# Herramientas para asegurar la información conservando la eficiencia de los procesos

Victor Mora Escobar

# Índice

- A que estamos expuestos
- Mecanismos para asegurar la información.
- Y como se hubiera podido evitar.
- Asegurar no significa Obstaculizar.
- Preguntas y Respuestas

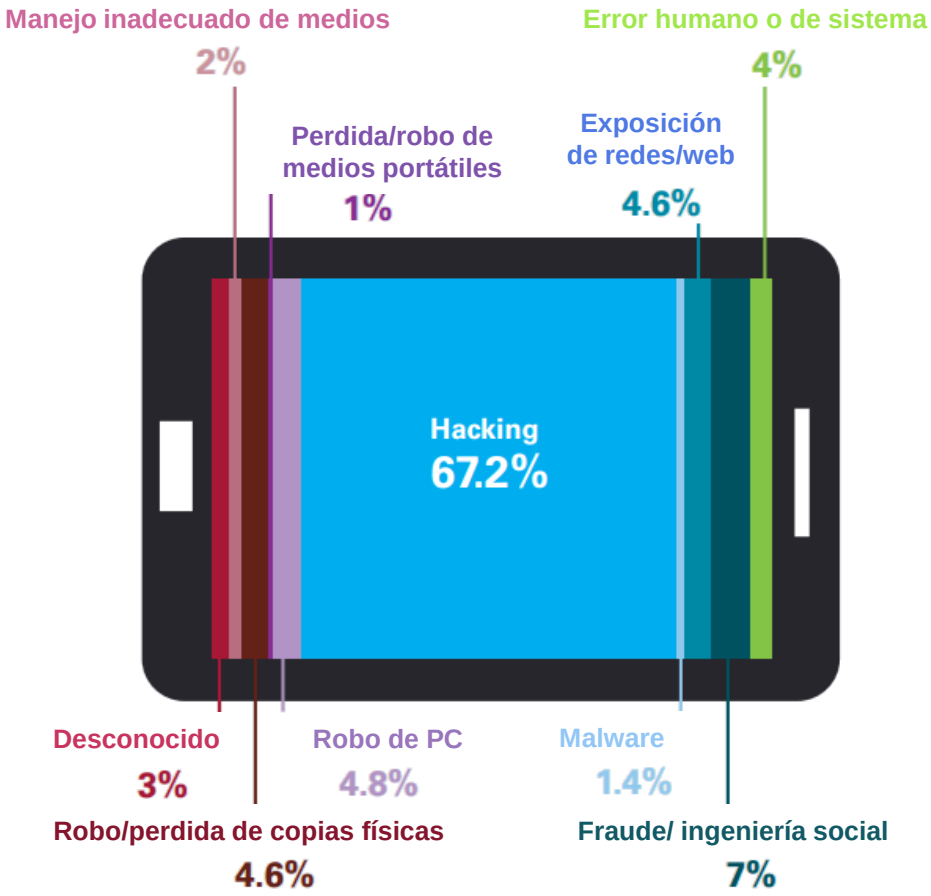
# Índice

- **A qué estamos expuestos**
- Mecanismos para asegurar la información.
- Y como se hubiera podido evitar.
- Asegurar no significa Obstaculizar.
- Preguntas y Respuestas

# A QUE ESTAMOS EXPUESTOS

- Proyecciones y Cifras

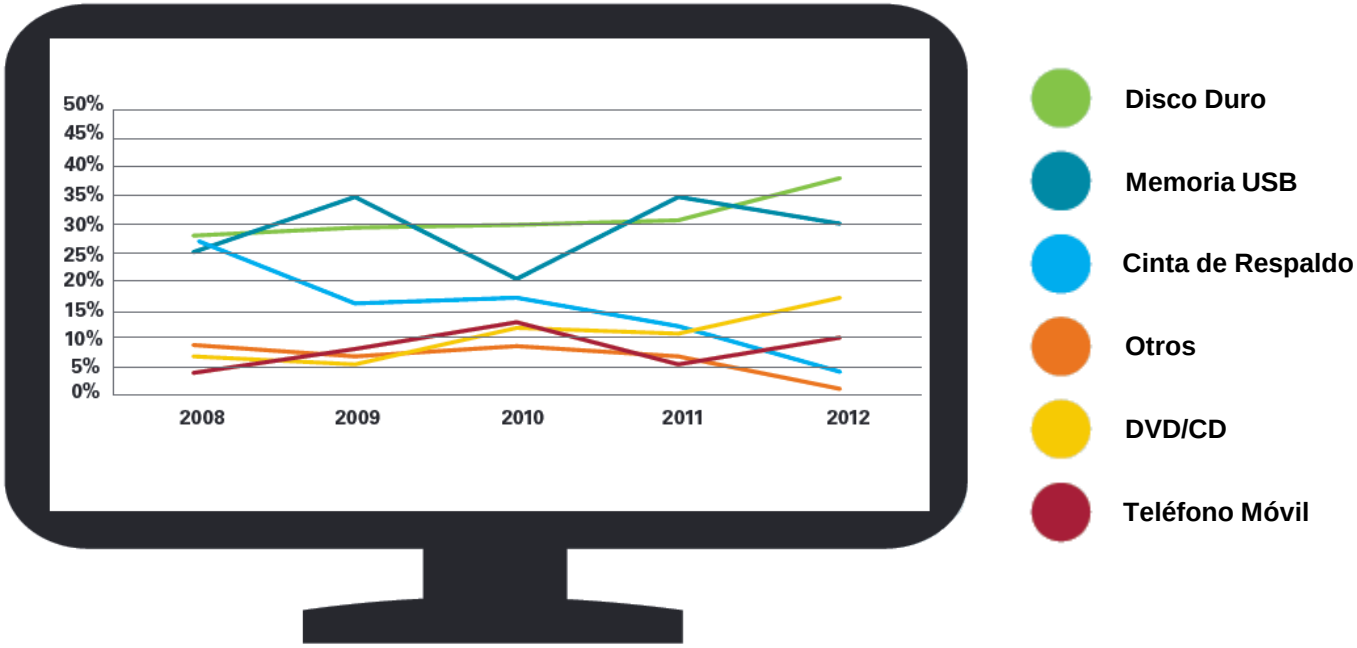
En el **2012** según cifras de un estudio de *KPMG* se presentaron la siguientes **categorías y porcentajes** de **incidentes de seguridad** relacionados con la perdida de datos:




