



**LA FORMACIÓN ES LA CLAVE
DEL ÉXITO**

Guía del Curso

IFCT0510 Gestión de Sistemas Informáticos

Modalidad de realización del curso: [A distancia y Online](#)

Titulación: [Diploma acreditativo con las horas del curso](#)

OBJETIVOS

Este curso se ajusta al itinerario formativo del Certificado de Profesionalidad IFCT0510 Gestión de Sistemas Informáticos, certificando el haber superado las distintas Unidades de Competencia en él incluidas, y va dirigido a la acreditación de las Competencias profesionales adquiridas a través de la experiencia laboral y de la formación no formal que permitirá al alumnado adquirir las habilidades profesionales necesarias para la administración hardware y software de un sistema informático y la seguridad en equipos informáticos.

CONTENIDOS

MÓDULO 1. MF0484_3 ADMINISTRACIÓN HARDWARE DE UN SISTEMA INFORMÁTICO

UNIDAD FORMATIVA 1. UF1891 DIMENSIONAR, INSTALAR Y OPTIMIZAR EL HARDWARE

UNIDAD DIDÁCTICA 1. CLASIFICAR E INVENTARIAR EL HARDWARE

1. Identificar y clasificar el hardware

2. Establecer la conectividad del hardware
3. Documentar e inventariar el hardware
4. Mantener el inventario

UNIDAD DIDÁCTICA 2. MONITORIZAR EL RENDIMIENTO

1. Diseñar la monitorización
2. Monitorizar el sistema
3. Diagnosticar el estado del sistema
4. Optimizar la parametrización para implementar un mejor rendimiento

UNIDAD DIDÁCTICA 3. DISEÑAR E IMPLEMENTAR ARQUITECTURAS TOLERANTES A FALLOS

1. Instalar los elementos hardware del sistema atendiendo a las especificaciones del fabricante y a las normas de la organización
2. Verificar el correcto funcionamiento del sistema tras su instalación
3. Diseñar los puntos de tolerancia a fallos del sistema
4. Conocer los procedimientos de respaldo y de recuperación de fallos definidos en la empresa
5. Conocer arquitecturas que permiten mayor tolerancia a fallos

UNIDAD DIDÁCTICA 4. DIAGNOSTICAR Y RESOLVER LAS AVERÍAS

1. Consultar la documentación del fabricante y la documentación interna de la organización, así como al servicio de asistencia técnica del fabricante, o de terceros con los que la organización tenga contrato de mantenimiento, en busca del origen y resolución de incidentes
2. Utilizar las herramientas de diagnóstico y documentación facilitadas por el fabricante
3. Planificar y ejecutar la reparación acorde a la documentación del fabricante y a los procedimientos internos
4. Planificar y ejecutar la reparación garantizando la integridad de la información, y

minimizando el impacto sobre la disponibilidad de servicio

5. Conocer e interpretar adecuadamente los planes de recuperación de servicio existentes en la empresa

UNIDAD FORMATIVA 2. UF1892 GESTIONAR EL CRECIMIENTO Y LAS CONDICIONES AMBIENTALES

UNIDAD DIDÁCTICA 1. GESTIONAR EL CRECIMIENTO

1. Planificar las ampliaciones. Dimensionar los crecimientos futuros
2. Analizar el mercado en busca de las soluciones hardware que ofrece
3. Localizar a los prescriptores de mercado

UNIDAD DIDÁCTICA 2. ESTABLECER LAS CONDICIONES AMBIENTALES ADECUADAS

1. Conocer los factores ambientales que pueden afectar al funcionamiento de la instalación
2. Interpretar adecuadamente las necesidades ambientales del hardware
3. Comprobar la calidad del suministro industrial
4. Diseñar la ubicación de los equipos en la sala

MÓDULO 2. MF0485_3 ADMINISTRACIÓN SOFTWARE DE UN SISTEMA INFORMÁTICO

UNIDAD FORMATIVA 1. UF1893 INSTALACIÓN Y PARAMETRIZACIÓN DEL SOFTWARE

UNIDAD DIDÁCTICA 1. SOFTWARE

1. Conocer y comprender qué es el software, y para qué sirve
2. Distinguir software, de firmware, y de hardware
3. Identificar los diferentes tipos de software

UNIDAD DIDÁCTICA 2. SISTEMAS OPERATIVOS

1. Comprender la definición y utilidad de los sistemas operativos
2. Identificar los distintos tipos de sistemas operativos, describiendo sus funciones y estructura
3. Clasificar los sistemas operativos
4. Conocer las políticas definidas en la organización, de aplicación en la instalación del sistema operativo
5. Instalar y parametrizar los sistemas operativos
6. Conocer y utilizar adecuadamente las herramientas de gestión del sistema operativo, de uso habitual
7. Securizar el sistema atendiendo a las normas definidas
8. Documentar la instalación

UNIDAD DIDÁCTICA 3. SOFTWARE DE APLICACIÓN

1. Distinguir entre los distintos tipos de software de aplicación atendiendo a su uso
2. Conocer las políticas definidas en la organización, de aplicación en la elección e instalación del software de aplicación
3. Instalar el software de aplicación, atendiendo a las recomendaciones del fabricante, y a las normas de seguridad de la organización
4. Comprobar el correcto funcionamiento del software de aplicación
5. Desplegar masiva y desatendidamente software de aplicación

