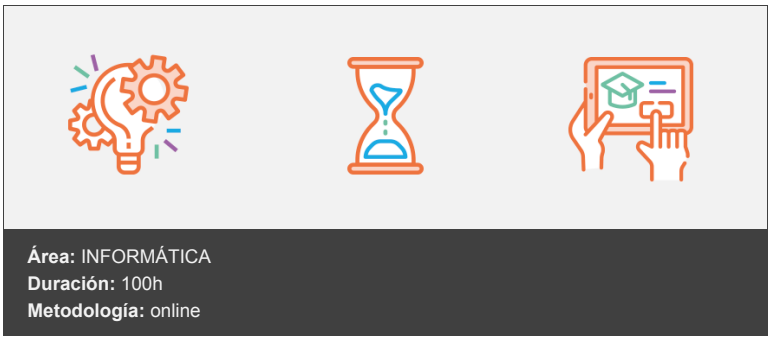
Gestión de la seguridad informática en la empresa. IFCT050PO



Área: INFORMÁTICA
Duración: 100h
Metodología: online

Objetivos

- Gestionar la seguridad informática en la empresa.
- Generar consciencia empresarial sobre la importancia de contar con un sistema de seguridad informática que haga frente a los peligros y amenazas de la red.
- Asegurar el acceso a los equipos informáticos, dispositivos móviles y navegación por internet como herramientas de gestión empresarial, mediante la aplicación práctica de los conocimientos básicos sobre seguridad.
- Incorporar a la filosofía de la empresa una educación en el uso responsable de los recursos tecnológicos, basados en la información, y que facilitan la tarea diaria en la consecución de los objetivos empresariales.
- Acercar conocimientos en política de seguridad informática para profesionales autónomos, pymes, empresas, organizaciones públicas o privadas, empleados, usuarios y colaboradores con el fin de identificar los elementos claves para salvaguardar y proteger la integridad de los sistemas de información frente a la ciberdelincuencia.
- Abordar los elementos relativos a las diligencias de las organizaciones destinadas a velar por la buena gestión de los activos de la información y por el cumplimiento de la normativa en gestión de seguridad informática.
- Afrontar los elementos relativos a las estrategias de seguridad informática, a fin de obtener una visión global de las maniobras de seguridad como respuesta a los peligros a los que se enfrentan diariamente las organizaciones.
- Arrojar elementos que determinen la importancia de gestionar adecuadamente tanto los canales de transmisión de los activos de información como las infraestructuras físicas y digitales que dan soporte a toda la operatividad de una empresa, con el fin de sentar unas bases de seguridad, a fin de obtener criterios claros de las maniobras básicas como respuesta a las amenazas o imprevistos.
- Abordar los elementos relativos a ataques informáticos remotos y locales, su clasificación y tipología, con el fin de definir las maniobras oportunas para que las organizaciones puedan gestionar adecuadamente la seguridad de sus activos.
- Examinar los elementos relativos a la seguridad en redes inalámbricas, encaminadas a proveer a las organizaciones de un recuso de inestimable valor para su quehacer diario.
- Abordar los elementos relativos al estudio de las complejas técnicas criptográficas y de criptoanálisis en un entorno de innovación tecnológica constante.
- Abordar los procesos de autenticación, como medio de someter la identidad de un posible usuario a las pruebas necesarias para autorizar y confirmar el acceso a recursos.

Contenidos y estructura del curso

1. Introducción a la seguridad.
2. Políticas de seguridad.
3. Auditoría y normativa de seguridad.
4. Estrategia de seguridad.
5. Exploración de redes.

6. Ataques remotos y locales.
7. Seguridad en redes inalámbricas.
8. Criptografía y criptoanálisis.
9. Autenticación.

Metodología

En Criteria creemos que para que la formación e-Learning sea realmente exitosa, tiene que estar basada en contenidos 100% multimedia (imágenes, sonidos, vídeos, etc.) diseñados con criterio pedagógico y soportados en una plataforma que ofrezca recursos de comunicación como chats, foros y conferencias...Esto se logra gracias al trabajo coordinado de nuestro equipo e-Learning integrado por profesionales en pedagogía, diseño multimedia y docentes con mucha experiencia en las diferentes áreas temáticas de nuestro catálogo.

Perfil persona formadora

Esta acción formativa será impartida por un/a experto/a en el área homologado/a por Criteria, en cumplimiento con los procedimientos de calidad, con experiencia y formación pedagógica.