

Seguridad informática para PYMES

Código del curso: 21412IN

Horas: 20

Descripción del curso:

Acerca de este curso

Cod: 21412IN

Seguridad Informática

Introducción

Los dominios y las regulaciones asociadas

Riesgos informáticos

Política de seguridad

Ejes principales en las estrategias de seguridad

La seguridad y sus aspectos legales

Resumen

La seguridad en la empresa I

Introducción

Requisitos previos

Generalidades sobre seguridad en redes

Redes privadas virtuales

Componentes utilizados en redes y su seguridad

Sistemas de detección y prevención de intrusos

Servidor DNS

Resumen

Seguridad en la empresa II

Introducción

Objetivos

Disponibilidad de datos y sistemas

Disponibilidad de la infraestructura

Identificación y autenticación

Seguridad física y de entorno

Protección frente a virus y malware

Prácticas de seguridad

Resumen

Movilidad y Seguridad

Introducción

Seguridad en dispositivos móviles

Móvil y terminal itinerante

Terminales itinerantes: problemas asociados

Buenas prácticas

Resumen

Seguridad en los datos

Introducción

¿En qué consiste la seguridad de los datos?

Riesgo de pérdida de datos

Respaldo y restauración

Objetivo de las copias de seguridad

¿Qué datos es aconsejable copiar?

Restauración de datos

Estrategias de copias de seguridad

El archivo de datos

Administración y supervisión de copias de seguridad

Recuperación del servidor de respaldo

Resumen

Plan de contingencia informática

Introducción

Plan de contingencia informática

Preparación ante un desastre

Elaboración de un plan de recuperación ante desastres

Fase 1: Planificación

Fase 2: Identificación de riesgos

Fase 3: Identificación de soluciones

Virtualización de servidores

Resumen

Cloud Computing

Introducción

¿Qué es Cloud Computing?

Principios del Cloud Computing

Cloud Computing: riesgos

Buenas prácticas de seguridad
Resumen

Internet de los objetos
Introducción
¿Qué es internet de los objetos?
Tecnología
Sectores afectados por la seguridad
Nuevas amenazas y nuevos riesgos
Evaluación de riesgos
Propuestas de Seguridad
Resumen

Sensibilización a la seguridad en la empresa
Introducción
La importancia de la sensibilización
Comportamiento de los usuarios/trabajadores
Sensibilización de los usuarios/trabajadores
Principios éticos
Resumen

¿Qué aprenderás?

Identificar los principales aspectos de la seguridad informática, para planificar y aplicar las medidas necesarias al respecto.

Aplicar las medidas básicas para mantener la seguridad informática en la empresa, previa identificación de los riesgos existentes.

Aplicar prácticas y técnicas que ayuden a protegerse de las amenazas y contribuyan al cumplimiento de los objetivos de seguridad informática perseguidos por la empresa.

Identificar los problemas asociados a la seguridad en los dispositivos móviles y terminales itinerantes, aplicando prácticas que permitan evitarlos.

Realizar el proceso de creación de copias de seguridad de datos, así como de respaldo y recuperación de las mismas, administrándolas y supervisándolas adecuadamente.

Planificar la actuación de una empresa ante los riesgos más comunes en la seguridad informática, previendo las consecuencias que supondría para la empresa y las acciones necesarias para evitarlas.

Identificar los servicios asociados al Cloud Computing así como las buenas prácticas de seguridad en la nube.

Identificar las amenazas y riesgos presentes en el internet de los objetos, así como las prácticas a seguir para evitarlos y mantener la seguridad.

Aplicar acciones y procedimientos conducentes a la sensibilización de los usuarios sobre la seguridad en la empresa, transmitiendo en todo momento los valores de la empresa.