ESIBE ESCUELA IBEROAMERICANA DE POSTGRADO

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

FORMACIÓN ONLINE

Máster en Análisis y Medidas de Seguridad contra el Malware + Titulación Universitaria

ESIBE
Formación
Online

ESIBE se basa en una metodología completamente a la vanguardia educativa

SOBRE ESIBE

ESIBE nace del afán por crear un punto de encuentro entre Europa, en conc Latinoamérica.

A raíz de este reto, desarrollamos una nueva oferta formativa, marcada por en línea y unos contenidos de gran calidad que te permitirán obtener los cor necesitas para especializarte en tu campo.

Además, hemos diseñado para ti un campus con la última tecnología en sist que recoge todos los materiales que te serán útiles en tu adquisición de nue

Las Titulaciones acreditadas por ESIBE pueden certificarse con la Apostilla (Certificación Oficial de Carácter Internacional que le da validez a las Titulac en más de 160 países de todo el mundo).
Hemos reinventado la formación online, de manera que nuestro alumnado p superando de forma flexible cada una de las acciones formativas con las qu todas las áreas del saber y, con la garantía de aprender las habilidades y he realmente demandados en el mercado laboral.

Nuestro centro forma parte del grupo educativo Euroinnova, líder en el secto gracias a su contenido de calidad e innovadora metodología con 20 años de ESIBE cuenta con el respaldo de INESEM, reconocida escuela de negocios Euroinnova, centro formativo con más de 300.000 alumnos de los cinco con Además, ESIBE imparte formaciones avaladas por Universidades de prestig como Universidad Nebrija, Universidad Europea Miguel de Cervantes o Univ E-Campus.

No somos solo una escuela, somos el lugar ideal donde formarte.

Máster en Análisis y Medidas de Seguridad contra el Malware + Titulación Universitaria

DURACIÓN:
1.500 horas

MODALIDAD:
Online

PRECIO:
A consultar
(Sujeto a política de becas)

CRÉDITOS:
8 ECTS

CENTRO DE FORMACIÓN:

ESIBE
Escuela Iberoamericana de Postgrado

ESIBE ESCUELA IBEROAMERICANA DE POSTGRADO

Titulación

Doble Múltiple: - Titulación de Master en Análisis y Medidas de Seguridad contra el Malware con 1500 horas expe
EUROINNOVA INTERNATIONAL ONLINE EDUCATION, miembro de la AEEN (Asociación Española de Escu
reconocido con la excelencia académica en educación online por QS World University Rankings - Titulación Univ
Consultor en Seguridad Informática IT: Ethical Hacking con 8 Créditos Universitarios ECTS.
Una vez finalizada la formación, el alumnado recibirá por parte de ESIBE vía correo postal, la titulación que acredit
con éxito todas las pruebas de conocimientos propuestas.
Esta titulación incluirá el nombre del curso/máster, su duración, el nombre y DNI, el nivel de aprovechamiento que
superación de las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de las instituciones q
formación recibida (Euroinnova Formación, Instituto Europeo de Estudios Empresariales y Comisión Internacional
a Distancia de la UNESCO)

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

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 20XX
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
JESÚS MORENO HIDALGO

Sello

Firma del Alumno/a
NOMBRE DEL ALUMNO

Descripción

En el contexto de avances tecnológicos incesantes y la sofisticación creciente de los ciberataques, el dominio del an de seguridad contra el malware se torna esencial. Este Máster en Análisis y Medidas de Seguridad contra el Malwar para formar expertos capaces de enfrentar dichos desafíos con eficiencia y proactividad. La cobertura de temáticas e abarcando desde la seguridad de los sistemas informáticos y la gestión de incidentes de seguridad hasta la auditoría olvidar la crucial competencia en ethical hacking y análisis de malware.

Nuestro programa destaca por ofrecer un contenido actualizado y en sintonía con las demandas del sector, priorizan teórica y práctica en estrategias de protección de datos personales, robustecimiento de sistemas, detección y respues y análisis forense. Además, el apartado de ethical hacking provee los fundamentos y habilidades necesarias para ide ante fallos de seguridad tanto en sistemas operativos como en aplicaciones web.

Elegir nuestro curso significa optar por una formación integral que no solo adapta su contenido a los cambios del pa la seguridad informática sino que también prepara a los alumnos para prevenir, detectar y contrarrestar sofisticados vulnerabilidades. Conviértase en un faro de ciberseguridad, listo para sobresalir en un ámbito en constante evolució

Objetivos

- Dominar seguridad de equipos.
- Ejecutar análisis de impacto.
- Aprender gestión de riesgos.
- Implementar seguridad lógica.
- Configurar cortafuegos.
- Gestionar normativas seguridad.
- Administrar sistemas de registro.
- Conocer auditoría informática.
- Controlar código malicioso.
- Responder a incidentes.
- Practicar análisis forense.
- Estudiar técnicas de malware.
- Realizar ethical hacking.

