Gestión de incidentes de seguridad informática



Código: 15032

Unidad Formativa:
MF0488_3 - Gestión de incidentes de seguridad informática

Módulo: MF0488_3 - GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Certificado de Profesionalidad:
IFCT0109 - SEGURIDAD INFORMÁTICA

Modalidad: ONLINE

Duración: 90h.

Metodología

El Curso está desarrollado con una metodología a distancia/online. Este sistema de enseñanza está organizado de tal forma que el alumno pueda compatibilizar el estudio con sus ocupaciones laborales o profesionales. También permite el acceso al curso a aquellas personas que viven en zonas rurales y que tienen interés en continuar formándose.
El alumno tiene que seguir un aprendizaje sistemático y un ritmo de estudio, adaptado a su disponibilidad de tiempo.

Se dispondrá de un extenso material sobre los aspectos teóricos del curso que deberá estudiar para la realización de pruebas objetivas tipo test. Para el aprobado, se exigirá un mínimo de 50% del total de las respuestas acertadas. Durante todo el transcurso de la formación, dispondrá de la atención de los tutores, así como la posibilidad de realizar consultas a través de la plataforma de teleformación para cursos online. Entre el material entregado en este curso, se adjunta un documento llamado *Guía didáctica del alumno* donde aparece el horario de tutorías y demás información relevante.

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la modalidad elegida y de las horas de formación. La titulación será remitida por correo una vez corregido su examen, o puesta a su disposición en la plataforma de teleformación una vez finalizado el curso.

Profesorado, medios y titulación

Nuestro centro de formación ha sido fundado en 1996 y en la actualidad, tiene presencia a nivel nacional disponiendo de una plantilla de más de 800 docentes entre personal laboral y freelance. Todos ellos son especialistas en diferentes familias profesionales y les acreditan los numerosos cursos que han impartido para nuestro grupo empresarial. Entre nuestro staff de formadores se encuentran ingenieros, arquitectos, economistas, informáticos, publicistas, diseñadores, médicos, enfermeros, veterinarios, fisioterapeutas, psicólogos, sociólogos, periodistas, filólogos, abogados, cocineros, licenciados en administración de empresas, licenciados en actividades físicas y deportivas, jardineros, peluqueros, educadores sociales, etc.

En todos nuestros cursos, independientemente de la metodología, se ponen a disposición del alumno los medios y materiales docentes necesarios para el desarrollo del mismo.
En los cursos en modalidad e-learning, las consultas y tutorías se pueden realizar a través de teléfono, email y la propia plataforma de teleformación.

En cuanto a la titulación, mostramos a continuación, el modelo de diploma que obtendrás a la finalización del curso:


Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

DIPLOMA
ACREDITATIVO

D./Dña. **XXXXX XXXXX XXXXX** con D.N.I. **11111111H**, ha realizado, con pleno aprovechamiento, el curso titulado **Curso Intensivo de Inglés B2**, con Código **19656** Grupo **30694**, entre los días **29/06/2023** y**30/08/2023**, con una duración total de **56** horas, en la modalidad formativa **ONLINE**

Contenidos impartidos (Ver Dorso)

Firma y sello de la entidad responsable de impartir la formación

Tel.: 91 1097505
www.aulaforma.es

Fecha de expedición
31 AGO 2023

Firma del alumno

Requistos previos

No hay requisitos previos, ni formativos ni profesionales.

Salidas profesionales

Este curso está específicamente diseñado para incrementar la cualificación profesional en la familia o sector correspondiente.

