Ciberseguridad para microempresas

Modalidad: curso e-Learning Duración: 15 horas

Categorías: Ofimática, informática y comunicaciones

OBJETIVOS

- Conocer, comprender y analizar los riesgos de seguridad más habituales en una microempresa, adquiriendo habilidades para el análisis y síntesis en la toma de decisiones en los ataques informáticos. - Establecer una política organizacional que defina unas normas de seguridad a tenor de los diferentes escenarios, sistemas y fórmulas de acceso, analizando los elementos básicos que toda microempresa, con independencia de sus necesidades particulares, debe contemplar para el diseño de unas políticas de seguridad efectiva.

CONTENIDOS

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.