

**Panel : *La visión jurídica: necesidad de marcos normativos***

# ***LA LEY 26388 Y LA PRODUCCION DE PRUEBA INFORMATICA***

***1° Octubre de 2009***

**Ing. Gustavo Daniel Presman – MCP , EnCE , CCE, EnCI, ACE**  
**ESTUDIO DE INFORMATICA FORENSE**  
**[gustavo@presman.com.ar](mailto:gustavo@presman.com.ar)**  
**[www.presman.com.ar](http://www.presman.com.ar)**

## LA 26388 Y EL NUEVO GLOSARIO

**Artículo 4.-** Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una **comunicación electrónica**, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

**Artículo 5.-** Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, 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. La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.”

**Artículo 8.-** Será reprimido con la pena de prisión de un mes a dos años el que: 2. Ilegítimamente proporcionare o revelare a otro información registrada en un **archivo** o en un **banco de datos** personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

**Art. 10.-** Incorporáse como segundo párrafo del artículo 183 del Código Penal, el siguiente: “En la misma pena incurrirá el que alterare, destruyere o inutilizare **datos, documentos, programas o sistemas informáticos**; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.”

## **VALIDEZ DE LOS MEDIOS DE PRUEBA INFORMATICA**

- **VALIDEZ TECNICA**  
**Procedimientos de Recolección y Validación**
  
- **VALIDEZ JUDICIAL**  
**Admisibilidad según fuero y criterio magistrado**

## **LA PRUEBA INFORMATICA**

- **La Prueba Informática es Independiente de la Ley 26388 .**
- **Es necesario trabajar con procedimientos estandarizados de validez internacional acordes al tipo de medio empleado**
- **Es necesario que los operadores intervinientes estén capacitados en el manejo de evidencia digital**

## ***Como Manipular EVIDENCIA INFORMATICA ?***

**Trabajar con Estándares de Mejores prácticas para la adquisición de evidencia digital (prueba informática)**

### **INTEGRIDAD - AUTENTICIDAD - CONFIABILIDAD**

- **La etapa de recolección (*evidence collecting*) debe iniciarse por un profesional con conocimientos en informática forense que pueda sostener los procedimientos empleados**
- **Se debe mantener una cadena de custodia durante todo el proceso**

## ***Donde se encuentra la evidencia ?***

### **Medios de Almacenamiento :**

- Diskette
- Disco rígido
- CD/DVD
- Pen drive , Compact Flash / Memory stick
- Cinta magnética
- Cinta DAT
- PC Card
- Minidisk
- Smart Card

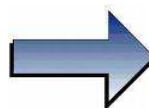
## *Donde se encuentra la evidencia ?*

### **Dispositivos de Almacenamiento :**

- PC
- Servidor
- Mainframe
- Notebook / Laptop
- PDA / Palm
- Teléfono celular
- Contestador electrónico
- Identificador de llamadas
- Faxes con memoria
- Impresoras
- Scanners con memoria
- Cámaras/filmadoras digitales
- Consolas de videojuegos
- GPS
- Dispositivos de acceso biométricos
- RFID

## AUTENTICACION DE EVIDENCIA

# POR MEDIO DE UN ALGORITMO DE HASH DEL ARCHIVO CONTENEDOR DE LA EVIDENCIA



$$GFP(t) = \frac{a}{\lambda \tau} \ln \left( 1 - \frac{b}{a} (1 - \exp(\lambda \tau t)) \right) + c$$
$$DD(t) = \frac{a \exp(\lambda \tau t)}{1 - \frac{b}{a} (1 - \exp(\lambda \tau t))}$$

5b748e186f622c1bdd6ea9843d1609c1

## ALGORITMOS DE HASH UTILIZADOS EN INFORMATICA FORENSE

MD5 (128 bits)

SHA-1(160 bits)

## **CLASIFICACION DE EVIDENCIA**

**EVIDENCIA ESTATICA** : Es aquella que se mantiene estable durante la adquisición



**EVIDENCIA DINAMICA** : Es aquella que se está modificando incluso durante la obtención



## **CADENA DE CUSTODIA**

- Que cosas debe incluir ?
- Nombre de la persona y fecha de contacto con la evidencia
- Registro del pasaje de una persona a otra
- Registro del pasaje de una ubicación física a otra
- Tareas realizadas durante la posesión
- Sellado de la evidencia al finalizar la posesión
- Registro de testigos
- Fotografías de la evidencia en las tareas realizadas
- Log de actividades durante la posesión

## **CONCLUSIONES**

Para que la evidencia informática tenga fuerza probatoria :

- ❖ Utilizar procedimientos estandarizados (Mejores prácticas)
- ❖ Emplear profesionales capacitados
- ❖ Documentar todo el procedimiento con la cadena de custodia (Expediente ó Formulario)

# Muchas Gracias por su participacion

**Ing. Gustavo Daniel Presman – MCP , EnCE , CCE, EnCI, ACE**

**ESTUDIO DE INFORMATICA FORENSE**

**[gustavo@presman.com.ar](mailto:gustavo@presman.com.ar)**

**[www.presman.com.ar](http://www.presman.com.ar)**