UNIDAD DIDÁCTICA 4. AUTOMATIZACIONES

1. Conocer los diferentes lenguajes de programación de uso habitual para la

automatización de tareas

2. Utilizar un editor adecuado para el desarrollo del código
3. Desarrollar pequeños scripts para la ejecución de tareas de mantenimiento
4. Seleccionar el lenguaje de programación más adecuado en función de los requisitos de la tarea a automatizar y del sistema operativo sobre el que se deba ejecutar
5. Configurar la ejecución automática de la tarea en el sistema operativo
6. Utilizar herramientas de automatización

UNIDAD DIDÁCTICA 5. INVENTARIO DE SW

1. Identificar los motivos de la necesidad de inventariar
2. Seleccionar adecuadamente los parámetros a inventariar en un sistema
3. Gestionar las licencias
4. Gestionar herramientas de inventariado
5. Inventariar la configuración base y de aplicación
6. Actualizar la lista de aplicaciones permitidas por usuario

UNIDAD FORMATIVA 2. UF1894 MANTENIMIENTO DEL SOFTWARE

UNIDAD DIDÁCTICA 1. PLANES DE MANTENIMIENTO

1. Conocer la utilidad y funciones de los planes de mantenimiento
2. Diseñar, desarrollar y documentar el plan de mantenimiento
3. Gestionar los problemas frecuentes
4. Utilizar el conocimiento adquirido con la experiencia
5. Atender al usuario
6. Actualizar el sistema, manteniéndolo al día en las versiones adecuadas a las funcionalidades requeridas por las necesidades, y a los requisitos de seguridad del sistema

UNIDAD DIDÁCTICA 2. OPTIMIZACIÓN DEL USO DE LOS RECURSOS

1. Comprobar la adecuación del rendimiento del sistema a las necesidades de la organización
2. Utilizar las herramientas de modelado para predecir el rendimiento del sistema en base a las previsiones de incremento de carga del sistema
3. Realizar pruebas de carga para comprobar la escalabilidad del sistema y su adecuación a las necesidades presentes y futuras de la organización

UNIDAD FORMATIVA 3. UF1895 AUDITORÍAS Y CONTINUIDAD DE NEGOCIO

UNIDAD DIDÁCTICA 1. COPIAS DE RESPALDO

1. Tipificar los datos según sus necesidades de copia
2. Diferenciar los distintos tipos de copias, distinguiendo las diferencias entre copias completas, incrementales, y diferenciales, así como las ventajas e inconvenientes de cada una de ellas, y las combinaciones más habituales de las mismas
3. Establecer correctamente los periodos de retención acordes con las normas de seguridad de la empresa, con las necesidades según el tipo de datos, y con la legislación vigente
4. Dimensionar las copias de seguridad
5. Establecer la política de copias de la organización
6. Proponer los dispositivos de copia y soportes más adecuados en base a las necesidades de la organización
7. Realizar las copias de seguridad según los procedimientos y políticas vigentes en la organización
8. Gestionar el ciclo de vida de los soportes
9. Documentación de planes de recuperación

UNIDAD DIDÁCTICA 2. LEGISLACIÓN VIGENTE

1. Conocer las Leyes vigentes relacionadas con el tratamiento de datos

2. Enumerar los puntos principales a tener en cuenta

UNIDAD DIDÁCTICA 3. ALTERNATIVAS A LAS COPIAS

1. Distinguir entre salvaguarda de datos, y disponibilidad del servicio
2. Enumerar las alternativas para garantizar la disponibilidad del servicio
3. Indicar ventajas e inconvenientes de las alternativas para garantizar la disponibilidad del servicio sobre las copias de seguridad

UNIDAD DIDÁCTICA 4. PLANES DE AUDITORÍA

1. Describir los objetivos de los planes de auditoría
2. Describir el perfil del auditor
3. Auditar el sistema

MÓDULO 3. MF0486_3 SEGURIDAD EN EQUIPOS INFORMÁTICOS

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
2. Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
3. Salvaguardas y tecnologías de seguridad más habituales
4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO

1. Identificación de procesos de negocio soportados por sistemas de información

2. Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
3. Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS

1. Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
2. Metodologías comúnmente aceptadas de identificación y análisis de riesgos
3. Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD

1. Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.
2. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
3. Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Principios generales de protección de datos de carácter personal
2. Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
3. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
4. Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

UNIDAD DIDÁCTICA 6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS

SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

1. Determinación de los perímetros de seguridad física
2. Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
3. Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
4. Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
5. Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
6. Elaboración de la normativa de seguridad física e industrial para la organización
7. Sistemas de ficheros más frecuentemente utilizados
8. Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
9. Configuración de políticas y directivas del directorio de usuarios
10. Establecimiento de las listas de control de acceso (ACLs) a ficheros
11. Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
12. Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
13. Sistemas de autenticación de usuarios débiles, fuertes y biométricos
14. Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
15. Elaboración de la normativa de control de accesos a los sistemas informáticos

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS

1. Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
2. Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
3. Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y

puertos

UNIDAD DIDÁCTICA 8. ROBUSTECIMIENTO DE SISTEMAS

1. Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información
2. Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
3. Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
4. Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
5. Actualización de parches de seguridad de los sistemas informáticos
6. Protección de los sistemas de información frente a código malicioso
7. Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
8. Monitorización de la seguridad y el uso adecuado de los sistemas de información

UNIDAD DIDÁCTICA 9. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

1. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
2. Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
3. Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
4. Definición de reglas de corte en los cortafuegos
5. Relación de los registros de auditoría del cortafuegos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6. Establecimiento de la monitorización y pruebas del cortafuegos



C/ San Lorenzo 2 - 2
29001 Málaga



Tlf: 952 215 476
Fax: 951 987 941



www.academiaintegral.com.es
E-mail: info@academiaintegral.com.es