

**Código:** 15031
**Unidad Formativa:**
MF0487_3 - Auditoría de seguridad informática
**Módulo:** MF0487_3 - AUDITORÍA 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**

securs@
CONSULTORÍA DE FORMACIÓN
Avda. Ramón Nieto nº 133, Bajo
36208 - VIGO
Telf.: 986912815

**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, ejecutar y documentar auditorías de seguridad informática con criterios profesionales, tanto en organizaciones públicas como privadas. Está orientado a personal técnico, responsables de sistemas y profesionales que necesitan verificar el cumplimiento normativo y la eficacia de las medidas de protección. A lo largo del recorrido se integran la deontología y las metodologías de auditoría, el marco de protección de datos personales, el análisis de riesgos y el manejo de herramientas de diagnóstico, análisis de red y evaluación de vulnerabilidades, prestando especial atención a la interpretación de hallazgos y a la revisión de cortafuegos. Al finalizar, el alumnado será capaz de diseñar un plan de auditoría, aplicar pruebas sustantivas y de cumplimiento, valorar los riesgos detectados y elaborar informes con recomendaciones útiles para mejorar la seguridad de los sistemas de información.

## Contenidos

Módulo 1: Criterios generales de la auditoría de sistemas de información
1.1 - Código deontológico y principios éticos de la función auditora
1.2 - Tipos de auditoría en el ámbito de los sistemas de información
1.3 - Composición y competencias del equipo auditor
1.4 - Pruebas sustantivas y pruebas de cumplimiento
1.5 - Técnicas de muestreo aplicadas al proceso de auditoría
1.6 - Herramientas CAAT de auditoría asistida por ordenador
1.7 - Requisitos de los hallazgos y su categorización como observaciones o no conformidades
1.8 - Normativas y metodologías de referencia en auditoría de sistemas
Resumen del módulo 1
Módulo 2: Aplicación de la normativa de protección de datos de carácter personal
2.1 - Principios generales de la protección de datos personales
2.2 - El marco europeo de protección de datos y la Directiva 95/46/CE
2.3 - Normativa nacional: Código Penal, LORTAD, LOPD y Reglamento de desarrollo
2.4 - Identificación y registro de ficheros con datos de carácter personal
2.5 - Medidas de seguridad recogidas en el Real Decreto 1720/2007
2.6 - Guía para la auditoría bienal obligatoria de la Ley Orgánica 15/1999
Resumen del módulo 2
Módulo 3: Análisis de riesgos en los sistemas de información
3.1 - Fundamentos y elementos del análisis de riesgos
3.2 - Vulnerabilidades, fallos de programa, código malicioso y programación segura
3.3 - Metodologías cualitativas y cuantitativas de análisis de riesgos
3.4 - Identificación y valoración de activos y amenazas
3.5 - Análisis de vulnerabilidades y contraste: local, caja blanca, caja negra e informe
3.6 - Salvaguardas y su efecto sobre vulnerabilidades y amenazas
3.7 - Escenarios de riesgo, probabilidad e impacto
3.8 - Nivel de riesgo y criterios de evaluación
3.9 - Alternativas y plan de gestión de riesgos: NIST SP 800-30 y Magerit versión 2
Resumen del módulo 3
Módulo 4: Uso de herramientas para la auditoría de sistemas
4.1 - Utilidades del sistema operativo: Ping, Traceroute y diagnóstico de red
4.2 - Análisis de red, puertos y servicios: Nmap, Netcat y NBTScan
4.3 - Escáneres de vulnerabilidades: Nessus
4.4 - Analizadores de protocolos: Wireshark, DSniff y Cain & Abel
4.5 - Análisis de aplicaciones web: Acunetix, Dirb y Paros Proxy
4.6 - Ataques de diccionario y fuerza bruta: Brutus y John the Ripper
Resumen del módulo 4
Módulo 5: Cortafuegos en las auditorías de sistemas informáticos
5.1 - Principios generales de los cortafuegos
5.2 - Componentes de un cortafuegos de red
5.3 - Tipos de cortafuegos según ubicación y funcionalidad
5.4 - Arquitecturas de cortafuegos de red

5.5 - Otras arquitecturas y modelos de despliegue
5.6 - Revisión de reglas y configuración en el contexto de la auditoría
Resumen del módulo 5
Módulo 6: Ejecución de las fases de la auditoría de sistemas de información
6.1 - Auditoría de la documentación y la normativa de seguridad de la organización
6.2 - Elaboración del plan de auditoría
6.3 - Diseño y ejecución de las pruebas de auditoría
6.4 - Elaboración del informe de auditoría
6.5 - Presentación de resultados y comunicación de hallazgos
6.6 - Seguimiento de las recomendaciones y cierre de la auditoría
Resumen del módulo 6