A quién va dirigido

Dirigido a expertos en IT, auditores, responsables de seguridad y profesionales técnicos, el Máster en Análisis y Me Seguridad contra el Malware ofrece formación avanzada en protección de sistemas informáticos, gestión de riesgos, y física, auditoría informática y estrategias de respuesta ante ciberataques. Ideal para quienes aspiran al máximo niv especialización en ciberseguridad.

Para qué te prepara

El Máster en Análisis y Medidas de Seguridad contra el Malware te prepara para ser un especialista en seguridad in Aprenderás a establecer criterios de protección de equipos, a elaborar análisis de impacto en negocios y a gestionar Podrás implementar planes de seguridad y auditar sistemas para detectar y prevenir intrusiones, configurar cortafue análisis forense. Además, adquirirás habilidades en la detección, confinamiento y erradicación de malware, utilizan ingeniería inversa y ethical hacking para asegurar infraestructuras IT.

Salidas Laborales

Con el Máster en Análisis y Seguridad contra Malware, prepárate para convertirte en un especialista en ciberseguri desempeñarte como analista de malware, auditor de sistemas informáticos, consultor IT en ethical hacking, o gestor de seguridad. Domina la prevención y respuesta ante amenazas, realizando análisis forenses y robusteciendo sistem formación clave para proteger la infraestructura crítica de cualquier organización en la era digital.

Materiales Didácticos

El alumn@ recibe un email con las Claves de Acceso al CAMPUS VIRTUAL en el que va a poder acced el contenido didáctico, así como las evaluaciones, vídeos explicativos, etc. así como a contactar con el t línea quien le va a ir resolviendo cualquier consulta o duda que le vaya surgiendo tanto por email, chat, telefono, etc.

Formas de Pago

- Tarjeta,
- Paypal

Otros: Otras formas de pago adaptadas a cada pais a traves de la plataforma de pago Ebanx.

Llama al teléfono (+34) 958 99 19 19 e infórmate de los pagos a plazos sin intereses que hay disponibles

Financiación

En ESIBE, tu aprendizaje es lo más importante. Por eso, hemos desarrollado contenidos, así como una innovadora en sistemas e-Learning con la que trabajarás para adquirir tus nuevos conocimientos con el nuestro claustro especializado en la materia. Te proporcionamos nociones imprescindibles para el desa actividad de tu ámbito.
Nuestro objetivo es convertirte en un profesional altamente cualificado, capaz de desempeñar las tarea puesto de responsabilidad en el sector.

Nuestra Metodología

En ESIBE, tu aprendizaje es lo más importante. Por eso, hemos desarrollado contenidos, así como una plataforma innovadora e sistemas e-Learning con la que trabajarás para adquirir tus nuevos conocimientos con el respaldo de nuestro claustro especializado en la materia. Te proporcionamos nociones imprescindibles para el desarrollo de la actividad de tu ámbito. Nuestro objetivo es convertirte en un profesional altamente cualificado, capaz de desempeñar las tareas propias de un pue de responsabilidad en el sector.

Redes Sociales

Síguenos en nuestras redes sociales y pasa a formar parte de nuest gran comunidad educativa, donde podrás participar en foros de opinión, acceder a contenido de interés, compartir material didácti e interactuar con otros/as alumnos/as, ex alumnos/as y profesores/ Además, te enterarás antes que nadie de todas las promociones y becas mediante nuestras publicaciones, así como también podrás contactar directamente para obtener información o resolver tus dudas.

Por qué estudiar en ESIBE

Formación en Linea

Organiza tu propio tiempo.

Apostilla de la Haya

Certifica tu titulación en países extranjeros.

Calidad Europea

Formacion especializada.

Contenido Actualizado

Revisamos de forma continua nuestro temario.

Campus Virtual

Plataforma con los últimos desarrollos del sector e-Learning.

Amplia Oferta Formativa

Encuentra la formación que se adapta a ti.

Valores ESIBE

Compromiso

En ESIBE, nuestros alumnos son lo más importante y, comiences tu formación con nosotros estaremos a tu la lograr tu máximo desarrollo profesional y personal.

Excelencia

Nuestros contenidos son de máxima calidad, ofreciénd oportunidad única de formación y crecimiento que te alcanzar puestos de gran responsabilidad en tu sector.

Unidad

Juntos, somos mucho más fuertes. Detrás de ESIBE ha equipo multidisciplinar que suma sus fuerzas para con sinergias que beneficien de forma directa a nuestros al

Adaptabilidad

Queremos facilitarte tu aprendizaje, por esto, tú marca propio ritmo.

Innovacion

ESIBE se sustenta en una cultura con un carácter innov diferenciado, promoviendo el desarrollo y uso de nuev tecnologías para el estudio y aprendizaje.

Flexibilidad

Tú tiempo es valioso para nosotros y, con el fin de que compaginar tu formación, te proporcionamos la flexibi necesitas, pudiendo realizar tu formación en cualquier del día.

