EUROINNOVA BUSINESS SCHOOL

FORMACIÓN ONLINE

Titulación certificada por EUROINNOVA BUSINESS SCHOOL

Master en Hacking Ético + Titulación Universitaria

EUROINNOVA FORMACIÓN

Especialistas en Formación Online

SOBRE EUROINNOVA BUSINESS SCHOOL

Bienvenidos/as a EUROINNOVA BUSINESS SCHOOL, una escuela de negocios apoyada por otras entidades de enorme prestigio a nivel internacional, que han visto el valor humano y personal con el que cuenta nuestra empresa; un valor que ha hecho que grandes instituciones de reconocimiento mundial se sumen a este proyecto.

EUROINNOVA BUSINESS SCHOOL es la mejor opción para formarse ya que contamos con años de experiencia y miles de alumnos/as, además del reconocimiento y apoyo de grandes instituciones a nivel internacional.

Como entidad acreditada para la organización e impartición de formación de postgrado, complementaria y para el empleo, Euroinnova es centro autorizado para ofrecer formación continua bonificada para personal trabajador, cursos homologados y baremables para Oposiciones dentro de la Administración Pública, y cursos y acciones formativas de máster online con título propio.

CERTIFICACIÓN EN CALIDAD

Euroinnova Business School es miembro de pleno derecho en la Comisión Internacional de Educación a Distancia, (con estatuto consultivo de categoría especial del Consejo Económico y Social de NACIONES UNIDAS), y cuenta con el Certificado de Calidad de la Asociación Española de Normalización y Certificación (AENOR) de acuerdo a la normativa ISO 9001, mediante la cual se Certifican en Calidad todas las acciones formativas impartidas desde el centro.

DESCUBRE EUROINNOVA FORMACIÓN

Líderes en Formación Online

APOSTILLA DE LA HAYA

Además de disponer de formación avalada por universidades de reconocido prestigio y múltiples instituciones, Euroinnova posibilita certificar su formación con la Apostilla de La Haya, dotando a sus acciones formativas de Titulaciones Oficiales con validez internacional en más de 160 países de todo el mundo.

PROFESIONALES A TU DISPOSICION

La metodología virtual de la formación impartida en Euroinnova está completamente a la vanguardia educativa, facilitando el aprendizaje a su alumnado, que en todo momento puede contar con el apoyo tutorial de grandes profesionales, para alcanzar cómodamente sus objetivos.

DESCUBRE NUESTRAS METODOLOGÍAS

Desde Euroinnova se promueve una enseñanza multidisciplinar e integrada, desarrollando metodologías innovadoras de aprendizaje que permiten interiorizar los conocimientos impartidos con una aplicación eminentemente práctica, atendiendo a las demandas actuales del mercado laboral.

NUESTRA EXPERIENCIA NOS AVALA

Más de 15 años de experiencia avalan la trayectoria del equipo docente de Euroinnova Business School, que desde su nacimiento apuesta por superar los retos que deben afrontar los/las profesionales del futuro, lo que actualmente lo consolida como el centro líder en formación online.

Master en Hacking Ético + Titulación Universitaria

DURACIÓN:
725 horas

MODALIDAD:
Online

PRECIO:
1.495 € *

CRÉDITOS:
5,00 ECTS

* Materiales didácticos, titulación y gastos de envío incluidos.

CENTRO DE FORMACIÓN:

Euroinnova Business School

TITULACIÓN

Titulación Múltiple: - Titulación de Master en Hacking Ético con 600 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 Universitaria en Consultor en Seguridad Informática IT: Ethical Hacking con 5 Créditos Universitarios ECTS

EUROINNOVA BUSINESS SCHOOL
TITULACIÓN EXPEDIDA POR EUROINNOVA BUSINESS SCHOOL CENTRO DE ESTUDIOS DE POSTGRADO

3ª Mejor Escuela de Negocios España (RANKING EL ECONOMISTA)

Una vez finalizado el curso, el alumno recibirá por parte de Euroinnova Formación vía correo postal, la titulación que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/master, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Euroinnova Formación, Instituto Europeo de Estudios Empresariales y Comisión Internacional para la Formación a Distancia de la UNESCO).


