



INESEM

BUSINESS SCHOOL

***Master en Dirección y Gestión de la Ciberseguridad
+ Titulación Universitaria***

+ Información Gratis

titulación de formación continua bonificada expedida por el instituto europeo de estudios empresariales

Master en Dirección y Gestión de la Ciberseguridad + Titulación Universitaria

duración total: 725 horas

horas teleformación: 300 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

Este Master en Dirección y Gestión de la Ciberseguridad le ofrece una formación especializada en la materia. Debemos saber que la seguridad informática (y ethical hacking), es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. En la actualidad, los ataques cibernéticos se suceden cada vez con mayor frecuencia y sofisticación, afectando por igual a entidades de todo tipo.



+ Información Gratis

a quién va dirigido

Todos aquellos trabajadores y profesionales en activo que deseen adquirir o perfeccionar sus conocimientos técnicos en este área.

objetivos

- Conocer la definición precisa de los diferentes tipos de hackers y de sus objetivos.
- 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.
- Saber sobre el Cloud Computing (su historia, su funcionamiento) para dominar mejor la seguridad.
- Tener en cuenta la seguridad en la web y los fallos actuales identificados gracias a la ayuda de herramientas que el lector puede implantar fácilmente en sus propios sistemas.
- Identificar siempre los posibles fallos para establecer después la estrategia de protección adecuada.
- Conocer algunos ejemplos los fallos de sistemas en Windows o Linux y los fallos de aplicación, para familiarizarse con el lenguaje ensamblador y comprender mejor las posibilidades de ataque.

para qué te prepara

Este Master en Dirección y Gestión de la Ciberseguridad le prepara para tener una visión amplia y precisa de la seguridad informática y ciberseguridad en cualquier entorno que trabaje en temas relacionados con la informática, adquiriendo las técnicas oportunas para realizar auditorías, gestión y otras acciones relacionadas con la seguridad informática.

salidas laborales

Seguridad informática / Auditor de seguridad informática / Ciberseguridad en empresas.

titulación

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

Esta titulación incluirá el nombre del curso/máster, 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 (Instituto Europeo de Estudios Empresariales).



INSTITUTO EUROPEO DE ESTUDIOS EMPRESARIALES

como centro de Formación acreditado para la impartición a nivel nacional de formación
EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXX ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación INESEM en la convocatoria de XXXX
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX- XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en
Granada, a (día) de (mes) de (año)

La dirección General

MARIA MORENO HIDALGO

Firma del alumno/a

Sello



NOMBRE DEL ALUMNO/A

forma de bonificación

- Mediante descuento directo en el TC1, a cargo de los seguros sociales que la empresa paga cada mes a la Seguridad Social.

metodología

El alumno comienza su andadura en INESEM a través del Campus Virtual. Con nuestra metodología de aprendizaje online, el alumno debe avanzar a lo largo de las unidades didácticas del itinerario formativo, así como realizar las actividades y autoevaluaciones correspondientes. Al final del itinerario, el alumno se encontrará con el examen final, debiendo contestar correctamente un mínimo del 75% de las cuestiones planteadas para poder obtener el título.

Nuestro equipo docente y un tutor especializado harán un seguimiento exhaustivo, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

El alumno dispone de un espacio donde gestionar todos sus trámites administrativos, la Secretaría Virtual, y de un lugar de encuentro, Comunidad INESEM, donde fomentar su proceso de aprendizaje que enriquecerá su desarrollo profesional.

materiales didácticos

- Manual teórico 'Gestión de Incidentes de Seguridad Informática'
- Manual teórico 'Sistemas Seguros de Acceso y Transmisión de Datos'
- Manual teórico 'Auditoría de Seguridad Informática'
- Manual teórico 'Seguridad en Equipos Informáticos'
- Manual teórico 'Ethical Hacking'
- Manual teórico 'Sistema de Gestión de Seguridad de la Información UNE-ISO/IEC 27001:2017'



profesorado y servicio de tutorías

Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “Guía del Alumno” entregado junto al resto de materiales de estudio.

Contamos con una extensa plantilla de profesores especializados en las distintas áreas formativas, con una amplia experiencia en el ámbito docente.

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas, así como solicitar información complementaria, fuentes bibliográficas y asesoramiento profesional. Podrá hacerlo de las siguientes formas:

- **Por e-mail:** El alumno podrá enviar sus dudas y consultas a cualquier hora y obtendrá respuesta en un plazo máximo de 48 horas.

- **Por teléfono:** Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.

- **A través del Campus Virtual:** El alumno/a puede contactar y enviar sus consultas a través del mismo, pudiendo tener acceso a Secretaría, agilizando cualquier proceso administrativo así como disponer de toda su documentación



plazo de finalización

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la misma duración del curso. Existe por tanto un calendario formativo con una fecha de inicio y una fecha de fin.

campus virtual online

especialmente dirigido a los alumnos matriculados en cursos de modalidad online, el campus virtual de ineseem ofrece contenidos multimedia de alta calidad y ejercicios interactivos.

comunidad

servicio gratuito que permitirá al alumno formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: becas, descuentos y promociones en formación, viajes al extranjero para aprender idiomas...

revista digital

el alumno 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, etc.

secretaría

Este sistema comunica al alumno directamente con nuestros asistentes, agilizando todo el proceso de matriculación, envío de documentación y solución de cualquier incidencia.

