EUROINNOVA
INTERNATIONAL ONLINE EDUCATION

Master en Cloud Computing y Virtualización + 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

Master en Cloud Computing y Virtualización + Titulación Universitaria

DURACIÓN
800 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

CREDITOS
8 ECTS

Titulación

Titulación Múltiple: - Titulación de Master en Cloud Computing y Virtualización con 600 horas expedida por EUROINNOVA BUSINESS SCHOOL como Escuela de Negocios Acreditada para la Impartición de Formación Superior de Postgrado y Avalada por la Escuela Superior de Cualificaciones Profesionales - Título Propio de Cloud Computing expedida por la Universidad Europea Miguel de Cervantes acreditada con 8 ECTS Universitarios (Curso Universitario de Especialización de la Universidad Europea Miguel de Cervantes)

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

Este Master en Cloud Computing y Virtualización le ofrece una formación especializada en la materia. Estamos ante un mundo globalizado en el que las fronteras prácticamente han desaparecido y las tecnologías de la información deben adaptarse a continuos cambios del mercado y del entorno en general. Estos cambios han contribuido a la proliferación del trabajo en la nube, siendo la formación en este ámbito fundamental para lograr una ventaja competitiva. Al finalizar este Master en Cloud Computing y Virtualización, los alumnos podrán liderar proyectos de implantación de sistemas en la nube, además de tomar decisiones estratégicas y de negocio para la adaptación de la nube a las necesidades del mismo.

Objetivos

- Dotar a los alumnos de una visión de cómo afrontar un proyecto de Cloud Computing.
- Conocer las características y aprender a distinguir los principales modelos de nubes: IaaS, PaaS, SaaS y XaaS, entre otros.
- Realizar un estudio pormenorizado de las nubes públicas, privadas e híbridas, conociendo cuál puede ser la mejor alternativa para la implantación en su negocio.
- Conocer con profundidad las implicaciones de seguridad y auditoría que supone trabajar con información en la nube.
- Conocer las funcionalidades de VMware vSphere 5.
- Integrar de forma adecuada vSphere 5 en el seno de los sistemas de información del Datacenter
- Conocer la experiencia detallada acerca de la implantación de un proyecto en cuatro grandes fases.
- Estudiar una metodología eficaz, que da las claves para el éxito de dicho proyecto.
- Aprender a identificar malware.

Ver en la web

- Analizar de manera básica los tipos de malware e implementar contramedidas.
- Comprender las diferentes técnicas de ofuscación.
- Aprender las técnicas y la metodología utilizadas por los profesionales del análisis de malwares.
- Dotar a los alumnos de los lineamientos básicos para la aplicación de la Norma ISO/IEC 27001 dentro de su organización.
- Ofrecer las pautas para implementar un sistema de gestión de seguridad de información basado en el estándar ISO/IEC 27001 siguiendo los controles recomendados por el estándar ISO/IEC 27002 en sus respectivas cláusulas.
- Exponer y explicar una serie de buenas prácticas para conseguir la seguridad de la información.

A quién va dirigido

Este Master en Cloud Computing y Virtualización está dirigido a quienes posean un grado o título equivalente en Administración y dirección de empresas, Empresariales, Economía, Informática, Marketing, Administración de sistemas o cualquier titulación que quiera reforzar o adquirir conocimientos en la tecnología Cloud Computing que le permita tomar decisiones en cuanto a la implantación de esta tecnología.

Para qué te prepara

Este Master en Cloud Computing y Virtualización pretende dotar al alumno de los conocimientos teóricos y prácticos necesarios para analizar detenidamente y evaluar las distintas alternativas del mercado para trabajar con datos a través de la nube. El alumno conocerá las ventajas y desventajas, además de las distintas tipologías, de cada modelo de nube y será capaz de identificar la alternativa más adecuada a sus proyecciones de trabajo en la nube.

Salidas laborales

Área administrativa y ejecutiva de cualquier tipo de empresa (tanto pyme como gran empresa), especialmente puestos directivos y estratégicos de negocio, consultores y coordinadores técnicos, consultores de aplicaciones en la nube, puestos directivos y de gestión de departamentos IT.