Objetivos

Este curso capacita al alumnado para planificar, implantar y operar los mecanismos de detección y prevención de intrusiones, control de código malicioso y respuesta ante incidentes de seguridad informática en entornos corporativos, y está dirigido a profesionales de sistemas, redes y ciberseguridad que asumen tareas de supervisión y gestión de la seguridad. A lo largo del recorrido se estudia el funcionamiento de los sistemas IDS/IPS, su ubicación y puesta en producción, así como la configuración, actualización y monitorización de las herramientas de protección frente a software malicioso. La parte aplicada ocupa un lugar central: el alumnado aprende a recolectar y correlacionar información, verificar intrusiones, clasificar los incidentes según su impacto, asignar responsabilidades y niveles de intervención, notificar y documentar su gestión hasta el cierre, coordinarse con los organismos de gestión de incidentes y aplicar técnicas de análisis forense con garantías sobre las evidencias. Al finalizar, el alumnado será capaz de desplegar y mantener los sistemas de detección y protección, gestionar el ciclo completo de un incidente de seguridad y elaborar el análisis forense necesario para determinar su alcance y sus consecuencias.

Contenidos

Módulo 1: Fundamentos y arquitecturas de los sistemas de detección y prevención de intrusiones
1.1 - Conceptos generales de la gestión de incidentes de seguridad
1.2 - Detección y prevención de intrusiones: principios y objetivos
1.3 - Identificación y caracterización de los datos de funcionamiento del sistema
1.4 - Arquitecturas habituales de los sistemas de detección de intrusos
1.5 - Tipos de IDS/IPS según su ubicación y funcionalidad
1.6 - Criterios de seguridad para ubicar los IDS/IPS en la red
Resumen del módulo 1
Módulo 2: Implantación y puesta en producción de sistemas IDS/IPS
2.1 - Análisis previo de servicios, protocolos, zonas y equipos implicados en los procesos de negocio
2.2 - Definición de políticas de corte de intentos de intrusión
2.3 - Análisis de eventos registrados y caracterización de falsos positivos
2.4 - Ajuste de las políticas de corte a partir de los falsos positivos detectados
2.5 - Registros de auditoría para monitorizar el funcionamiento del IDS/IPS
2.6 - Niveles de actualización, monitorización y pruebas del sistema
Resumen del módulo 2
Módulo 3: Control de código malicioso
3.1 - Sistemas de detección y contención de código malicioso
3.2 - Herramientas de control según la topología de la instalación y las vías de infección
3.3 - Criterios de seguridad para configurar las herramientas de protección
3.4 - Requerimientos y técnicas de actualización de las herramientas
3.5 - Registros de auditoría para supervisar el funcionamiento y los eventos de seguridad
3.6 - Monitorización y pruebas de las herramientas de protección
3.7 - Análisis de programas maliciosos con desensambladores y entornos controlados
Resumen del módulo 3
Módulo 4: Respuesta ante incidentes de seguridad
4.1 - Procedimiento de recolección de información relacionada con incidentes
4.2 - Técnicas de análisis de información y eventos de seguridad
4.3 - Herramientas de correlación de información y eventos
4.4 - Proceso de verificación de la intrusión
4.5 - Organismos de gestión de incidentes tipo CERT nacionales e internacionales: naturaleza y funciones
4.6 - Documentación y trazabilidad de las actuaciones de respuesta
Resumen del módulo 4
Módulo 5: Notificación y gestión de intentos de intrusión
5.1 - Responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
5.2 - Categorización de los incidentes y nivel de intervención según el impacto potencial
5.3 - Criterios para determinar las evidencias objetivas que sustentan la gestión del incidente
5.4 - Detección y registro de incidentes derivados de intentos de intrusión o infecciones

5.5 - Clasificación y análisis inicial del intento de intrusión o infección
5.6 - Investigación y diagnóstico del incidente
5.7 - Resolución y recuperación de los sistemas tras el incidente
5.8 - Comunicación del incidente a terceros, cuando proceda
5.9 - Cierre del incidente y registros para documentar su histórico
Resumen del módulo 5
Módulo 6: Análisis forense informático
6.1 - Conceptos generales y objetivos del análisis forense
6.2 - El Principio de Lockard y su aplicación práctica
6.3 - Recogida de evidencias electrónicas
6.4 - Estudio de ficheros y directorios ocultos e información oculta del sistema
6.5 - Recuperación de ficheros borrados
6.6 - Selección de herramientas de análisis forense
Resumen del módulo 6