EUROINNOVA FORMACIÓN

EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXXX que presta sus servicios en la empresa LABORATORIO ELECTROTECNICO, S.C.C.L. con C.I.F. XXXXXXXXX ha cursado la acción formativa

Nombre de la Acción Formativa

perteneciente al Plan de Formación Continua impartido por EUROINNOVA con Nº Exp.XXXXXXXXX dentro del marco de la Fundación Estatal para la Formación en el empleo dirigido a trabajadores de todos los sectores en la convocatoria del 2019.

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 11 de Noviembre de 2019

La Dirección General

JESÚS MORENO HIDALGO

Sello

Firma del Alumno/a

VÍCTOR LUIS LLORENTE

DESCRIPCIÓN

Este Master en Hacking Ético le ofrece una formación especializada en la materia. La necesidad de ambientes computacionales más seguros es cada vez más importante, y la única forma de alcanzar nuestro objetivo y afrontar el reto es poner en práctica tres aspectos claves: - Estableciendo medidas de seguridad adecuadas, que se anticipen a posibles fallas del sistema y de forma efectiva protejan los activos de la red. - Utilizar la tecnología apropiada y correctamente configurada para mantener un sistema de datos confiable. - Conocimiento de los tipos de ataques de los que podemos ser víctimas y de posibles modalidades de código malicioso que interviene en dichos ataques. Este curso brinda los conocimientos suficientes y necesarios para apoyar a los profesionales en la toma de decisiones de que medidas implantar a la hora de mejorar la seguridad en las empresas.

OBJETIVOS

- Conocer los requisitos de Seguridad en Sistemas de las TIC.
- Identificar las amenazas y vulnerabilidades que representan las nuevas tecnologías.
- Tomar decisiones sobre las medidas a implantar para la mejora de la seguridad en las empresas.
- Aprender sobre la metodología de un ataque y los medios para identificar las vulnerabilidades o fallos de seguridad a través de los que introducirse en un sistema.
- Conocer los fallos físicos, que permiten un acceso directo a ordenadores, y los fallos de red y Wi-Fi se presentan e ilustran cada uno con propuestas de contramedidas.

A QUIÉN VA DIRIGIDO

Este Master en Hacking Ético está especialmente orientado a técnicos y profesionales, gerentes, administradores y todo aquel relacionado con las áreas de Redes, Internet, Seguridad, Sistemas, Informática y tecnologías afines, que quieran adquirir los conocimientos sobre Seguridad en las comunicaciones y la información.

PARA QUÉ TE

Al terminar el Master en Hacking Ético el alumno tendrá amplios conocimientos de Seguridad en Sistemas de las TIC.

SALIDAS LABORALES

Departamentos de informática de empresas de todos los sectores.

MATERIALES DIDÁCTICOS

- Maletín porta documentos

- Manual teórico 'Gestión de Incidentes de Seguridad Informática'

- Manual teórico 'Sistemas Seguros de Acceso y Transmisión de Datos'

- Manual teórico 'Técnico en Instalación, Configuración y Mantenimiento de Redes'

- Manual teórico 'Seguridad Informática'

- Manual teórico 'Gestión de Servicios en el Sistema Informático'

- Manual teórico 'Ethical Hacking'

- Subcarpeta portafolios
- Dossier completo Oferta Formativa
- Carta de presentación
- Guía del alumno
- Bolígrafo