TEMARIO

PARTE 1. CLOUD COMPUTING

MÓDULO 1. INTRODUCCIÓN AL CLOUD COMPUTING

UNIDAD DIDÁCTICA 1. ASPECTOS INTRODUCTORIOS DE CLOUD COMPUTING

1. Orígenes del cloud computing
2. Qué es cloud computing
3. Características del cloud computing
4. La nube y los negocios
5. Modelos básicos en la nube

UNIDAD DIDÁCTICA 2. HARDWARE CLOUD

1. Virtualización
2. Categorías de virtualización
3. Cloud storage
4. Proveedores fiables de cloud storage

UNIDAD DIDÁCTICA 3. SERVICIOS CLOUD

1. Servicios cloud para el usuario
2. Escritorio virtual o VDI
3. Servicio de centro de datos remoto

MÓDULO 2. TIPOS Y MODELOS DE NUBES

UNIDAD DIDÁCTICA 4. MODELOS DE NUBES

1. Introducción
2. IaaS
3. PaaS
4. SaaS
5. Otros modelos comerciales

UNIDAD DIDÁCTICA 5. NUBES PRIVADAS

1. Qué es una nube privada
2. Ventajas e inconvenientes del servicio de la nube privada
3. La transición a la nube privada
4. Alternativas para crear una nube privada

UNIDAD DIDÁCTICA 6. NUBES PÚBLICAS

1. Qué es una nube pública
2. Ventajas e inconvenientes del servicio de nube pública

3. Análisis DAFO de la nube pública
4. Nubes públicas vs Nubes privadas

UNIDAD DIDÁCTICA 7. NUBES HÍBRIDAS Y VISIÓN ESTRATÉGICA

1. Qué es una nube híbrida
2. Ventajas e inconvenientes de las nubes híbridas
3. Aspectos clave en la implantación de una nube híbrida
4. Evaluación de alternativas para el establecimiento de una nube híbrida

MÓDULO 3. CONCEPTOS AVANZADOS DE CLOUD COMPUTING Y SEGURIDAD

UNIDAD DIDÁCTICA 8. CONCEPTOS AVANZADOS DE CLOUD COMPUTING

1. Interoperabilidad en la nube
2. Centro de procesamiento de datos y operaciones
3. Cifrado y gestión de claves
4. Gestión de identidades

UNIDAD DIDÁCTICA 9. CONCEPTOS AVANZADOS DE CLOUD COMPUTING

1. Interoperabilidad en la nube
2. Centro de procesamiento de datos y operaciones
3. Cifrado y gestión de claves
4. Gestión de identidades

PARTE 2. LINUX Y AZURE: EXPERTO EN CLOUD

UNIDAD DIDÁCTICA 1. CLOUD COMPUTING.

1. Introducción al Cloud computing
2. Modo de trabajo y funcionamiento
3. Virtualización
4. Tipos de Cloud
5. Niveles de Programación
6. Historia
7. Ventajas e inconvenientes
8. Análisis DAFO

UNIDAD DIDÁCTICA 2. AGENTES QUE INTERVIENEN EN EL CLOUD COMPUTING

1. El Cloud Computing y el departamento IT
2. Niveles del Cloud Computing
3. ¿Qué es la virtualización?
4. Centros de datos para Cloud

UNIDAD DIDÁCTICA 3. PROYECTO DE CLOUD COMPUTING

1. Ventajas y desventajas del Cloud Computing
2. Análisis DAFO de la implantación del Cloud

UNIDAD DIDÁCTICA 4. SEGURIDAD Y ASPECTOS LEGALES DEL CLOUD COMPUTING

1. (LOPD) Ley de Protección de Datos
2. Propiedad intelectual
3. Relaciones laborales
4. Los retos del Cloud Computing
5. Implementación de la seguridad en el Cloud Computing
6. Análisis forense en el Cloud Computing
7. Cloud Security Alliance (CSA)

UNIDAD DIDÁCTICA 5. TOPOLOGÍA

1. Tipos de nube
2. Tipo de cloud que debo de usar
    1. - IaaS
    2. - PaaS
    3. - SaaS
    4. - Otros modelos comerciales
3. La topología en el ámbito de los servicios cloud

UNIDAD DIDÁCTICA 6. AZURE.

