REVISION DE LA SEGURIDAD Y CONTROL DE LA INFORMACION ENLA EMPRESA

60 Horas

Objetivos:

- 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.

- 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.

- Adquirir los conocimientos necesarios para poder realizar una auditoría de protección de datos, así como conocer las distintas fases en las que se divide.

Contenidos:

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 autentificación
Seguridad física y de entorno
Protección frente a virus y malware
Prácticas 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

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

Auditoría según la Ley Orgánica 3/2018 y el Reglamento General de Protección de Datos
Auditoría
Objetivos de la Auditoría
Ámbitos de la Auditoría
Auditoría de cumplimiento

Auditoría de seguridad
Violación de la seguridad de los datos personales.
Comunicación de una violación de la seguridad de los datos personales al interesado
Fases de la Auditoría
Fase 1: planificación de la Auditoría
Fase 2: realización de la Auditoría
Listado de cumplimiento de la Ley Orgánica 3/2018 y el RGPD
Fase 3: informar de la Auditoría
Informe de Auditoría

1.