FORMAS DE PAGO

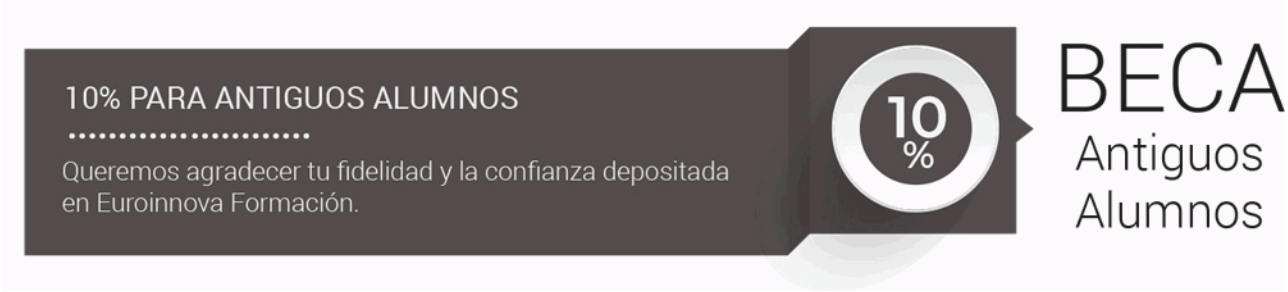
Contrareembolso / Transferencia / Tarjeta de Crédito / Paypal
Tarjeta de Crédito / PayPal Eligiendo esta opción de pago, podrá abonar el importe correspondiente, cómodamente en este mismo instante, a través de nuestra pasarela de pago segura concertada con Paypal Transferencia Bancaria
Eligiendo esta opción de pago, deberá abonar el importe correspondiente mediante una transferencia bancaria. No será aceptado el ingreso de cheques o similares en ninguna de nuestras cuentas bancarias.
Contrareembolso Podrá pagar sus compras directamente al transportista cuando reciba el pedido en su casa . Eligiendo esta opción de pago, recibirá mediante mensajería postal, en la dirección facilitada
Otras: PayU, Sofort, Western Union / SafetyPay
Fracciona tu pago en cómodos Plazos sin Intereses + Envío

Llama gratis al 900 831 200 e infórmate de nuestras facilidades de pago.

FINANCIACIÓN Y BECAS

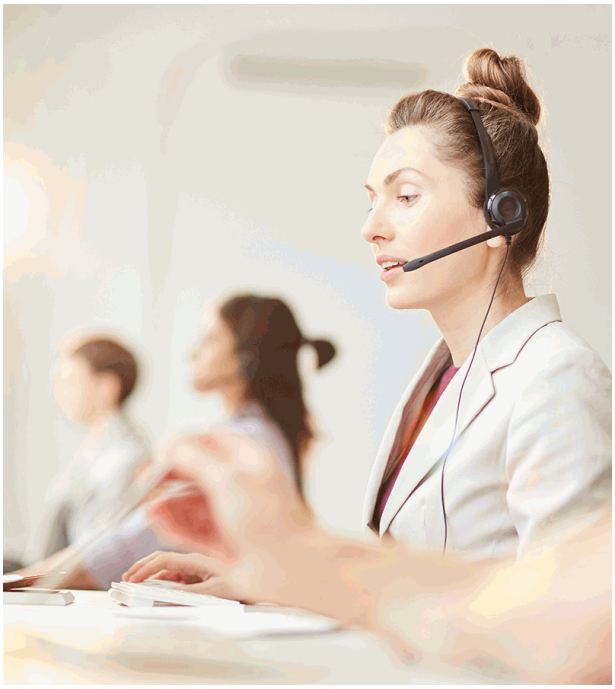
Facilidades económicas y financiación 100% sin intereses

En EUROINNOVA, ofrecemos a nuestros alumnos facilidades económicas y financieras para la realización de pago de matrículas, todo ello 100% sin intereses.
10% Beca Alumnos :Como premio a la fidelidad y confianza ofrecemos una beca a todos aquellos que hayan cursado alguna de nuestras acciones formativas en el pasado.



