**SEGURIDAD Y AUDITORÍA INFORMÁTICA**

**Programa Analítico**

**Ciclo Lectivo 2023.**

**Unidad 1: INTRODUCCION – ASPECTOS CONCEPTUALES**

Conceptos de seguridad informática. Objetivos generales. Protección de la Información: propiedades y características de la información.

Seguridad Física y lógica. Seguridad activa y pasiva. Fundamentos de la seguridad Informática: Estándares.

**Unidad 2: SEGURIDAD FISICA EN INSTALACIONES**

Definición de seguridad física. Desastres: Tipos. Protección contra: agresiones, desastres naturales. Abastecimiento de electricidad: UPS. Esquema básico de seguridad eléctrica. Seguridad en comunicaciones. Acceso físico: métodos biométricos, otros métodos. Seguridad en el Lay-Out. Seguridad de acceso y transporte de información.

**SEGURIDAD FISICA EN EQUIPOS Y DATOS.**

Tolerancia a fallos: redundancia, duplicación, método RAID y sus variantes. Mantenimiento de equipos. Niveles de aplicación. Tipos de mantenimiento. Resguardo de datos: tipos, planificación, copias. Diseño de un plan de recuperación de contingencias. Recuperación de desastres. Ejemplos.

**Unidad 3: RIESGO INFORMATICO.**

Amenazas. Vulnerabilidad. Ataques. Contingencias: clasificación. Activos de información: identificación, clasificación y valoración. Análisis de riesgos. Valoración de riesgos. Tablas de valoración de riesgos. Fraudes y delitos informáticos, tipificación. Políticas de Protección de la información. Acceso no autorizado a servicios y sistemas informáticos.

**Unidad 4: SEGURIDAD LOGICA**

Principios fundamentales. Medidas de seguridad. Control de acceso lógico: por organización del control, passwords. Motivaciones para activar mecanismos de seguridad. Proceso de identificación y autentificación. Tipos de dispositivos de identificación. Sistemas Biométricos.

**SEGURIDAD EN INTERNET**

Seguridad en la web. Internet: Características y generalidades. Etapas de seguridad en la web. Ataques: a la navegación, al servidor, a la información en tránsito.

**VIRUS INFORMATICOS Y OTROS CODIGOS MALICIOSOS**

Antivirus. Tipos de daños. Técnicas de detección de virus. Virus, gusanos, programas mal intencionados (Malware). Programas espía (spyware) y publicitarios (adware). Otras tendencias dañinas (spam, phishing).

**Unidad 5: PROCESO DE ENCRIPTACION**

Esteganografïa. Criptografía: definiciones, métodos clásicos.

Sistemas de encriptación. Algoritmos. Métodos simétricos y asimétricos. Estándares sistema DES y sus variantes. Sistema RSA y sus alternativas. Métodos para la determinación de claves. Firma digital. Política de manejo de claves (Creación, distribución, Mantenimiento). Certificado Digital

**Unidad 6: AUDITORIA INFORMATICA – CONCEPTOS GENERALES**

Definiciones. Auditoria de sistemas de Información: requisitos de área y del personal, aplicaciones. Descripción del ciclo metodológico: Diagnostico, justificación, adecuación, formalización, desarrollo, implementación. Informe final: estructura y pautas. El perfil del auditor y su papel. Tareas y responsabilidades.

**Unidad 7: METODOS DE AUDITORIA INFORMATICA**

Método alrededor del computador. Usando el computador: variantes. Metodologías: mini compañía, datos de prueba. Mapping, Comparadores de programas, procesamiento duplicado, tagging snapshot, scarf, tracing. Normativa aplicada a la auditoria. Standart cobit, determinación de los objetivos de control, marco metodológico.

**Unidad 8: CONCEPTOS DE ERGONOMIA**

Normas de Seguridad laboral en un ambiente informático. El entorno, el espacio, la iluminación. Normas ISO. La ergonomía y la salud.

Ing. María C. Aparicio

Profesor Adjunto.