Acreditaciones y Reconocimientos

Temario

MÓDULO 1. SEGURIDAD EN EQUIPOS INFORMÁTICOS

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE L 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 seguri 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 carácte

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

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

seguridad

6.Establecimiento de la monitorización y pruebas del cortafuegos

MÓDULO 2. GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTIC

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 po

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 RENDI

SISTEMAS

1.Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de infor

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 COMUNIC

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 REQUERIMIE 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, confide 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 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)

MÓDULO 3. AUDITORÍA INFORMÁTICA

UNIDAD DIDÁCTICA 1. 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 aceptad

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

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), I Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 4. Identificación y ficheros con datos de carácter personal utilizados por la organización

4.Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto realización de la auditoría bienal obligatoria de ley orgánica

UNIDAD DIDÁCTICA 3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS INFORMÁTICOS.

1.Introducción al análisis de riesgos
2.Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como 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 materializaci 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 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 determin 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 18. Exposición de la metodología Magerit

UNIDAD DIDÁCTICA 4. USO DE HERRAMIENTAS PARA LA AUDITORÍA INFORMÁTICA

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, Sucuri, 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 S 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 INFO

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

4.Guía para la elaboración del informe de auditoría

MÓDULO 4. GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTI

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 cor
4.Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y l 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 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 malicic
5.Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monito 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 se
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 mi
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 intru

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.○ Evidencias volátiles y no volátiles
5.○ Etiquetado de evidencias
6.○ Cadena de custodia
7.○ Ficheros y directorios ocultos
8.○ Información oculta del sistema
9.○ Recuperación de ficheros borrados
10.Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, info sistema y la recuperación de ficheros borrados
11.Guía para la selección de las herramientas de análisis forense

MÓDULO 5. ANÁLISIS DE MALWARE

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN

1.¿Qué es un Malware?
2.Tipos de Malware
1.- Backdoor
2.- Ransomware y locker
3.- Stealer
4.- Rootkit

UNIDAD DIDÁCTICA 2. ESCENARIO DE INFECCIÓN Y TÉCNICAS DE COMUNICACIÓN

1.Ejecución de un archivo adjunto
2.Clic desafortunado
3.Apertura de un documento infectado
4.Ataques informáticos
5.Ataques físicos: infección por llave USB
6.Introducción a las técnicas de comunicación con el C&C
1.- Comunicación a través de HTTP/HTTPS/FTP/IRC
2.- Comunicación a través e-mail
3.- Comunicación a través una red punto a punto
4.- Fast flux y DGA (Domain Generation Algorithms)

UNIDAD DIDÁCTICA 3. OBTENCIÓN Y ANÁLISIS DE INFORMACIÓN

1.Analizando datos del registro
2.Analizando datos del registros de eventos
3.Analizando archivos ejecutados durante el arranque
4.Analizando sistema de archivos

UNIDAD DIDÁCTICA 4. FUNCIONALIDADES DE LOS MALWARES. COMO OPERAR ANTE AMENAZAS

1.Técnicas de persistencia
2.Técnicas de ocultación
3.Malware sin archivo
4.Evitar el UAC
5.Fases para operar ante amenzas:
    1.- Reconocimiento
    2.- Intrusión
    3.- Persistencia
    4.- Pivotar
    5.- Filtración
    6.- Pistas dejadas por el atacante

UNIDAD DIDÁCTICA 5. ANÁLISIS BÁSICO DE ARCHIVOS

1.Análisis de un archivo PDF
2.Extraer el código JavaScript
3.Desofuscar código JavaScript
4.Análisis de un archivo de Adobe Flash
    1.- Extraer y analizar el código ActionScript
5.Análisis de un archivo JAR
6.Análisis de un archivo de Microsoft Office
    1.- Herramientas que permiten analizar archivos de Office

UNIDAD DIDÁCTICA 6. REVERSE ENGINEERING

1.¿Qué es Reverse Engineering?
2.Ensamblador x86
3.Ensamblador x64
4.Análisis estático
    1.- IDA Pro
    2.- Radare2
    3.- Técnicas de análisis
5.Análisis dinámico
    1.- WinDbg
    2.- Análisis del núcleo de Windows
    3.- Límites del análisis dinámico y conclusión

UNIDAD DIDÁCTICA 7. OFUSCACIÓN: INTRODUCCIÓN Y TÉCNICAS

1.¿Qué es la ofuscación?
2.Ofuscación de cadenas de caracteres
3.Ofuscación mediante la API de Windows
4.Packers
5.Otras tipos de técnicas ofuscación

UNIDAD DIDÁCTICA 8. DETECCIÓN Y CONFINAMIENTO

1.Primeros pasos en la detección y confinamiento
2.Compromiso de red: Indicadores
  1.- Presentación a los indicadores
  2.- Proxys
  3.- Sistemas de detectores de intrusión
3.Tips de firmas de archivo
  1.- Firmas (o Hash)
  2.- Firmas con YARA
  3.- Firmas con ssdeep
4.Detección y erradicación a través de ClamAV
  1.- Instalación
  2.- Usando ClamAV: Funciones básicas

UNIDAD DIDÁCTICA 9. OPENIOC

1.Introducción a OpenIOC
2.Pimeros pasos con
3.Interfaz gráfica de edición
4.Detección

MÓDULO 6. CONSULTOR EN SEGURIDAD INFORMÁTICA IT: ETHIC

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