METODOLOGÍA Y TUTORIZACIÓN

El modelo educativo por el que apuesta Euroinnova es el aprendizaje colaborativo con un método de enseñanza totalmente interactivo, lo que facilita el estudio y una mejor asimilación conceptual, sumando esfuerzos, talentos y competencias.
El alumnado cuenta con un equipo docente especializado en todas las áreas.
Proporcionamos varios medios que acercan la comunicación alumno tutor, adaptándonos a las circunstancias de cada usuario.
Ponemos a disposición una plataforma web en la que se encuentra todo el contenido de la acción formativa. A través de ella, podrá estudiar y comprender el temario mediante actividades prácticas, autoevaluaciones y una evaluación final, teniendo acceso al contenido las 24 horas del día.
Nuestro nivel de exigencia lo respalda un acompañamiento



CARÁCTER OFICIAL DE LA FORMACIÓN

La presente formación no está incluida dentro del ámbito de la formación oficial reglada (Educación Infantil, Educación Primaria, Educación Secundaria, Formación Profesional Oficial FP, Bachillerato, Grado Universitario, Master Oficial Universitario y Doctorado). Se trata por tanto de una formación complementaria y/o de especialización, dirigida a la adquisición de determinadas competencias, habilidades o aptitudes de índole profesional, pudiendo ser baremable como mérito en bolsas de trabajo y/o concursos oposición, siempre dentro del apartado de Formación Complementaria y/o Formación Continua siendo siempre imprescindible la revisión de los requisitos específicos de baremación de las bolsa de trabajo público en concreto a la que deseemos presentarnos.

REDES SOCIALES

Síguenos en nuestras redes sociales y pasa a formar parte de nuestra gran comunidad educativa, donde podrás participar en foros de opinión, acceder a contenido de interés, compartir material didáctico e interactuar con otros alumnos, ex alumnos y profesores.

Además serás el primero en enterarte de todas las promociones y becas mediante nuestras publicaciones, así como también podrás contactar directamente para obtener información o resolver tus dudas.

LÍDERES EN FORMACION ONLINE

Somos Diferentes

Amplio Catálogo Format

Nuestro catálogo está formado por más de 18.000 cursos de múltiples áreas de conocimiento, adaptándonos a las necesidades formativas de nuestro alumnado.

Confianza

Contamos con el Sello de Confianza Online que podrás encontrar en tus webs de confianza. Además colaboramos con las más prestigiosas Universidades, Administraciones Públicas y Empresas de Software a nivel

Campus Online

Nuestro alumnado puede acceder al campus virtual desde cualquier dispositivo, contando con acceso ilimitado a los contenidos de su programa formativo.

Profesores/as Especialis

Contamos con un equipo formado por más de 50 docentes con especialización y más de 1.000 colaboradores externos a la entera disposición de nuestro alumnado.

Bolsa de Empleo

Disponemos de una bolsa de empleo propia con diferentes ofertas de trabajo correspondientes a los distintos cursos y masters. Somos agencia de colaboración Nº 9900000169 autorizada por el Ministerio de Empleo y Seguridad Social.

Garantía de Satisfacción

Más de 15 años de experiencia con un récord del 96% de satisfacción en atención al alumnado y miles de opiniones de personas satisfechas nos avalan.

Precios Competitivos

Garantizamos la mejor relación calidad/precio en todo nuestro catálogo formativo.

Calidad AENOR

Todos los procesos de enseñanza aprendizaje siguen los más rigurososcontroles de calidad extremos, estando certificados por AENOR conforme a la ISO 9001, llevando a cabo auditorías externas que garantizan la máxima calidad.

Club de Alumnos/as

Servicio Gratuito que permitirá al alumnado formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: beca, descuentos y promociones en formación. En esta, el alumnado podrá relacionarse con personas que estudian la misma área de conocimiento, compartir opiniones, documentos, prácticas y un sinfín de

Bolsa de Prácticas

Facilitamos la realización de prácticas de empresa gestionando las ofertas profesionales dirigidas a nuestro alumnado, para realizar prácticas relacionadas con la formación que ha estado recibiendo

Revista Digital

El alumnado podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, y otros recursos

Innovación y Calidad

Ofrecemos el contenido más actual y novedoso, respondiendo a la realidad empresarial y al entorno cambiante con una alta rigurosidad académica combinada con formación práctica.