1. Plataforma Windows Azure.
2. Usuario: modo de acceso y trabajo.
3. Administración de Azure.
4. Virtualización con Azure.
5. Vista programador.
6. Servicios de Azure.
7. Bases de Datos con Azure.
8. Programación en Azure.
    1. - Librerías.
    2. - Análisis.
    3. - Diseño.
    4. - Codificación.
    5. - Compilación.
    6. - Depuración.
    7. - Implementación.

UNIDAD DIDÁCTICA 7. LINUX.

1. Distribuciones Linux en la Nube.
2. Usuario: modo de acceso y trabajo
3. Administración.
4. Virtualización con Linux.
5. Vista programador.
6. Servicios en Linux.
7. Bases de Datos en Linux.
    1. - Programación en la Nube bajo Linux.
    2. - Librerías.

3. - Análisis.
4. - Diseño.
5. - Codificación.
6. - Compilación.
7. - Depuración.
8. - Implementación.

UNIDAD DIDÁCTICA 8. SERVICIOS.

1. Acceso a servicios misma plataforma.
2. Acceso a servicios diferentes plataforma.
3. Interoperabilidad.
4. Futuro de los Servicios Cloud Computing.

PARTE 3. VIRTUALIZACIÓN CON VMWARE VSPHERE

UNIDAD DIDÁCTICA 1. PRIMERO PASOS CON VMWARE VSPHERE

1. ¿Qué es Vmware vSphere?
2. Archivos que componen una Máquina Virtual
3. Interconexión del servidor y las máquinas
    1. - Aspectos más relevantes del Networing en Hyper-V..
    2. - vSphere Distributed Switch (VDS)
4. Almacenamiento
    1. - Vmware ESX para crear un datastore NFS o ISCSI.
5. VMware Capacity Planner
    1. - Ventajas de vCenter Converter
    2. - Redimensionamiento de máquinas virtuales
    3. - Sistemas HOST vmware ESX y ESXi
    4. - Acceso a los servidores HOST (Esx e Hyper-V)
    5. - Elementos de la interface

UNIDAD DIDÁCTICA 2. NETWORKING: VMWARE VSPHERE

1. Funcionamiento de los adaptadores virtuales de Ethernet
2. Configuración de VLANs en un entorno virtual con vSphere
3. Compartir la carga de tráfico entre las redes física y virtual “NIC Teaming”
4. ESX Server para Networking: Componentes

UNIDAD DIDÁCTICA 3. VMWARE VSPHERE. EL ENTORNO DE CLUSTER EN VSPHERE

1. Uso de Vmware Update Manager
2. Aplicar un parche a un host ESXi 5.x/6.x desde la línea de comandos
3. Instalación del componente VMware Update Manager en vSphere 5
4. Utilizando Host Update Utility
5. Configurar la política de rutas predeterminada para LUN

UNIDAD DIDÁCTICA 4. VSPHERE: INTRODUCCIÓN AL ENTORNO DE CLUSTER

1. Introducción al Cluster en vSphere

2. Requisitos previos para la configuración de un Cluster
3. Cluster: Descripción y propiedades
4. VMware HA
5. Opciones avanzadas

UNIDAD DIDÁCTICA 5. VMWARE VSPHERE: CAMBIAR TAMAÑO DE DISCOS Y CLONACIÓN

1. Rendimensionamiento de discos.
2. Clonación de un disco de una máquina virtual
3. vmkfstools: Uso de la herramienta
4. Modificación de Formato de Discos
5. Configuración de Discos RDM

