



## PROGRAMA DE EXAMEN

CARRERA: Tecnicatura Superior en Informática y Redes de datos

CÁTEDRA: Seguridad Informática

AÑO : Tercero

DIVISIÓN: Única



### CONTENIDOS

#### Unidad 1: Fundamentos de la Seguridad Informática

Fundamentos de Seguridad Informática

Conceptos Fundamentales sobre SI

Seguridad Informática

Aspectos. Triángulo fundamental de la seguridad informática (CID)

Elementos

Amenazas

Niveles de Seguridad

Normas y principios

Amenazas. Tipos de amenaza. Amenazas Lógicas: ransomware, phishing, código malicioso, spam.

Amenazas Humanas: Personal Interno, exempleados, curiosos, terroristas, intrusos remunerados.

Desastres. Tipos de desastres. Prevención. Recuperación

Metodologías de Ataque. Ataques de acceso. Ataques de reconocimiento. Ataques de Denegación de Servicio

Firewall. IDS. IPS

Terminología Hacking



## Terminología

### Pasos para hackear un sistema

Reconocimiento

Scanning

Obtener Acceso

Mantener el acceso

Limpiar las Pistas

Denial of Service

Bugs y Exploits

## Delitos Informáticos

### **Unidad 2: Auditoría en Sistemas de Información y Políticas de Seguridad Informática**

Auditoría en Informática. Generalidades. Alcance. Importancia. Tipos. Metodología de una Auditoría.

Políticas de Seguridad Informática. Generalidades. Definición de Políticas de Seguridad Informática. Elementos de una Política de Seguridad Informática. Parámetros para Establecer Políticas de Seguridad. Razones que Impiden la Aplicación de las Políticas de Seguridad Informática.

**IMPORTANTE:** De Unidad 2, estudiar sólo conceptos generales de Auditoría. Se les preguntará del Trabajo práctico realizado por Ustedes mismos: Tipo de Auditoría elegido, lugar donde se realizó, metodología utilizada (pasos), vulnerabilidades encontradas, propuestas de mejora.

### **Unidad 3. Criptografía**

Introducción a los Criptosistemas

Criptografía y Criptoanálisis. Criptografía clásica. Operaciones de sustitución y permutación.

Clave secreta. Ejemplos de cifrado clásico. Criptografía moderna. Cifrado por flujo. Cifrado por bloque.

Cifradores tipo Feistel. Cifradores más conocidos. DES y su criptoanálisis. 3DES. IDEA. AES.



Cifrado Asimétrico. RSA

Autenticación y Firma Digital. Los problemas de la integridad. Diferencias Firma Digital - Firma Electrónica – Digitalizada. Firma Digital en Argentina

Certificados Digitales. Certificado digital X.509 Introducción a las Autoridades de Certificación.

#### **Unidad 4. Seguridad en redes alámbricas e inalámbricas**

WEP y sus deficiencias. WPA, WPA2 y 802.11i.

Mecanismos de defensa. Consideraciones para asegurar una red inalámbrica

Comparación AES / TKIP. Diferencias entre WEP, WPA, WPA2, AES y TKIP