ACREDITACIONES Y RECONOCIMIENTOS

TEMARIO

PARTE 1. INSTALACIÓN, CONFIGURACIÓN Y MANTENIMIENTO DE REDES

UNIDAD DIDÁCTICA 1. REDES ALÁMBRICAS O CABLEADAS

1.Introducción
2.Definiciones
3.Características de la red local
4.Medio de transmisión
5.Capacidad del medio: ancho de banda
6.Topología
7.Método de acceso
8.El modelo de referencia OSI
9.Datagramas
10.Protocolos

UNIDAD DIDÁCTICA 2. ELEMENTOS HARDWARE DE UNA RED

1.Elementos Hardware de una red
2.¿Cómo construir una red y compartir un acceso a Internet?

UNIDAD DIDÁCTICA 3. CONFIGURACIÓN DE RED EN WINDOWS 7

1.Centro de redes y recursos compartidos
2.Conectarse a una red
3.Administración de conexiones de red
4.Equipos y dispositivos
5.Grupo Hogar
6.Internet
7.Internet Explorer
8.Favoritos
9.Opciones de Internet
10.Exploración InPrivate
11.Compartir carpetas y recursos en red bajo Windows 7

UNIDAD DIDÁCTICA 4. INTERNET

1.Internet: una red de redes
2.¿Cómo se transmite la información en Internet?
3.El sistema de nombres por dominio
4.Formas de acceder a Internet
5.Seguridad en comunicaciones

UNIDAD DIDÁCTICA 5. REDES INALÁMBRICAS

1.¿Qué es una WLAN?
2.Tecnología utilizada

3.Aspectos importantes en las redes inalámbricas
4.Productos existentes en el mercado
5.¿Cómo configurar una red inalambrica en el Windows 7?

PARTE 2. SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

UNIDAD DIDÁCTICA 1. CRIPTOGRAFÍA

1.Perspectiva histórica y objetivos de la criptografía
2.Teoría de la información
3.Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos
4.Elementos fundamentales de la criptografía de clave privada y de clave publica
5.Características y atributos de los certificados digitales
6.Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente
7.Algoritmos criptográficos mas frecuentemente utilizados
8.Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización
9.Elementos fundamentales de las funciones resumen y los criterios para su utilización
10.Requerimientos legales incluidos en la ley 59/2003, de 19 de diciembre, de firma electrónica
11.Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización
12.Criterios para la utilización de técnicas de cifrado de flujo y de bloque
13.Protocolos de intercambio de claves
14.Uso de herramientas de cifrado tipo PGP, GPG o CryptoLoop

UNIDAD DIDÁCTICA 2. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1.Identificación de los componentes de una PKI y su modelo de relaciones
2.Autoridad de certificación y sus elementos
3.Política de certificado y declaración de practicas de certificación (CPS)
4.Lista de certificados revocados (CRL)
5.Funcionamiento de las solicitudes de firma de certificados (CSR)
6.Infraestructura de gestión de privilegios (PMI)
7.Campos de certificados de atributos, incluyen la descripción de sus usos habituales y la relación con los certificados digitales
8.Aplicaciones que se apoyan en la existencia de una PKI

UNIDAD DIDÁCTICA 3. COMUNICACIONES SEGURAS

1.Definición, finalidad y funcionalidad de redes privadas virtuales
2.Protocolo IPSec
3.Protocolos SSL y SSH

4.Sistemas SSL VPN
5.Túneles cifrados
6.Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN

PARTE 3. GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1.Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2.Identificación y caracterización de los datos de funcionamiento del sistema
3.Arquitecturas más frecuentes de los sistemas de detección de intrusos
4.Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5.Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

UNIDAD DIDÁCTICA 2. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1.Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio.
2.Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3.Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
4.Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
5.Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 3. CONTROL DE CÓDIGO MALICIOSO

1.Sistemas de detección y contención de código malicioso
2.Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar
3.Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso
4.Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
5.Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6.Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso
7.Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

UNIDAD DIDÁCTICA 4. RESPUESTA ANTE INCIDENTES DE SEGURIDAD

1.Procedimiento de recolección de información relacionada con incidentes de seguridad
2.Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad

3.Proceso de verificación de la intrusión
4.Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