PARTE 4. SEGURIDAD INFORMÁTICA. ANÁLISIS DE MALWARE

UNIDAD DIDÁCTICA 1. IDENTIFICACIÓN DE UN MALWARE

1. Presentación de los malwares por familias
    1. - Introducción
    2. - Backdoor
    3. - Ransomware y locker
    4. - Stealer
    5. - Rootkit
2. Escenario de infección
    1. - Introducción
    2. - Escenario: la ejecución de un archivo adjunto
    3. - Escenario: el clic desafortunado
    4. - Escenario: la apertura de un documento infectado
    5. - Escenario: los ataques informáticos
    6. - Escenario: los ataques físicos: infección por llave USB
3. Técnicas de comunicación con el C&C
    1. - Introducción
    2. - Actualización de la lista de nombres de dominio
    3. - Comunicación mediante HTTP/HTTPS/FTP/IRC
    4. - Comunicación mediante e-mail
    5. - Comunicación mediante una red punto a punto
    6. - Comunicación mediante protocolos propietarios
    7. - Comunicación pasiva
    8. - Fast flux y DGA (Domain Generation Algorithms)
4. Recogida de información
    1. - Introducción
    2. - Recogida y análisis del registro
    3. - Recogida y análisis de los registros de eventos
    4. - Recogida y análisis de los archivos ejecutados durante el arranque
    5. - Recogida y análisis del sistema de archivos
    6. - Gestión de los archivos bloqueados por el sistema operativo
    7. - Framework de investigación inforense
    8. - Herramienta FastIR Collector
5. Imagen de memoria

1. - Presentación
2. - Realización de una imagen de memoria
3. - Análisis de una imagen de memoria
4. - Análisis de la imagen de memoria de un proceso

6. Funcionalidades de los malwares
    1. - Técnicas para ser persistente
    2. - Técnicas para ocultarse
    3. - Malware sin archivo
    4. - Esquivar el UAC
7. Modo operativo en caso de amenazas a objetivos persistentes (APT)
    1. - Introducción
    2. - Fase: reconocimiento
    3. - Fase: intrusión
    4. - Fase: persistencia
    5. - Fase: pivotar
    6. - Fase: filtración
    7. - Trazas dejadas por el atacante
8. Conclusión

UNIDAD DIDÁCTICA 2. ANÁLISIS BÁSICO

1. Creación de un laboratorio de análisis
    1. - Introducción
    2. - VirtualBox
    3. - La herramienta de gestión de muestras de malware Viper
2. Información sobre un archivo
    1. - Formato de archivo
    2. - Cadenas de caracteres presentes en un archivo
3. Análisis en el caso de un archivo PDF
    1. - Introducción
    2. - Extraer el código JavaScript
    3. - Desofuscar código JavaScript
    4. - Conclusión
4. Análisis en el caso de un archivo de Adobe Flash
    1. - Introducción
    2. - Extraer y analizar el código ActionScript
5. Análisis en el caso de un archivo JAR
    1. - Introducción
    2. - Recuperar el código fuente de las clases
6. Análisis en el caso de un archivo de Microsoft Office
    1. - Introducción
    2. - Herramientas que permiten analizar archivos de Office
    3. - Caso de malware que utiliza macros: Dridex
    4. - Caso de malware que utiliza alguna vulnerabilidad
7. Uso de PowerShell
8. Análisis en el caso de un archivo binario
    1. - Análisis de binarios desarrollados en AutoIt
    2. - Análisis de binarios desarrollados con el framework .NET
    3. - Análisis de binarios desarrollados en C o C++

9. El formato PE
    1. - Introducción
    2. - Esquema del formato PE
    3. - Herramientas para analizar un PE
    4. - API de análisis de un PE
10. 1Seguir la ejecución de un archivo binario
11. Introducción
12. Actividad a nivel del registro
13. Actividad a nivel del sistema de archivos
14. Actividad de red
15. Actividad de red de tipo HTTP(S)
16. 1Uso de Cuckoo Sandbox
17. Introducción
18. Configuración
19. Uso
20. Limitaciones
21. Conclusión
22. 1Recursos en Internet relativos a los malwares
23. Introducción
24. Sitios que permiten realizar análisis en línea
25. Sitios que presentan análisis técnicos
26. Sitios que permiten descargar samples de malwares

UNIDAD DIDÁCTICA 3. REVERSE ENGINEERING

1. Introducción
    1. - Presentación
    2. - Legislación
2. Ensamblador x86
    1. - Registros
    2. - Instrucciones y operaciones
    3. - Gestión de la memoria por la pila
    4. - Gestión de la memoria por el montículo
    5. - Optimización del compilador
3. Ensamblador x64
    1. - Registros
    2. - Parámetros de las funciones
4. Análisis estático
    1. - Presentación
    2. - IDA Pro
    3. - Radare2
    4. - Técnicas de análisis
    5. - API Windows
    6. - Límites del análisis estático
5. Análisis dinámico
    1. - Presentación
    2. - WinDbg
    3. - Análisis del núcleo de Windows
    4. - Límites del análisis dinámico y conclusión

