Código: 13340

Unidad Formativa:
MF0487_3 - Auditoría de seguridad informática

Módulo: MF0487_3 - AUDITORÍA DE SEGURIDAD INFORMÁTICA

Certificado de Profesionalidad:
IFCT0109 - SEGURIDAD INFORMÁTICA

Modalidad: DISTANCIA

Duración: 90h.

Metodología

El Curso está desarrollado con una metodología Online. Este sistema de enseñanza e-learning está organizado de tal forma, que el alumno pueda compatibilizar el estudio con sus ocupaciones laborales o profesionales. Esta modalidad 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. También podrá acceder a la *Guía didáctica del alumno* dónde 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 puesta a disposición del alumno 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:

C/ de Ríos Rosas 42, planta 1ª 28003 Madrid
Tlf: 91 1097505
www.aulaforma.es

CERTIFICADO DE PARTICIPACIÓN Y APROVECHAMIENTO

D./Dña. **XXXXX XXXXX XXXXX** con D.N.I. **11111111H** , ha realizado, con pleno aprovechamiento, el curso titulado **Almacenamiento de la información e introducción a los SGBD** , que forma parte del certificado ADMINISTRACIÓN DE BASES DE DATOS, con Código **13643**, entre los días **15/07/2020** y **15/10/2020**, con una duración total de **50** horas, en la modalidad formativa **ONLINE**

Contenidos impartidos (Ver Dorso)

Firma y sello de la entidad responsable de impartir la formación

Telf.: 91 1097505
www.aulaforma.es

Fecha de expedición
15 OCT 2020

Firma del alumno

ISO 9001
BUREAU VERITAS Certification

Requistos previos

Estar en posesión de uno de los siguientes títulos:
Título de Bachillerato.
Certificado de profesionalidad del mismo nivel.
Prueba de Acceso a Ciclo Formativo de Grado Superior.
Certificado de profesionalidad de nivel 2 de la misma familia profesional.
Prueba de Acceso a la Universidad (PAU) para mayores de 25 y/o 45 años.

Salidas profesionales

Un certificado de profesionalidad, es un documento que acredita a un trabajador/a en una cualificación profesional del *Catálogo Nacional de las Cualificaciones Profesionales*. Son emitidos por el Servicio Público de Empleo Estatal o, en su caso, por las Comunidades Autónomas, y tienen validez en todo el territorio nacional.

Poseer un certificado de profesionalidad, supone sin lugar a dudas incrementar sustancialmente tu currículum profesional, ya que al ser un documento oficial, se valora en cualquier proceso de selección que convoquen las Administraciones Públicas, y te acredita profesionalmente ante la empresa privada.

Nosotros te formaremos para que puedas optar a conseguir el certificado de profesionalidad elegido, participando en las pruebas que convoque la Administración al amparo del R.D. 1224/2009 de 17 de julio y pudiendo además, convalidar módulos formativos para la obtención de un título de Formación Profesional.

Objetivos

Analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático implantando aquellas que se adecuen a las especificaciones de seguridad informática.
Aplicar procedimientos relativos al cumplimiento de la normativa legal vigente.
Planificar y aplicar medidas de seguridad para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental.
Describir los términos asociados al análisis de riesgos, estableciendo la relación consistente entre ellos.

Contenidos

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

Aplicación de la normativa de protección de datos de carácter personal
Principios generales de protección de datos de carácter personal.
Normativa europea recogida en la Directiva 95/46/CE.
Normativa nacional recogida en el Código penal, la Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), la Ley Orgánica de Protección de Datos (LOPD) y el Reglamento de desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007).
Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización.
Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007.
Guía para la realización de la auditoría bienal obligatoria de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

Análisis de los riesgos de los sistemas de información
Introducción al análisis de riesgos.
Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura.
Particularidades de los distintos tipos de código malicioso.
Principales elementos del análisis de riesgos y sus modelos de relaciones.
Metodologías cualitativas y cuantitativas de análisis de riesgos.
Identificación de los activos involucrados en el análisis de riesgos y su valoración.
Identificación de las amenazas que pueden afectar a los activos identificados previamente.
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.
Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría.
Identificación de las medidas de salvaguarda existentes en el momento de la realización

del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas.
Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse.
Determinación de la probabilidad e impacto de materialización de los escenarios.
Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza.
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.
Relación de las distintas alternativas de gestión de riesgos.
Guía para la elaboración del plan de gestión de riesgos.
Exposición de la metodología NIST SP 800-30.
Exposición de la metodología Magerit versión 2.

Uso de herramientas para la auditoría de sistemas
Herramientas del sistema operativo tipo ping, traceroute, etc.
Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
Herramientas de análisis de vulnerabilidades tipo Nessus.
Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.
Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

Descripción de los aspectos sobre cortafuegos en auditorías de sistemas informáticos
Principios generales de cortafuegos.
Componentes de un cortafuegos de red.
Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad.
Arquitecturas de cortafuegos de red.
Otras arquitecturas de cortafuegos de red.

Guías para la ejecución de las distintas fases de la auditoría de sistemas de información
Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada.
Guía para la elaboración del plan de auditoría.
Guía para las pruebas de auditoría.
Guía para la elaboración del informe de auditoría.