UNIDAD DIDÁCTICA 5. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN

1.Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
2.Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
3.Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente
4.Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
5.Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo
6.Establecimiento del nivel de intervención requerido en función del impacto previsible
7.Guía para la investigación y diagnostico del incidente de intento de intrusión o infecciones
8.Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección
9.Proceso para la comunicación del incidente a terceros, si procede
10.Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE INFORMÁTICO

1.Conceptos generales y objetivos del análisis forense
2.Exposición del Principio de Lockard
3.Guía para la recogida de evidencias electrónicas:
4.Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta del sistema y la recuperación de ficheros borrados
5.Guía para la selección de las herramientas de análisis forense

PARTE 4. SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE 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 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. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

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 800-30
18.Exposición de la metodología Magerit versión 2

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

PARTE 5. GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

UNIDAD DIDÁCTICA 1. GESTIÓN DE LA SEGURIDAD Y NORMATIVAS

1.Norma ISO 27002 Código de buenas practicas para la gestión de la seguridad de la información
2.Metodología ITIL Librería de infraestructuras de las tecnologías de la información
3.Ley orgánica de protección de datos de carácter personal.
4.Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

UNIDAD DIDÁCTICA 2. ANÁLISIS DE LOS PROCESOS DE SISTEMAS

1.Identificación de procesos de negocio soportados por sistemas de información
2.Características fundamentales de los procesos electrónicos

3. Estados de un proceso,
4. Manejo de señales, su administración y los cambios en las prioridades
5.Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
6.Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
7.Técnicas utilizadas para la gestión del consumo de recursos

UNIDAD DIDÁCTICA 3. DEMOSTRACIÓN DE SISTEMAS DE ALMACENAMIENTO

1.Tipos de dispositivos de almacenamiento más frecuentes
2.Características de los sistemas de archivo disponibles
3.Organización y estructura general de almacenamiento
4.Herramientas del sistema para gestión de dispositivos de almacenamiento

UNIDAD DIDÁCTICA 4. UTILIZACIÓN DE MÉTRICAS E INDICADORES DE MONITORIZACIÓN DE RENDIMIENTO DE SISTEMAS

1.Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información
2.Identificación de los objetos para los cuales es necesario obtener indicadores
3.Aspectos a definir para la selección y definición de indicadores
4.Establecimiento de los umbrales de rendimiento de los sistemas de información
5.Recolección y análisis de los datos aportados por los indicadores
6.Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

UNIDAD DIDÁCTICA 5. CONFECCIÓN DEL PROCESO DE MONITORIZACIÓN DE SISTEMAS Y COMUNICACIONES

1.Identificación de los dispositivos de comunicaciones
2.Análisis de los protocolos y servicios de comunicaciones
3.Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
4.Procesos de monitorización y respuesta
5.Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
6.Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
7.Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
8.Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

UNIDAD DIDÁCTICA 6. SELECCIÓN DEL SISTEMA DE REGISTRO DE EN FUNCIÓN DE LOS REQUERIMIENTOS DE LA ORGANIZACIÓN

1.Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
2.Análisis de los requerimientos legales en referencia al registro
3.Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
4.Asignación de responsabilidades para la gestión del registro

5.Alternativas de almacenamiento para los registros del sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
6.Guía para la selección del sistema de almacenamiento y custodia de registros

UNIDAD DIDÁCTICA 7. ADMINISTRACIÓN DEL CONTROL DE ACCESOS ADECUADOS DE LOS SISTEMAS DE INFORMACIÓN

1.Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
2.Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
3.Requerimientos legales en referencia al control de accesos y asignación de privilegios
4.Perfiles de de acceso en relación con los roles funcionales del personal de la organización
5.Herramientas de directorio activo y servidores LDAP en general
6.Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
7.Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

PARTE 6. ETHICAL HACKING

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LOS ATAQUES Y AL HACKING ÉTICO

1.Introducción a la seguridad informática
2.El hacking ético
3.La importancia del conocimiento del enemigo
4.Seleccionar a la víctima
5.El ataque informático
6.Acceso a los sistemas y su seguridad
7.Análisis del ataque y seguridad

UNIDAD DIDÁCTICA 2. SOCIAL ENGINEERING

1.Introducción e historia del Social Engineering
2.La importancia de la Ingeniería social
3.Defensa ante la Ingeniería social