UNIDAD DIDÁCTICA 4. TÉCNICAS DE OFUSCACIÓN

1. Introducción
2. Ofuscación de las cadenas de caracteres
    1. - Introducción
    2. - Caso de uso de ROT13
    3. - Caso de uso de la función XOR con una clave estática
    4. - Caso de uso de la función XOR con una clave dinámica
    5. - Caso de uso de funciones criptográficas
    6. - Caso de uso de funciones personalizadas
    7. - Herramientas que permiten decodificar las cadenas de caracteres
3. Ofuscación del uso de la API de Windows
    1. - Introducción
    2. - Estudio del caso de Duqu
    3. - Estudio del caso de EvilBunny
4. Packers
    1. - Introducción
    2. - Packers que utilizan la pila
    3. - Packers que utilizan el montículo
    4. - Encoder Metasploit
5. Otras técnicas
    1. - Anti-VM
    2. - Anti-reverse engineering y anti-debug
6. Conclusión

UNIDAD DIDÁCTICA 5. DETECCIÓN, CONFINAMIENTO Y ERRADICACIÓN

1. Introducción
2. Indicadores de compromiso de red
    1. - Presentación
    2. - Uso de los proxys
    3. - Uso de detectores de intrusión
    4. - Casos complejos
3. Detección de archivos
    1. - Presentación
    2. - Firmas (o Hash)
    3. - Firmas con YARA
    4. - Firmas con ssdeep
4. Detección y erradicación de malwares con ClamAV
    1. - Presentación
    2. - Instalación
    3. - Uso
5. Artefactos del sistema
    1. - Tipos de artefactos
    2. - Herramientas
6. Uso de OpenIOC
    1. - Presentación
    2. - Uso
    3. - Interfaz gráfica de edición

4. - Detección
7. Conclusión

PARTE 5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

MÓDULO I. LA SEGURIDAD DEL LA INFORMACIÓN

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
    1. - Principio Básico de Confidencialidad
    2. - Principio Básico de Integridad
    3. - 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
    1. - Planes de acción para la utilización más segura de Internet
    2. - Estrategias para una sociedad de la información más segura
    3. - Ataques contra los sistemas de información
    4. - La lucha contra los delitos informáticos
    5. - La Agencia Europea de Seguridad de las Redes y de la información (ENISA)
3. Normas sobre gestión de la seguridad de la información: Familia de Normas ISO 27000
    1. - Familia de Normas ISO 27000
    2. - Norma ISO/IEC 27002:2009
4. Legislación española sobre seguridad de la información
    1. - La protección de datos de carácter persona
    2. - La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
    3. - El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
    4. - La Agencia Española de Protección de Datos
    5. - El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
    6. - La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos
    7. - La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico
    8. - La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
    9. - La Ley 59/2003, de 19 de diciembre, de firma electrónica
    10. - La Ley de propiedad intelectual

11. - La Ley de propiedad industrial

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
    1. - Las cláusulas del control de seguridad
    2. - Las principales categorías de seguridad
4. Evaluación y tratamiento de los riesgos de seguridad
    1. - Evaluación de los riesgos de seguridad
    2. - 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 77
    1. - Etapas en el desarrollo de una política de seguridad de la información
    2. - Características esenciales de una política de seguridad de la información
    3. - Documento de política de la seguridad de la información
    4. - Revisión de la política de seguridad de la información
2. Organización de la seguridad de la información
3. Organización interna de la seguridad de la información
    1. - Compromiso de la dirección con la seguridad de la información
    2. - Coordinación de la seguridad de la información
    3. - Asignación de responsabilidad de seguridad de la información
    4. - Autorización de procesos para facilidades procesadoras de la información
    5. - Acuerdos de confidencialidad para la protección de la información
    6. - Contacto con las autoridades y con grupos de interés especial en los incidentes de seguridad
    7. - Revisión independiente de la seguridad de la información
4. Grupos o personas externas: el control de acceso a terceros
    1. - Identificación de los riesgos de seguridad relacionados con personas externas
    2. - Tratamiento de la seguridad de la información en las relaciones con los clientes
    3. - Tratamiento de la seguridad de la información en acuerdos con terceros
5. Clasificación y control de activos de seguridad de la información
6. Responsabilidad por los activos de seguridad de la información
    1. - Inventario de los activos de seguridad de la información
    2. - Propiedad de los activos de seguridad de la información
    3. - Uso aceptable de los activos de seguridad de la información
7. Clasificación de la información
    1. - Lineamientos de clasificación de la información
    2. - Etiquetado y manejo de 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

