



## Introducción a la seguridad Informática

### Sinopsis

La seguridad informática es un aspecto de gran importancia en estos tiempos, tanto de manera personal como organizacional y empresarial. Por ello, es importante identificar nuestros activos informáticos, conocer los servicios de seguridad que se requieren proveer y aplicar las herramientas adecuadas para poder protegerlos.

### Objetivo

Los participantes al curso identificarán las vulnerabilidades y riesgos que tiene un activo informático, para así implementar algunas herramientas de seguridad que permitan proteger al activo de posibles ataques.

### Dirigido a

Todas aquellas personas que no cuenten con una preparación en seguridad informática y para aquellas que estén interesadas en mejorar o actualizar sus conocimientos.

### Metodología

Sesiones teóricas con ejemplos prácticos y ejercicios de clase tipo taller, lecturas referenciadas para ampliar el panorama de los temas expuestos en clase y presentación de software comercial para complementar habilidades.

La presentación del software comercial y el pago del curso no implica la obligación por parte del expositor o de CAPIT de proporcionarlo para su uso, ni el otorgar Licencia de uso.

**ES INDISPENSABLE QUE CADA ASISTENTE TRAIGA SU PC Y SOFTWARE CARGADO.**



# CONTENIDO



## Capítulo 1 Fundamentos teóricos

Conocer el mundo de la seguridad informática y sus agentes involucrados. Identificar algunas definiciones más coloquiales y usadas cuando un equipo se encuentre vulnerable.

- 1.1. *¿Qué es la seguridad?*
- 1.2. *Virus, troyanos y gusanos*
- 1.3. *¿Qué es un ataque?*
- 1.4. *¿Qué es una amenaza?*
- 1.5. *Vulnerabilidad*
- 1.6. *Práctica 1*

## Capítulo 2 Medios de contagio

Identificar los medios de contagio más comunes y que ponen en riesgo la seguridad e integridad de un equipo.

- 2.1. *Sistemas operativos*
- 2.2. *Mitos y realidades*
- 2.3. *Dispositivos de almacenamiento externos USB.*
- 2.4. *Conexión a Internet en lugares públicos*
- 2.5. *Robo de identidad.*
- 2.6. *Suplantación*
- 2.7. *Las toolbar y los pop-up*
- 2.8. *Software malicioso*
- 2.9. *Práctica 2.*

## Capítulo 3 Medios de Protección

Identificar cuáles son los medios de protección más comunes y evaluar el costo-beneficio de contar con una protección informática.

- 3.1. *Evaluación de la información a proteger*
- 3.2. *Tipos de protección*
- 3.3. *Práctica 3*

## Capítulo 5 Antivirus

Identificar las diferencias entre Antivirus y Software que complementa al antivirus para una mejor protección de los equipos.

- 5.1. *Tipos de antivirus*
- 5.2. *¿Cuál elegir? ¿Cómo instalarlo?*
- 5.3. *Práctica 4*

## Capítulo 5 Buenas Prácticas

Adquirir conciencia de las buenas prácticas que tiene que llevar a cabo durante el uso de un equipo de cómputo.