UNIDAD DIDÁCTICA 3. LOS FALLOS FÍSICOS EN EL ETHICAL HACKING Y LAS PRUEBAS DEL ATAQUE

1.Introducción
2.Ataque de Acceso físico directo al ordenador
3.El hacking ético
4.Lectura de logs de acceso y recopilación de información

UNIDAD DIDÁCTICA 4. LA SEGURIDAD EN LA RED INFORMÁTICA

1.Introducción a la seguridad en redes
2.Protocolo TCP/IP
3.IPv6
4.Herramientas prácticas para el análisis del tráfico en la red
5.Ataques Sniffing

6.Ataques DoS y DDoS
7.Ataques Robo de sesión TCP (HIJACKING) y Spoofing de IP
8.Ataques Man In The Middle (MITM).
9.Seguridad Wi-Fi
10.IP over DNS
11.La telefonía IP

UNIDAD DIDÁCTICA 5. LOS FALLOS EN LOS SISTEMAS OPERATIVOS Y WEB

1.Usuarios, grupos y permisos
2.Contraseñas
3.Virtualización de sistemas operativos
4.Procesos del sistema operativo
5.El arranque
6.Hibernación
7.Las RPC
8.Logs, actualizaciones y copias de seguridad
9.Tecnología WEB Cliente - Servidor
10.Seguridad WEB
11.SQL Injection
12.Seguridad CAPTCHA
13.Seguridad Akismet
14.Consejos de seguridad WEB

UNIDAD DIDÁCTICA 6. ASPECTOS INTRODUCTORIOS DEL CLOUD COMPUTING

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

UNIDAD DIDÁCTICA 7. CONCEPTOS AVANZADOS Y ALTA SEGURIDAD DE CLOUD COMPUTING

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

UNIDAD DIDÁCTICA 8. SEGURIDAD, AUDITORÍA Y CUMPLIMIENTO EN LA NUBE

1.Introducción
2.Gestión de riesgos en el negocio
1.- Recomendaciones para el gobierno

2.- Recomendaciones para una correcta gestión de riesgos
3.Cuestiones legales básicas. eDiscovery
4.Las auditorías de seguridad y calidad en cloud computing
5.El ciclo de vida de la información
1.- Recomendaciones sobre seguridad en el ciclo de vida de la información

UNIDAD DIDÁCTICA 9. CARACTERÍSTICAS DE SEGURIDAD EN LA PUBLICACIÓN DE PÁGINAS WEB

1.Seguridad en distintos sistemas de archivos.
1.- Sistema operativo Linux.
2.- Sistema operativo Windows.
3.- Otros sistemas operativos.
2.Permisos de acceso.
1.- Tipos de accesos
2.- Elección del tipo de acceso
3.- Implementación de accesos
3.Órdenes de creación, modificación y borrado.
1.- Descripción de órdenes en distintos sistemas
2.- Implementación y comprobación de las distintas órdenes.

UNIDAD DIDÁCTICA 10. PRUEBAS Y VERIFICACIÓN DE PÁGINAS WEB

1.Técnicas de verificación.
1.- Verificar en base a criterios de calidad.
2.- Verificar en base a criterios de usabilidad.
2.Herramientas de depuración para distintos navegadores.
1.- Herramientas para Mozilla.
2.- Herramientas para Internet Explorer.
3.- Herramientas para Opera.
4.- Creación y utilización de funciones de depuración.
5.- Otras herramientas.
3.Navegadores: tipos y «plug-ins».
1.- Descripción de complementos.
2.- Complementos para imágenes.
3.- Complementos para música.
4.- Complementos para vídeo.
5.- Complementos para contenidos.
6.- Máquinas virtuales.

UNIDAD DIDÁCTICA 11. LOS FALLOS DE APLICACIÓN

1.Introducción en los fallos de aplicación
2.Los conceptos de código ensamblador y su seguridad y estabilidad
3.La mejora y el concepto de shellcodes
4.Buffer overflow
5.Fallos de seguridad en Windows