    1. - Establecimiento de roles y responsabilidades de los candidatos
    2. - Investigación de antecedentes de los candidatos para el empleo
    3. - Términos y condiciones del empleo
3. Medidas de seguridad de la información durante el empleo
    1. - Responsabilidades de la gerencia o dirección de la organización
    2. - Conocimiento, educación y capacitación en seguridad de la información
    3. - Incumplimiento de las previsiones relativas a la seguridad de la información: el proceso disciplinario
4. Seguridad de la información en la finalización de la relación laboral o cambio de puesto de trabajo
    1. - Responsabilidades de terminación
    2. - Devolución de los activos
    3. - Cancelación de los derechos de acceso a la información
5. Seguridad de la información ligada a la seguridad física y ambiental o del entorno
6. Las áreas seguras
    1. - El perímetro de seguridad física
    2. - Los controles de ingreso físico
    3. - Aseguramiento de oficinas, locales, habitaciones y medios
    4. - Protección contra amenazas internas y externas a la información
    5. - El trabajo en áreas aseguradas
    6. - Control y aislamiento de áreas de carga y descarga
7. Los equipos de seguridad
    1. - Seguridad en el emplazamiento y protección de equipos
    2. - Instalaciones de suministro seguras
    3. - Protección del cableado de energía y telecomunicaciones
    4. - Mantenimiento de los equipos
    5. - Seguridad de los equipos fuera de las instalaciones
    6. - Reutilización o retirada segura de equipos
    7. - Retirada de materiales propiedad de la empresa

UNIDAD DIDÁCTICA 6. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

1. Aproximación a la gestión de las comunicaciones y operaciones
2. Procedimientos y responsabilidades operacionales
    1. - Documentación de los procesos de operación
    2. - La gestión de cambios en los medios y sistemas de procesamiento de información
    3. - Segregación de tareas o deberes para reducir las modificaciones no autorizadas
    4. - Separación de los recursos de desarrollo, prueba y operación para reducir los riesgos de acceso no autorizado
3. Gestión de la prestación de servicios de terceras partes
    1. - Provisión o entrega del servicio
    2. - Supervisión y revisión de los servicios prestados por terceros
    3. - Gestión de cambios en los servicios prestados por terceros
4. Planificación y aceptación del sistema
    1. - Gestión de capacidades de los sistemas
    2. - Aceptación del sistema de información nuevo o actualizado
5. Protección contra códigos maliciosos y móviles
    1. - Controles contra el código malicioso
    2. - Control contra códigos móviles

6. Copias de seguridad de la información
7. Gestión de la seguridad de la red
    1. - Los controles de red
    2. - La seguridad de los servicios de red
8. Gestión de medios
    1. - Gestión de medios removibles o extraíbles
    2. - Eliminación de soportes o medios
    3. - Procedimientos para el manejo de la información
    4. - La seguridad de la documentación del sistema
9. El intercambio de información
    1. - Políticas y procedimientos de intercambio de información
    2. - Acuerdos de intercambio de información y software
    3. - Seguridad de los soportes físicos en tránsito
    4. - Seguridad de la información en el uso de la mensajería electrónica
    5. - Los sistemas de información empresariales
10. Los servicios de comercio electrónico
    1. - Información relativa al comercio electrónico
    2. - Las transacciones en línea
    3. - La seguridad de la información puesta a disposición pública
11. Supervisión para la detección de actividades no autorizadas
    1. - Registro de incidencias o de auditoría
    2. - Supervisión del uso del sistema
    3. - La protección de la información de los registros
    4. - Mantenimiento de los registros del administrador del sistema y del operador
    5. - El registro de fallos
    6. - Sincronización de reloj entre los equipos

