



Gestión de la ciberseguridad en PYMES. Comercio Electrónico Seguro

Duración: 60 horas

Modalidad: Online

Coste Bonificable: 420 €

Objetivos del curso

Este curso COMM03 Gestión de la ciberseguridad en PYMES. Comercio Electrónico Seguro ofrece una especialidad formativa de la Familia Profesional del Comercio y Marketing. Este curso COMM03 Gestión de la ciberseguridad en PYMES. Comercio Electrónico Seguro permite al alumno conocer todos aquellos aspectos en los que se basa la ciberseguridad y que pueden emplearse en PYMES para permitir aumentar la protección de nuestra seguridad e impedir ciberataques.

Contenidos

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA CIBERSEGURIDAD

1. Identificación de los conceptos básicos de ciberseguridad y su relación con la seguridad
 - Definición y alcance de la ciberseguridad
 - Áreas de actuación de la ciberseguridad
 - Ubicación de la ciberseguridad
 - Dimensiones de la seguridad y garantías que ofrece
 - Implementación de las dimensiones
 - Protección de la información
2. Relación entre las amenazas y las vulnerabilidades reconociendo sus efectos en los sistemas



- Ingeniería social
 - Vulnerabilidades en la autenticación
 - Malware y botnets
 - Seguridad en el perímetro de las redes
 - Riesgos de seguridad
 - Incidentes de seguridad
3. Identificación de los mecanismos de defensa a implementar en las redes privadas
- Defensa en profundidad y la DMZ
 - Antimalware
 - Contraseñas
 - Control de acceso
 - Controles para definir una red segura
 - Sistemas de detección de ataques
 - Recuperación de los sistemas ante un ciberataque
4. Utilidad de la correlación de eventos en la prevención e investigación de incidentes
- Eventos y tipos
 - Eventos de los sistemas de seguridad
 - Criticidad de los eventos
 - Tratamiento de los eventos para su automatización
 - Soluciones de automatización. El SIEM



5. Identificación de las medidas de seguridad en las redes inalámbricas y dispositivos móviles
 - La conexión inalámbrica y las redes
 - Configuración de seguridad de las WLAN
 - Medidas de seguridad en el router
 - Amenazas en los terminales móviles
6. Caracterización de los mecanismos de protección de la información
 - Fuga de la información
 - Gestión de la fuga de información
 - Métodos de copia de seguridad
 - Restauración de los datos
7. Reconocimiento de los sistemas biométricos y aplicaciones
 - Técnicas biométricas
 - Aplicaciones de la biometría
 - Gestión de riesgos en biometría
8. Identificación de los servicios que se implementan en la nube
 - Cloud computing
 - Seguridad en la nube
 - Servicios de seguridad en la nube
9. Caracterización de los diferentes tipos de ciberataques
 - Categorías de los ciberataques
 - Ataques para obtener información



- Ataques a nivel de red
- Ataques de monitorización
- Ataques de autenticación
- Ataques de denegación de servicio

UNIDAD DIDÁCTICA 2. APLICACIÓN DE LA CIBERSEGURIDAD EN LAS PYMES

1. Introducción de la ciberseguridad en la empresa
 - Seguridad en la empresa
 - Causas de los ataques en la empresa
 - Revisión de ciberseguridad en la empresa
 - Pilares de una estrategia de ciberseguridad
 - Roles en ciberseguridad
 - Controles de seguridad a establecer en una organización
2. Identificación del usuario como elemento de ciberseguridad en la empresa
 - Rol del usuario en el puesto de trabajo
 - Protección del puesto de trabajo
 - Acceso remoto y teletrabajo
 - Escritorio virtual
3. Detección de necesidades de protección y seguridad en las empresas
 - Clasificación de la información empresarial
 - Medidas de protección de la información



- Almacenamiento seguro de la información
 - Eliminación de los datos. Borrado seguro
 - Conservación de la información
 - Almacenamiento extraíble
4. Desarrollo de planes y políticas de seguridad en una empresa
 - Plan director de seguridad
 - Políticas de seguridad dirigidas a los componentes de la empresa
 - Normas y procedimientos técnicos
 5. Utilidad de los planes de continuidad de negocio en la empresa
 - Análisis y gestión de riesgos
 - Plan de continuidad de negocio
 - Plan de contingencia
 - Auditorías de seguridad
 6. Necesidad de un plan de recuperación de desastres en la empresa
 - En plan de recuperación de desastres
 - Guía de desarrollo de un plan de recuperación de desastres
 7. Introducción a la seguridad en el comercio electrónico
 - Identidad digital y reputación empresarial
 - Cliente online y su protección
 - Redes sociales y la empresa
 - Fraude online
 - Protección de la web



www.formatesincoste.com

info@formatesincoste.com

Tfno: 956 074 222/655 617 059

Fax: 956 922 482

8. Aplicación de medidas de ciberseguridad en redes inalámbricas y dispositivos móviles

- Formas de ataque y métodos de seguridad en las redes inalámbricas
- Sistemas de gestión de dispositivos móviles de la empresa
- Estrategia BYOD

9. Caracterización de la tecnología IoT en la empresa

- IoT en la empresa en la actualidad y en el futuro.
- Riesgos de seguridad
- Recomendaciones de seguridad