Contenidos:

1. Conceptos básicos sobre TI y Seguridad de la Información. Hardware y Software. Mecanismos que entran en juego cuando usamos un equipo (desktop, netbook, smartphone) de modo particular, la red del trabajo, Internet, el correo electrónico, dispositivos de seguridad.

Dato e información. Soportes en los que se pueden encontrar. Documento digital. Falta de confidencialidad, integridad, disponibilidad.

Amenazas y vulnerabilidades. Mecanismos de protección. Identificación de usuario. Firma Digital. Certificado digital.

2. Seguridad de la información sobre datos personales. Nociones de bases de datos. Medidas de Seguridad para las bases de datos dictadas por la DNPDP (privados y públicos). Mecanismos para proteger la confidencialidad, la integridad, la cesión. Esto es: roles, perfiles (autorización de usuarios y recursos), identificación y autenticación. Registración de las operaciones (logs). Vinculación con el art. 8º de la Ley 26.388.

3. Relación con las figuras de delitos incorporados por la ley 26.388.

Métodos utilizados para la distribución de pornografía infantil (Art. 2). Acciones que recaen en la tipificación: "*abriere o accediere indebidamente a una comunicación electrónica*". Mecanismos que los permiten. Qué puede hacer un usuario interno o externo, especialmente si es un criminal. (Art. 4º).

Acciones que recaen en la tipificación: "*el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido*." (Art. 5º).

Acciones que recaen en la tipificación "*el que hallándose en posesión de una correspondencia, una comunicación electrónica…..*" (Art. 6º).

Métodos de las organizaciones delictivas. Ingeniería social. Fraude en Internet. Robo de identidad. Software malicioso y software de protección. Recomendaciones para evitar los riesgos.

4. Análisis forense. Evidencia. Validez de la prueba. Tratamiento de la evidencia.