SEGURIDAD INFORMATICA PARA LA PYME

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.
- 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. sistemas de pago y la tributación aplicable al comercio electrónico nacional e internacional.

Contenidos:

MÓDULO 1: SEGURIDAD INFORMÁTICA PARA PYMES

Seguridad Informática
Introducción
Los dominios y las regulaciones asociadas
Riesgos informáticos
Política de seguridad
Ejes principales en las estrategias de seguridad

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

MÓDULO 2: CIBERSEGURIDAD EN LA MICROEMPRESA

Contextualización de la ciberseguridad en la microempresa
Introducción.
Activos de información:
    Seguridad de la información.
Conoce a tu enemigo y conócete a ti mismo.
    Identificación de los riesgos:
        Malware.
        Tipos de *malware.*
        Conocer al enemigo.
La cultura en ciberseguridad en los negocios.

Utilización de técnicas y recursos para el análisis de datos. Recopilación de evidencias:
- Uso seguro de las nuevas tecnologías en la empresa.
- Identificación de las principales medidas para prevenir amenazas.
- Seguridad en dispositivos móviles y redes wifi.
  - *Virtual Private Network* o VPN.
  - *Virtual Desktop Infrastructure* o VDI.
  - *Virtual Mobil Infraestructure* o VMI.
  - Aplicaciones de escritorio remoto.
- Relación segura con proveedores y clientes.
- Seguridad en la nube.

Resumen.

Política de ciberseguridad para microempresas
Introducción.
Desarrollo de una política de prevención de incidentes de seguridad en la microempresa:
- Prevención y protección:
  - Políticas de seguridad dirigidas al empresario.
  - Políticas de seguridad dirigidas al personal técnico.
  - Políticas de seguridad dirigidas a los empleados.

Incidentes de seguridad.
Resumen.