



INESEM

BUSINESS SCHOOL

Gestión de Sistemas Informáticos (Online)

+ Información Gratis

titulación de formación continua bonificada expedida por el instituto europeo de estudios empresariales

Gestión de Sistemas Informáticos (Online)

duración total: 500 horas

horas teleformación: 250 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

En la actualidad, en el mundo de la informática y las comunicaciones y dentro del área profesional de sistemas y telemática, más concretamente en la gestión de sistemas informáticos, es muy importante conocer los diferentes procesos por cual se realizan. Por ello, con el presente curso se trata de aportar los conocimientos necesarios para dimensionar, instalar y optimizar el hardware y gestionar el crecimiento y las condiciones ambientales.



a quién va dirigido

Todos aquellos trabajadores y profesionales en activo que deseen adquirir o perfeccionar sus conocimientos técnicos en este área.

objetivos

- Administrar los dispositivos hardware del sistema
- Instalar, configurar y administrar el software de base y de aplicación del sistema
- Asegurar equipos informáticos

para qué te prepara

La presente formación 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, vía por la que va a optar a la obtención del correspondiente Certificado de Profesionalidad, a través de las respectivas convocatorias que vayan publicando las distintas Comunidades Autónomas, así como el propio Ministerio de Trabajo (Real Decreto 659/2023, de 18 de julio, que desarrolla la ordenación del Sistema de Formación Profesional y establece un procedimiento permanente para la acreditación de competencias profesionales adquiridas por experiencia laboral o formación no formal).

salidas laborales

Desarrolla su actividad profesional en empresas o entidades de naturaleza pública o privada de cualquier tamaño en el área de sistemas del departamento de informática.

titulación

Una vez finalizado el curso, el alumno recibirá por parte de INESEM vía correo postal, la Titulación Oficial que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/máster, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Instituto Europeo de Estudios Empresariales).

**INSTITUTO EUROPEO DE ESTUDIOS EMPRESARIALES**

como centro de Formación acreditado para la impartición a nivel nacional de formación
EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXX ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación INESEM en la convocatoria de XXXX
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX- XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en
Granada, a (día) de (mes) de (año)

La dirección General

MARIA MORENO HIDALGO

Firma del alumno/a

Sello



NOMBRE DEL ALUMNO/A

**forma de bonificación**

- Mediante descuento directo en el TC1, a cargo de los seguros sociales que la empresa paga cada mes a la Seguridad Social.

metodología

El alumno comienza su andadura en INESEM a través del Campus Virtual. Con nuestra metodología de aprendizaje online, el alumno debe avanzar a lo largo de las unidades didácticas del itinerario formativo, así como realizar las actividades y autoevaluaciones correspondientes. Al final del itinerario, el alumno se encontrará con el examen final, debiendo contestar correctamente un mínimo del 75% de las cuestiones planteadas para poder obtener el título.

Nuestro equipo docente y un tutor especializado harán un seguimiento exhaustivo, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

El alumno dispone de un espacio donde gestionar todos sus trámites administrativos, la Secretaría Virtual, y de un lugar de encuentro, Comunidad INESEM, donde fomentar su proceso de aprendizaje que enriquecerá su desarrollo profesional.

materiales didácticos

- Manual teórico 'MF0486_3 Seguridad en Equipos Informáticos'
- Manual teórico 'UF1893 Instalación y Parametrización del Software'
- Manual teórico 'UF1894 Mantenimiento del Software'
- Manual teórico 'UF1895 Auditorías y Continuidad de Negocio'
- Manual teórico 'UF1891 Dimensionar, Instalar y Optimizar el Hardware'
- Manual teórico 'UF1892 Gestionar el Crecimiento y las Condiciones Ambientales'



profesorado y servicio de tutorías

Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “Guía del Alumno” entregado junto al resto de materiales de estudio. Contamos con una extensa plantilla de profesores especializados en las distintas áreas formativas, con una amplia experiencia en el ámbito docente.

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas, así como solicitar información complementaria, fuentes bibliográficas y asesoramiento profesional. Podrá hacerlo de las siguientes formas:

- **Por e-mail:** El alumno podrá enviar sus dudas y consultas a cualquier hora y obtendrá respuesta en un plazo máximo de 48 horas.
- **Por teléfono:** Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.
- **A través del Campus Virtual:** El alumno/a puede contactar y enviar sus consultas a través del mismo, pudiendo tener acceso a Secretaría, agilizando cualquier proceso administrativo así como disponer de toda su documentación



plazo de finalización

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la misma duración del curso. Existe por tanto un calendario formativo con una fecha de inicio y una fecha de fin.

campus virtual online

especialmente dirigido a los alumnos matriculados en cursos de modalidad online, el campus virtual de ineseem ofrece contenidos multimedia de alta calidad y ejercicios interactivos.

comunidad

servicio gratuito que permitirá al alumno formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: becas, descuentos y promociones en formación, viajes al extranjero para aprender idiomas...

revista digital

el alumno podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, etc.

secretaría

Este sistema comunica al alumno directamente con nuestros asistentes, agilizando todo el proceso de matriculación, envío de documentación y solución de cualquier incidencia.

Además, a través de nuestro gestor documental, el alumno puede disponer de todos sus documentos, controlar las fechas de envío, finalización de sus acciones formativas y todo lo relacionado con la parte administrativa de sus cursos, teniendo la posibilidad de realizar un seguimiento personal de todos sus trámites con INESEM

programa formativo**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. Securitizar 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 la 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 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