Además, a través de nuestro gestor documental, el alumno puede disponer de todos sus documentos, controlar las fechas de envío, finalización de sus acciones formativas y todo lo relacionado con la parte administrativa de sus cursos, teniendo la posibilidad de realizar un seguimiento personal de todos sus trámites con INESEM

programa formativo

PARTE 1. ETHICAL HACKING

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

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

UNIDAD DIDÁCTICA 2. SOCIAL ENGINEERING

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

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

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

UNIDAD DIDÁCTICA 4. LA SEGURIDAD EN LA RED INFORMÁTICA

- 1.Introducción a la seguridad en redes
- 2.Protocolo TCP/IP
- 3.IPv6
- 4.Herramientas prácticas para el análisis del tráfico en la red
- 5.Ataques Sniffing
- 6.Ataques DoS y DDoS
- 7.Ataques Robo de sesión TCP (HIJACKING) y Spoofing de IP
- 8.Ataques Man In The Middle (MITM).
- 9.Seguridad Wi-Fi
- 10.IP over DNS
- 11.La telefonía IP

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

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

UNIDAD DIDÁCTICA 6. ASPECTOS INTRODUCTORIOS DEL CLOUD COMPUTING

- 1.Orígenes del cloud computing
- 2.Qué es cloud computing

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

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

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

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

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

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

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

UNIDAD DIDÁCTICA 10. PRUEBAS Y VERIFICACIÓN DE PÁGINAS WEB

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

UNIDAD DIDÁCTICA 11. LOS FALLOS DE APLICACIÓN

- 1.Introducción en los fallos de aplicación

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

PARTE 2. GESTIÓN DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

MÓDULO 1. LA SEGURIDAD DE 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 personal
 - 2.- La Ley Orgánica - de 13 de diciembre, de Protección de Datos de Carácter Personal
 - 3.- El Real Decreto - de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de 13 de diciembre, de protección de datos de carácter personal
 - 4.- La Agencia Española de Protección de Datos
 - 5.- El Real Decreto - de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
 - 6.- Ley - de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
 - 7.- La Ley - de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico
 - 8.- La Ley - de 9 de mayo, General de Telecomunicaciones
 - 9.- La Ley - 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

- 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.- Seguridad de oficinas, locales, habitaciones y medios
- 4.- Protección contra amenazas internas y externas a la información
- 5.- El trabajo en áreas aseguradas

- 6.- 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
 - 8.- Equipo de usuario desatendido
 - 9.- Política de puesto de trabajo despejado y pantalla limpia

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.- Gestión de capacidades
 - 4.- Separación de los recursos de desarrollo, prueba y operación para reducir los riesgos de acceso no autorizac
- 3.Gestión de la prestación de servicios de terceras partes
 - 1.- Política de seguridad de la información en las relaciones con los proveedores
 - 2.- Requisitos de seguridad en contrato con terceros
 - 3.- Cadena de suministros de tecnología de la información y de las comunicaciones
- 4.Planificación y aceptación del sistema
 - 1.- Políticas para la seguridad de la información
 - 2.- Revisión de las políticas para la seguridad de la información
- 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
 - 3.- Segregación en redes
- 8.Gestión de medios
 - 1.- Gestión de medios removibles o extraíbles
 - 2.- Eliminación de soportes o medios
 - 3.- Soportes físicos en tránsito
 - 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
 - 3.- Seguridad de los soportes físicos en tránsito
 - 4.- Mensajería electrónica
 - 5.- Acuerdos de confidencialidad o no revelación
- 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 eventos
 - 2.- Protección de la información de los registros
 - 3.- Sincronización de reloj

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.- Autenticación 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 autenticación 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 información
 - 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.- Entorno de desarrollo seguro
- 5.- Externalización 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
 - 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 2. EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 11. LA NORMA UNE-EN-ISO/IEC 27001:2017

- 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
- 3. Planificación
 - 1.- Acciones para tratar los riesgos y oportunidades
 - 2.- Objetivos de seguridad de la información y planificación para su consecución
- 4. 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

PARTE 3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

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. ROBUSTECIMIENTO DE SISTEMAS

1. Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información
2. Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
3. Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
4. Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
5. Actualización de parches de seguridad de los sistemas informáticos
6. Protección de los sistemas de información frente a código malicioso
7. Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
8. Monitorización de la seguridad y el uso adecuado de los sistemas de información

UNIDAD DIDÁCTICA 9. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

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

PARTE 4. AUDITORÍA DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA

1. Código deontológico de la función de auditoría
2. Relación de los distintos tipos de auditoría en el marco de los sistemas de información
3. Criterios a seguir para la composición del equipo auditor
4. Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
5. Tipos de muestreo a aplicar durante el proceso de auditoría
6. Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
7. Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
8. Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
9. Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

UNIDAD DIDÁCTICA 2. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Principios generales de protección de datos de carácter personal
2. Normativa europea recogida en la directiva 95/46/CE
3. Normativa nacional recogida en el código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007)

4. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
5. Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
6. Guía para la realización de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de carácter personal

UNIDAD DIDÁCTICA 3. 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 efecto sobre las vulnerabilidades y amenazas
11. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializar
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 4. 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 5. 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 6. 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 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 política 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 diagnóstico 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 oculta información oculta del sistema y la recuperación de ficheros borrados
- 5.Guía para la selección de las herramientas de análisis forense

PARTE 6. 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

+ Información Gratis