Seguridad Informática

1) Introducción.
   a) Definición de seguridad de la información.
   b) Importancia de la seguridad.
   c) Triada de la seguridad.
2) Definición de vulnerabilidades y amenazas.
   a) Tipos de vulnerabilidades.
   b) Tipos de amenazas.
   c) Definición de ataques.
3) Implementación de sistemas de seguridad.
   a) Seguridad física.
   b) Seguridad lógica.
   c) Sistemas de control de acceso.
   d) Seguridad perimetral.
   e) Sistemas de detección de intrusos.
4) Análisis de riesgos.
   a) Definición de activo, riesgo, riesgo residual.
   b) Análisis cualitativo.
   c) Análisis cuantitativo.
   d) Metodologías de análisis.
5) Política de seguridad.
   a) Objetivo de la política de seguridad.
   b) Estructura y elementos de la política.
   c) Implementación de la política.
   d) Planes de recuperación y continuidad del negocio.
6) Seguridad en ambientes virtualizados.
   a) Riesgos de la virtualización.
      i) Principales riesgos de la virtualización.
      ii) Esquemas de red utilizados.
      iii) Diseño de un esquema de red seguro para virtualización.
      iv) Integración con la red y otros equipos externos.
   b) Seguridad en Virtualización en Servers.
      i) Ventajas y Desventajas desde el punto de vista de la seguridad.
      ii) Seguridad del hypervisor y/o host.
      iii) Administración del Hypervisor / host.
      iv) Seguridad en Máquinas Virtuales.
      v) Roles o perfiles de usuarios.
7) Seguridad en sistemas Linux.
   a) Ventajas del uso de Software Libre en términos de seguridad.
   b) Desventajas del uso de Software Libre en términos de seguridad,
   c) Seguridad en GNU.
      i) ¿Es GNU/Linux un sistema seguro?
      ii) Ofrecer seguridad a un sistema GNU.

8) Seguridad en base de datos.
   a) Conceptos generales de Bases de Datos.
   b) Principales riesgos.
   c) Elementos de seguridad a considerar.
   d) Características de una base de datos Oracle.