

# **Propuesta de Curso: Introducción a la Ciberseguridad**

***Duración del Curso:*** 12 semanas (3 meses)

***Modalidad:*** Presencial

***Horas por Semana:*** 4 horas (2 sesiones de 2 horas cada una)

***Total de Horas:*** 48 horas

## **Objetivos del Curso:**

- Comprender los conceptos básicos de ciberseguridad.
- Conocer amenazas, vulnerabilidades y riesgos más comunes en el ámbito digital.
- Aprender a implementar prácticas de seguridad básicas para la protección de datos personales y empresariales.
- Introducirse en el uso de herramientas y técnicas de ciberseguridad.

## **Requisitos Previos:**

- Conocimientos básicos de informática.
- Familiaridad con sistemas operativos y redes.

Si no se cuenta con ningún conocimiento previo y no hay problema solo se extendería 2 semanas el curso para dotar de dichos conocimientos a los alumnos.

## **Materiales y Recursos:**

- Acceso a una computadora con conexión a Internet.
- Herramientas de Ciberseguridad (Kali Linux, Wireshark, etc.).
- Lecturas recomendadas y material de apoyo.

## **Público Objetivo:**

- Estudiantes dirigidos a carreras de informática o carreras afines.
- Profesionales de TI interesados en la seguridad de la información.
- Cualquier persona interesada en adquirir conocimientos básicos en ciberseguridad.

# Plan de Estudios

## Módulo 1: Fundamentos de Ciberseguridad (semana 1-2)

### *Conceptos Básicos de Ciberseguridad*

- Definición y objetivos de la ciberseguridad.
- Triada CIA (Confidencialidad, Integridad y Disponibilidad).
- Historia y evolución de la ciberseguridad.

### *Amenazas y Vulnerabilidades*

- Tipos de Amenazas: malware, phishing, ransomware, etc.
- Conceptos de vulnerabilidad y riesgo.
- Análisis de casos reales de ciberataques.

## Módulo 2: Redes y Seguridad en la Red (Semana 3-4)

### *Conceptos Básicos de Redes*

- Protocolos de red: TCP/IP, DNS, HTTP/HTTPS.
- Modelo OSI y su relación con la seguridad.

### *Seguridad en Redes*

- Firewalls y sistemas de detección de intrusos (IDS/IPS).
- VPNs y su importancia en la protección de datos.
- Conceptos de Wi-Fi seguro y ataques comunes (ej. Man-in-the-Middle).

## Módulo 3: Criptografía Básica (Semana 5-6)

### *Fundamentos de Criptografía*

- Historia de la criptografía y su importancia.
- Criptografía simétrica y asimétrica.
- Hashing y su aplicación en la seguridad.

### *Implementación Práctica de Criptografía*

- Uso de certificados digitales.
- Cifrado de datos y comunicaciones.

## Módulo 4: Seguridad en Aplicaciones y Sistemas (Semana 7-8)

### *Principios de Seguridad en el Desarrollo de Software*

- Ciclo de vida seguro del desarrollo de software (SDLC).
- Pruebas de seguridad en aplicaciones.

### *Seguridad en Sistemas Operativos*

- Hardening de sistemas: Windows y Linux.
- Control de acceso y gestión de permisos.

## Módulo 5: Gestión de Identidades y Acceso (semana 9-10)

### *Autenticación y Autorización*

- Métodos de autenticación: contraseñas, 2FA, biometría.
- Control de acceso basado en roles (RBAC).

### *Gestión de Identidades*

- Introducción a sistemas de gestión de identidades (IAM).
- Buenas prácticas para la gestión de contraseñas y políticas de acceso.

## **Módulo 6: Aspectos Legales y Éticos de la Ciberseguridad (semana 11)**

### **Marco Legal y Normativo**

- Leyes y regulaciones relevantes: GDPR, Ley de Protección de Datos, etc.
- Conceptos de privacidad y protección de datos.

### **Ética en Ciberseguridad**

- Principios éticos en la ciberseguridad.
- Responsabilidad profesional y ética del hacker.

## **Módulo 7: Prácticas y Evaluación Final (Semana 12)**

### **Simulaciones y Laboratorios**

- Simulación de ciberataques y defensa.
- Análisis forense básico.

### **Evaluación Final**

- Proyecto integrador.
- Examen teórico y práctico.

### **Evaluación:**

- Participación y asistencia: 20%
- Tareas y laboratorios: 30%
- Proyecto final: 30%
- Examen teórico/práctico: 20%

### **Datos de Contacto:**

Nombre: Leonardo Ernesto Correa Hernández

Correo: [mystogan785@gmail.com](mailto:mystogan785@gmail.com)

Número Celular: 5563267998