Gestión de la seguridad informática en la empresa

Formación **online** • 100 horas de duración

4 créditos ECTS

femxa

CENTRO COLABORADOR | UNIVERSIDAD NEBRIJA

CARACTERÍSTICAS

Objetivo principal del curso

Con este curso online de Gestión de la seguridad informática en la empresa, aprenderás las herramientas necesarias para proteger tu negocio de las amenazas de la red.

100 horas • 4 créditos ECTS

Válidos en concursos-oposición, traslados, bolsas de contratación, oposiciones y plazas interinas.

Doble titulación:

- Diploma de Aprovechamiento de Femxa.
- Título certificado por la Universidad Nebrija*.

Formación de calidad:

Metodología 100% online y tutor especializado.

COMPROMISO FEMXA
Riesgo Cero

Formación online (bonificable hasta el 100%)

* Enseñanzas que no conducen a la obtención de un título con valor oficial.

TEMARIO

x x x x x

¿Qué **aprenderás** con nosotros?

1 INTRODUCCIÓN A LA SEGURIDAD.

- Introducción a la seguridad de información.
- Modelo de ciclo de vida de la seguridad de la información.
- Confidencialidad, integridad y disponibilidad. Principios de protección de la seguridad de la información.
- Políticas de seguridad.
- Tácticas de ataque.
- Concepto de hacking.
- Árbol de ataque.
- Lista de amenazas para la seguridad de la información.
- Vulnerabilidades.
- Vulnerabilidades en sistemas Windows.
- Vulnerabilidades en aplicaciones multiplataforma.
- Vulnerabilidades en sistemas Unix y Mac OS.
- Buenas prácticas y salvaguardas para la seguridad de la red.
- Recomendaciones para la seguridad de su red.

2 POLÍTICAS DE SEGURIDAD.

- Introducción a las políticas de seguridad.
- ¿Por qué son importantes las políticas?
- Qué debe de contener una política de seguridad.
- Lo que no debe contener una política de seguridad.
- Cómo conformar una política de seguridad informática.
- Hacer que se cumplan las decisiones sobre estrategia y políticas.

3 AUDITORÍA Y NORMATIVA DE SEGURIDAD.

- Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información.
- Ciclo del sistema de gestión de seguridad de la información.
- Seguridad de la información.
- Definiciones y clasificación de los activos.
- Seguridad humana, seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Gestión de continuidad del negocio.
- Conformidad y legalidad.

4 ESTRATEGIAS DE SEGURIDAD.

- Menor privilegio.
- Defensa en profundidad.
- Punto de choque.
- El eslabón más débil.
- Postura de fallo seguro.
- Postura de negación establecida: lo que no está prohibido.
- Postura de permiso establecido: lo que no está permitido.
- Participación universal.
- Diversificación de la defensa.
- Simplicidad.

5 EXPLORACIÓN DE LAS REDES.

- Exploración de la red.
- Inventario de una red. Herramientas del reconocimiento.
- NMAP Y SCANLINE.
- Reconocimiento. Limitar y explorar.
- Reconocimiento. Exploración.
- Reconocimiento. Enumerar.

6 ATAQUES REMOTOS Y LOCALES.

- Clasificación de los ataques.
- Ataques remotos en UNIX.
- Ataques remotos sobre servicios inseguros en UNIX.
- Ataques locales en UNIX.
- ¿Qué hacer si recibimos un ataque?

7 SEGURIDAD EN REDES ILANÁMBRICAS.

- Introducción.
- Introducción al estándar inalámbrico 802.11 – WIFI.
- Topologías.
- Seguridad en redes Wireless. Redes abiertas.
- WEP.
- WEP. Ataques.
- Otros mecanismos de cifrado.

8 CRIPTOGRAFÍA Y CRIPTOANÁLISIS.

- Criptografía y criptoanálisis: introducción y definición.
- Cifrado y descifrado.
- Ejemplo de cifrado: relleno de una sola vez y criptografía clásica.
- Ejemplo de cifrado: criptografía moderna.
- Comentarios sobre claves públicas y privadas: sesiones.

9 AUTENTICACIÓN.

- Validación de identificación en redes.
- Validación de identificación en redes: métodos de autenticación.
- Validación de identificación basada en clave secreta compartida: protocolo.
- Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman.
- Validación de identificación usando un centro de distribución de claves.
- Protocolo de autenticación Kerberos.
- Validación de identificación de clave pública.
- Validación de identificación de clave pública: protocolo de interbloqueo.

METODOLOGÍA

100% ONLINE. FLEXIBILIDAD

Nuestra **metodología online** está pensada para que tú, como alumno, adquieras un nivel de conocimiento adecuado a tu ocupación profesional. Te ofrecemos un nivel alto de interactividad que sirve de refuerzo al aprendizaje y a la asimilación de la información.

Una vez confirmado el pago, formalizaremos tu matrícula en el curso y, el día del inicio (miércoles o viernes), recibirás un correo electrónico con tus claves de acceso al **Campus Virtual.**

Además, el ritmo y el itinerario didáctico del curso están diseñados para ser conciliados con tus responsabilidades personales y laborales. ¡Tú organizas tu tiempo!

¿Qué te vas a encontrar?

Una vez dentro del Campus, podrás descargar y estudiar el material didáctico, ver videotutoriales explicativos, participar en foros de debate, plantear tus dudas a tu tutor personal, leer documentación complementaria, realizar las actividades o interactuar con otros alumnos.

Fácil de utilizar: no se necesitan conocimientos específicos de informática para realizar el curso. Nuestra plataforma online te guiará paso a paso en todo el proceso de formación.

Tutor personal: resuelve todas tus dudas en directo en horario de tutorías o consulta con tu tutor personal a través de email.

Desde cualquier dispositivo: sin desplazamientos. Estés donde estés, con tus claves de acceso podrás hacer el curso desde cualquier ordenador.

Vídeos y herramientas multimedia: foros, chats, casos prácticos y múltiples vídeos que harán que tu aprendizaje sea mucho más ameno.

Disponible las 24 horas: se puede acceder al curso en cualquier momento del día.

Contenido descargable: el contenido del curso y todo el material complementario está disponible para su descarga.

Soporte técnico: Contarás con el apoyo de un equipo de soporte informático para cualquier necesidad que te pueda surgir.

Tutorías telefónicas: podrás contactar con tu tutor telefónicamente.

femxa

CENTRO COLABORADOR | UNIVERSIDAD NEBRIJA

Tel. 900 100 957 | hola@cursosfemxa.es | **www.cursosfemxa.es**