



Redes y Seguridad

Las organizaciones se han visto en la necesidad de conectarse en red para aumentar el rendimiento de sus procesos y compartir tanto recursos como información, actividades que les permiten alcanzar de manera acelerada sus objetivos económicos. Asimismo, se han visto en la imperante necesidad de conectarse a la Internet para poder llegar a mayor cantidad de clientes y posibles consumidores. Sin embargo, esta conexión entre computadores y la apertura a la red trae como consecuencia la posibilidad de ser vulnerables ante personas malintencionadas cuyo propósito puede ser tanto el robo de información, como la simple destrucción de protocolos, estándares y procesos de las empresas, ya que el uso de dispositivos compartidos lleva como consecuencia inevitable la apertura de “puertos” y agujeros en los esquemas de conexión. Es por esta razón que las redes deben ser administradas y vigiladas de una manera eficiente y cuidadosa por personal calificado en la seguridad de las mismas. Y no solo esto, como las redes son manipuladas por usuarios, a veces las herramientas usadas en su protección no son suficientes para que los usuarios, sea por error o con intención, no generen vulnerabilidades y posibles daños a la red. Es también por esta razón que el administrador de la red debe tener conocimiento de las diversas políticas que pueden y deben instaurarse en una organización para proteger su información. Este curso está dirigido principalmente a formar las competencias necesarias que habilitan a un administrador de red para proteger, controlar, politizar y volver eficiente, (de una manera básica), la transferencia y uso de la información en las redes.

Contenido

- 1. Redes y modelo OSI:
 - o Transmisión de información.
 - o Tipos de redes.
 - o Modelo OSI.
 - o Conceptos de seguridad.
- 2. Políticas generales de seguridad:
 - o Políticas de seguridad informática (PSI).
 - o Riesgos en la organización.
 - o Niveles de trabajo con los datos.
 - o Establecimiento de riesgos de los recursos de la organización
- 3. Vulnerabilidades en la organización: tipos y soluciones:
 - o Denial of service.
 - o Cracking de passwords.
 - o E-mail bombing y spamming.
 - o Problemas de seguridad en el FTP.



- TELNET.
- Herramientas de control de accesos.
- Herramientas que chequean la integridad del sistema.
- 4. Proyecto final:
 - Creación manual.

Habilidades que Desarrolla

- Ensamblar y configurar una red básica.
- Instalar software en servidores.
- Monitorear el flujo de datos en una red de información.
- Crear informes para diversos elementos jerárquicos de una empresa.

Requisitos de Ingreso

Es importante que las personas interesadas en el curso, tengan conocimientos básicos sobre las redes de computadores y software básico.

Se requiere que el aprendiz tenga acceso a Internet y tecnología como computador. Además, dominio de los elementos básicos relacionados con el manejo de herramientas informáticas y de comunicación: correo electrónico, software para ofimática y navegadores.

Inscríbese aquí! 