

Código: 15030

Unidad Formativa:
MF0486_3 - Seguridad en equipos informáticos

Módulo: MF0486_3 - SEGURIDAD EN EQUIPOS INFORMÁTICOS

Certificado de Profesionalidad:
IFCT0109 - SEGURIDAD INFORMÁTICAIFCT0510 - GESTIÓN DE SISTEMAS INFORMÁTICOS

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 proteger los sistemas de información de una organización, identificando las amenazas y los riesgos que afectan a la confidencialidad, la integridad y la disponibilidad de los datos. A lo largo del recorrido se aborda el análisis de impacto en el negocio, la gestión de riesgos y la definición de un plan de implantación de salvaguardas, junto con la protección de datos de carácter personal, la seguridad física de las instalaciones y el control lógico de accesos a los sistemas. La parte práctica ocupa un lugar central, con la identificación de servicios y puertos, el robustecimiento de equipos y la configuración de cortafuegos para reducir la exposición de la organización. Al finalizar, el alumnado será capaz de evaluar el nivel de seguridad de los sistemas, seleccionar y aplicar las medidas de protección adecuadas y elaborar la documentación que sostiene la seguridad de los equipos informáticos.

Contenidos

Módulo 1: Criterios generales de seguridad de los equipos informáticos
1.1 - La seguridad orientada a la gestión del riesgo en el uso de los sistemas de información
1.2 - Amenazas habituales, riesgos asociados y primeras medidas de salvaguarda
1.3 - Salvaguardas y tecnologías de seguridad de uso más extendido
1.4 - La gestión de la seguridad como complemento de las medidas tecnológicas
1.5 - Activos de información y criterios para su protección
1.6 - Cultura de seguridad y responsabilidad de los usuarios
Resumen del módulo 1
Módulo 2: Análisis de impacto de negocio
2.1 - Identificación de los procesos de negocio apoyados en sistemas de información
2.2 - Valoración de la confidencialidad, la integridad y la disponibilidad en los procesos
2.3 - Sistemas de información que dan soporte a cada proceso de negocio
2.4 - Requerimientos de seguridad derivados de los procesos críticos
2.5 - Análisis de dependencias entre procesos y sistemas
2.6 - Documentación y revisión del análisis de impacto en el negocio
Resumen del módulo 2
Módulo 3: Gestión de riesgos
3.1 - El proceso de gestión de riesgos y sus alternativas de aplicación
3.2 - Metodologías habituales para identificar y analizar los riesgos
3.3 - Valoración del impacto y de la probabilidad de las amenazas
3.4 - Controles y medidas de salvaguarda para reducir el riesgo
3.5 - Tratamiento, aceptación y seguimiento del riesgo residual
3.6 - Registro y comunicación de los resultados del análisis
Resumen del módulo 3
Módulo 4: Plan de implantación de seguridad
4.1 - Diagnóstico del nivel de seguridad existente frente al requerido
4.2 - Selección de salvaguardas según los requerimientos de los sistemas
4.3 - Guía para elaborar el plan de implantación de las salvaguardas
4.4 - Priorización de actuaciones y planificación de recursos
4.5 - Seguimiento, indicadores y revisión del plan
4.6 - Comunicación del plan y coordinación con las áreas implicadas
Resumen del módulo 4
Módulo 5: Protección de datos de carácter personal
5.1 - Principios generales de la protección de datos personales
5.2 - Infracciones y sanciones previstas en la normativa de protección de datos
5.3 - Identificación y registro de los ficheros con datos personales
5.4 - Elaboración del documento de seguridad exigido por la normativa
5.5 - Responsabilidades del personal que trata datos personales
5.6 - Revisiones y actualización de la documentación de seguridad
Resumen del módulo 5
Módulo 6: Seguridad física e industrial de los sistemas
6.1 - Delimitación de los perímetros de seguridad física

6.2 - Sistemas de control de acceso físico a instalaciones y áreas críticas
6.3 - Criterios para la ubicación física de los equipos informáticos
6.4 - Protección y continuidad del suministro eléctrico
6.5 - Climatización y protección contra incendios en las salas de sistemas
6.6 - Elaboración de la normativa de seguridad física e industrial
Resumen del módulo 6
Módulo 7: Seguridad lógica y control de accesos a los sistemas
7.1 - Sistemas de ficheros de uso más frecuente y su configuración segura
7.2 - Control de acceso de los equipos a la red de comunicaciones
7.3 - Políticas y directivas del directorio de usuarios
7.4 - Listas de control de acceso (ACL) a ficheros
7.5 - Gestión de altas, bajas, modificaciones y privilegios de usuarios
7.6 - Control de acceso de los usuarios al sistema operativo
7.7 - Autenticación de usuarios: métodos débiles, fuertes y biométricos
7.8 - Registros de auditoría para supervisar el control de accesos
7.9 - Elaboración de la normativa de control de accesos
Resumen del módulo 7
Módulo 8: Identificación de servicios
8.1 - Protocolos, servicios y puertos empleados por los sistemas de información
8.2 - Herramientas de análisis de puertos y servicios abiertos
8.3 - Detección de servicios innecesarios y valoración de su riesgo
8.4 - Análisis del tráfico de comunicaciones
8.5 - Uso real de protocolos, servicios y puertos en la organización
8.6 - Documentación de los resultados y medidas derivadas
Resumen del módulo 8
Módulo 9: Robustecimiento de sistemas
9.1 - Cambio de usuarios y contraseñas por defecto
9.2 - Directivas de gestión de contraseñas y privilegios en el directorio de usuarios
9.3 - Eliminación y cierre de herramientas, utilidades, servicios y puertos prescindibles
9.4 - Configuración de protocolos seguros en los sistemas de información
9.5 - Actualización y aplicación de parches de seguridad
9.6 - Protección frente a código malicioso
9.7 - Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos
9.8 - Monitorización de la seguridad y del uso adecuado de los sistemas
Resumen del módulo 9
Módulo 10: Implantación y configuración de cortafuegos
10.1 - Tipos de cortafuegos según su ubicación y funcionalidad
10.2 - Segregación de redes y zonas desmilitarizadas (DMZ)
10.3 - Redes privadas virtuales (VPN) para canales seguros de comunicación
10.4 - Definición de reglas de corte en el cortafuegos
10.5 - Registros de auditoría del cortafuegos y eventos de seguridad
10.6 - Monitorización y pruebas del cortafuegos
Resumen del módulo 10