**Nombre de la asignatura:** Seguridad Informática

**Créditos:** 2 - 3 - 5

**Aportación al perfil**

- Aplicar conocimientos científicos y tecnológicos en la solución de problemas en el área informática con un enfoque interdisciplinario.
- Seleccionar y utilizar de manera óptima técnicas y herramientas computacionales actuales y emergentes.
- Aplicar normas, marcos de referencia y estándares de calidad y seguridad vigentes en el ámbito del desarrollo y gestión de tecnologías y sistemas de información.

**Objetivo de aprendizaje**

- Hacer uso de las herramientas de software para contribuir a mejorar los niveles de seguridad informática en una organización.

**Competencias previas**

- Conocimiento en el manejo y funcionalidad de los sistemas de información (bases de datos), redes de computadores, software base (sistemas operativos, lenguajes de programación).

**Temario**

- Introducción
  - Introducción a la seguridad informática
  - El valor de la información
  - Definición y tipos de seguridad informática
  - Objetivos de la seguridad informática
  - Posibles riesgos
  - Técnicas de aseguramiento del sistema

- Algoritmos criptográficos
  - En la antigüedad
  - Cifradores del siglo XIX
  - Criptosistemas clásicos
  - Máquinas de cifrar (siglo XX) y estadística del lenguaje

- Certificados y firmas digitales
  - Distribución de claves.
  - Certificación.
  - Componentes de una PKI (infraestructura de clave pública).
  - Arquitecturas PKI.
  - Políticas y prácticas de certificación.
  - Gestión de una PKI.
  - Estándares y protocolos de certificación.
  - Prueba con OpenCA.

- Seguridad en redes
  - Aspectos de la seguridad en las comunicaciones.
  - Debilidades de los protocolos TCP/IP.
  - Estándares para la seguridad en redes.
  - Seguridad en Redes Wireless (wep, wpa, wpa2).

- Firewalls como Herramientas de Seguridad
  - Tipos de Firewall.
  - Ventajas de un Firewall.
  - Limitaciones de un Firewall.
  - Políticas del Firewall.
  - Enlaces externos.
  - Creación de DMZ.

- Vigilancia de los Sistemas de Información
  - Definición de vigilancia.
  - Anatomía de un ataque.
  - Escaneos.
  - Identificación de vulnerabilidades.
  - Actividades de infiltración.
  - Consolidación.
  - Defensa perimetral.

**Actividades de aprendizaje**

- Analizar el funcionamiento del protocolo TCP/IP.
- Conocer como se da el control de acceso a los medios.
- Implementar los algoritmos de manera manual y mediante un lenguaje de programación.
- Conocer y aplicar el funcionamiento de los protocolos que existen en redes y redes inalámbricas y sus diferencias.
- Analizar de las diversas vulnerabilidades que pueden presentar las redes Wireless.
- Instalar, configuración y administración de un firewall con IPcop de Linux.
- Administrar usuarios, grupos cuentas y terminales remotas.
- Instalación de herramientas para el monitoreo y análisis de tráfico de una red.

**Sugerencias didácticas transversales para el desarrollo de competencias profesionales.**

- Instalación y administración de un sistema de cortafuegos:
    - Firewall por hardware
    - Firewalls por software
    - Instalación de un servidor headless.
- Realizar una práctica con OpenCA, cumpliendo con los lineamientos
- Creación de un servidor web, asignación de IP pública con el fin de practicar y mostrar su vulnerabilidad si no es configurado de manera adecuada.
- Ejemplos con mínimo 2 sistemas operativos.
- Instalación de Soluciones de Antivirus Centralizadas.
- Creación de un Servidor Proxy en diversas plataformas
- Uso de herramientas de monitoreo de red.
- Uso de IPSEC.

**Prácticas**

- Formulación de una política de seguridad
- Instalación, configuración y administración de un Firewall con IPcop
- Instalación de un servidor Proxy con SQUID.
- Instalación de un servidor Proxy con ISA Server
- Instalación de una aplicación centralizada con Symantec o alguna solución de antivirus que posea.
- Instalación de un servidor de Directorio con Windows 2003.
- Instalación y pruebas de seguridad de una red inalámbrica.
- Instalación de un servidor WEB con Apache en Linux, IIS en Windows 2003.
- Instalación de herramientas bajo el model NSM.
- Formulación de un esquema de red segura con la implementación de todas las prácticas anteriores elaboradas.