
2. Puntos clave
3. Requisitos, prerrequisitos y métodos de obtención

UNIDAD DIDÁCTICA 9. NIST SP 800-30

1. Interesados
2. Puntos clave
3. Requisitos, prerrequisitos y métodos de obtención

UNIDAD DIDÁCTICA 10. BS 25999

1. Interesados
2. Puntos clave
3. Requisitos, prerrequisitos y métodos de obtención

MÓDULO 14. PROYECTO INTEGRADOR DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. IDENTIFICACIÓN DE ACTIVOS

1. Lógicos
2. Físicos
3. Flujos de información
4. Otros tipos de activos

UNIDAD DIDÁCTICA 2. IDENTIFICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

1. Políticas
2. Procedimientos
3. Formatos, bitácoras y oficios

UNIDAD DIDÁCTICA 3. IDENTIFICACIÓN DE VULNERABILIDADES

1. Detección de vulnerabilidad
2. Tipo de vulnerabilidad
3. Grado de vulnerabilidad

UNIDAD DIDÁCTICA 4. IDENTIFICACIÓN DE AMENAZAS

1. Detección de Amenazas por vulnerabilidad
2. Tipo de Amenaza
3. Grado de amenaza y probabilidad de ocurrencia

UNIDAD DIDÁCTICA 5. MECANISMOS DE SEGURIDAD

1. Preventivos
2. Correctivos
3. Detectivos

UNIDAD DIDÁCTICA 6. IDENTIFICACIÓN DE IMPACTOS

1. Tipo de impacto
2. Grado del impacto
3. Pérdidas ocasionadas por el impacto

UNIDAD DIDÁCTICA 7. MEDICIÓN DE RIESGOS

1. Matriz de riesgos
2. Nivel de impacto
3. Probabilidad de ocurrencia
4. Nivel de riesgo

UNIDAD DIDÁCTICA 8. IDENTIFICACIÓN DE CONTROLES

1. Tipos de controles (lógicos, físicos y humanos)
2. Mecanismos de controles (correctivos y detectivos)
3. Políticas y procedimientos actualizados
4. Objetivos de los Controles

UNIDAD DIDÁCTICA 9. ESTÁNDARES DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA

1. La organización ISO y la familia de normas ISO
2. Normas ISO/IEC 27000

3. Otros estándares de gestión (ITIL, COBIT)

UNIDAD DIDÁCTICA 10. ANÁLISIS DE RIESGO

1. Riesgo residual
2. Documentación e informa
3. Propuestas de mejora

MÓDULO 14. HACKING ÉTICO

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN Y CONCEPTOS PREVIOS

1. ¿Qué es el hacking ético?
2. Aspectos legales del hacking ético
3. Perfiles del hacker ético

UNIDAD DIDÁCTICA 2. FASES DEL HACKING ÉTICO EN LOS ATAQUES A SISTEMAS Y REDES

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tests de vulnerabilidades

UNIDAD DIDÁCTICA 3. FASES DEL HACKING ÉTICO EN LOS ATAQUES A REDES WIFI

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tipos de seguridad WiFi
4. Sniffing

UNIDAD DIDÁCTICA 4. FASES DEL HACKING ÉTICO EN LOS ATAQUES WEB

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tipos de seguridad web
4. Tipo de test de seguridad en entornos web

UNIDAD DIDÁCTICA 5. AUDITORÍA DE SEGURIDAD INFORMÁTICA

1. Criterios Generales
2. Aplicación de la normativa de protección de datos de carácter personal
3. Herramientas para la auditoría de sistemas
4. Descripción de los aspectos sobre cortafuego en auditorías de sistemas de información
5. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información

MÓDULO 15. HACKING TRAINING PLATFORM

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A HACKING TRAINING PLATFORMS

1. ¿Qué es el hacking ético?
2. Máquinas virtuales
3. Plataformas para practicar hacking ético

UNIDAD DIDÁCTICA 2. HACK THE BOX (HTB)

1. Introducción a Hack The Box
2. Crear una cuenta
3. Tutoriales

UNIDAD DIDÁCTICA 3. TRYHACKME

1. ¿Qué es TryHackMe?
2. Crear una cuenta
3. Interfaz de TryHackMe
4. Introducción a la ciberseguridad
5. Seguridad ofensiva
6. Ciencia forense digital

UNIDAD DIDÁCTICA 4. HACKER101

1. ¿Qué es Hacker101?
2. Hacker101 CTF
3. Tutoriales

UNIDAD DIDÁCTICA 5. VULNHUB

1. ¿Qué es Vulnhub?
2. Interfaz de Vulnhub
3. Tutoriales

UNIDAD DIDÁCTICA 6. HACK THIS SITE

1. ¿Qué es Hack This Suite?
2. Desafíos Hack This Site

UNIDAD DIDÁCTICA 7. GOOGLE XSS GAME

1. ¿Qué es Google XSS Game?
2. Niveles de Google XSS game

UNIDAD DIDÁCTICA 8. HACKTHIS

1. ¿Qué es HackThis?
2. Tutorial HackThis
3. Basic+

## ¿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)

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

UDAVINCI

UDAVINCI

By
EDUCA EDTECH
Group