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
    1. - Política de control de acceso
3. Gestión de acceso de usuario
    1. - Registro del usuario
    2. - Gestión o administración de privilegios
    3. - Gestión de contraseñas de usuario
    4. - Revisión de los derechos de acceso de usuario
4. Responsabilidades del usuario
    1. - El uso de contraseñas
    2. - Protección de equipos desatendidos
    3. - Política de puesto de trabajo despejado y pantalla limpia
5. Control de acceso a la red
    1. - La política de uso de los servicios en red
    2. - Autentificación de los usuarios de conexiones externas
    3. - Identificación de equipos en las redes
    4. - Diagnóstico remoto y protección de los puertos de configuración
    5. - Segregación de las redes
    6. - Control de la conexión a la red
    7. - El control de routing o encaminamiento de red

6. Control de acceso al sistema operativo
    1. - Procedimientos seguros de inicio de sesión
    2. - Identificación y autentificación del usuario
    3. - El sistema de gestión de contraseñas
    4. - El uso de los recursos del sistema
    5. - La desconexión automática de sesión
    6. - Limitación del tiempo de conexión
7. Control de acceso a las aplicaciones y a la información
    1. - Restricciones del acceso a la información3
    2. - Aislamiento de sistemas sensibles
8. Informática móvil y teletrabajo
    1. - Los ordenadores portátiles y las comunicaciones móviles
    2. - El 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
    1. - Validación de los datos de entrada
    2. - El control de procesamiento interno
    3. - La integridad de los mensajes
    4. - Validación de los datos de salida
4. Controles criptográficos
    1. - Política de uso de los controles criptográficos
    2. - Gestión de claves
5. Seguridad de los archivos del sistema
    1. - Control del software en explotación
    2. - Protección de los datos de prueba en el sistema
    3. - El control de acceso al código fuente de los programas
6. Seguridad de los procesos de desarrollo y soporte
    1. - Procedimientos para el control de cambios
    2. - Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo
    3. - Restricciones a los cambios en los paquetes de software
    4. - Las fugas de información
    5. - Desarrollo de software por terceros
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
    1. - Notificación de los eventos en la seguridad de la información
    2. - Notificación de puntos débiles de la seguridad
3. Gestión de incidentes y mejoras en la seguridad de la información
    1. - Responsabilidades y procedimientos
    2. - Aprendizaje de los incidentes de seguridad de la información

3. - Recopilación de evidencias
4. Gestión de la continuidad del negocio
5. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio
    1. - Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
    2. - Continuidad del negocio y evaluación de riesgos 237
    3. - Desarrollo e implantación de planes de continuidad del negocio que incluyan la seguridad de la información
    4. - Marco de referencia para la planificación de la continuidad del negocio
    5. - Pruebas, mantenimiento y reevaluación de los planes de continuidad

UNIDAD DIDÁCTICA 10. CUMPLIMIENTO DE LAS PREVISIONES LEGALES Y TÉCNICAS

1. Cumplimiento de los requisitos legales
    1. - Normativa aplicable
    2. - Derechos de propiedad intelectual
    3. - Protección de registros organizacionales
    4. - Privacidad de la información personal
    5. - Prevención del mal uso de los medios de procesamiento de la información
    6. - Regulación de los controles criptográficos
2. Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico
    1. - Cumplimiento de las políticas y estándares de seguridad
    2. - Verificación del cumplimiento técnico
3. Consideraciones de la auditoría de los sistemas de información
    1. - Controles de auditoría de los sistemas de información
    2. - Protección de las herramientas de auditoría de los sistemas de información

MÓDULO II. EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 11. LA NORMA UNE-EN-ISO/IEC 27001:2014

1. Objeto y ámbito de aplicación
2. Relación con la Norma ISO/IEC 27002:2009
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
    1. - Acciones para tratar los riesgos y oportunidades
    2. - Objetivos de seguridad de la información y planificación para su consecución
3. Soporte

UNIDAD DIDÁCTICA 13.SEGUIMIENTO DE LA IMPLANTACIÓN DEL SISTEMA

1. Operación
2. Evaluación del desempeño

1. - Seguimiento, medición, análisis y evaluación
2. - Auditoría interna
3. - Revisión por la dirección

3. Mejora
    1. - No conformidad y acciones correctivas
    2. - Mejora continua

¿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