***Fuente:"Data Loss Barometer", 2012, KPMG***

# A QUE ESTAMOS EXPUESTOS

- Proyecciones y Cifras




Según el mismo estudio de *KPMG* la clasificación de i**ncidentes en medios removibles** se comporto de acuerdo a la grafica:

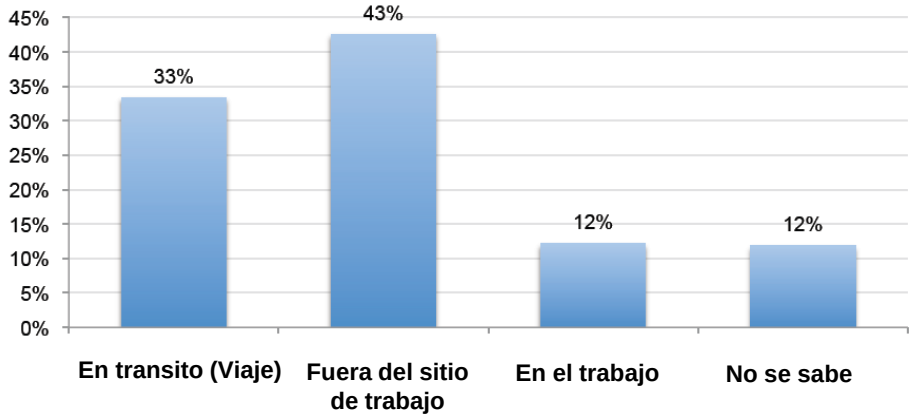
***Fuente:"Data Loss Barometer", 2012, KPMG***

# A QUE ESTAMOS EXPUESTOS

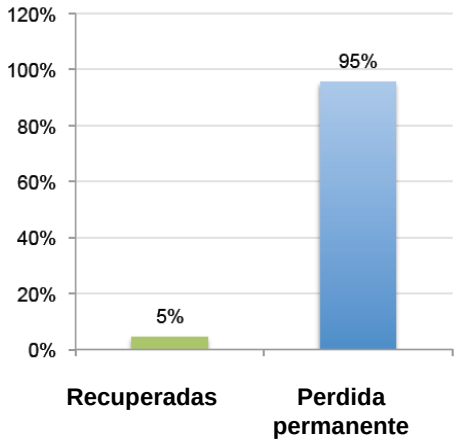
- Proyecciones y Cifras

En otro estudio encargado por **Intel** al **Ponemon Institute**, se alerta del problema de la **perdida de laptops** y la relevancia de su **información**.

Se tomo como base **3,676,000 laptops** en **349 compañías**, con una media de **86,455** Laptops perdidas








**Donde se pierden las laptops?**

Robadas **21,812 (25%)**
Sospecha de Robo **12,474 (15%)**
Perdida y/o olvidada **52,169 (60%)**

***Fuente:" The Billion Dollar Lost Laptop Problem", 2010, Ponemon Institute***

# A QUE ESTAMOS EXPUESTOS

- Casos mas renombrados de perdida de información

PlayStation®Network SONY make.believe

**Descripción**

*Abril 17 – Abril 19, 2011* .Fuera de línea (Caída) de los sitios principales **de PlayStation Network** y **Qriocity** como resultado de una **intrusión externa** en sus servidores centrales que almacenan la información de todos los usuarios con **consolas Playstation**, **dispositivos de audio** MP3 de Sony.

**Impacto**

Robo de Información sensible (usuario, password, nombres, direcciones físicas, direcciones de correo, fechas de nacimiento, perfil de jugador, historia de compra y numero de tarjetas de crédito) de **77 millones** de usuarios.

**Brecha**

A través de la utilización de la técnica de **SQL Injection** se consigue sacar información de sus bases de datos desde su sitio web, adicional los datos encontrados **no estaban encriptados**.

# A QUE ESTAMOS EXPUESTOS

- Casos mas renombrados de perdida de información


**Descripción**

*Mayo 2005*. Mastercard descubre **transacciones fraudulentas** en tarjetas procesadas por la firma **Card Systems**, procesador de tarjetas de los Estados Unidos. Este mismo incidente afecto igualmente tarjetas American Express, Discover, y Visa

**Impacto**

Robo de Información sensible de **40 millones** de tarjetas en Estados Unidos.

**Brecha**

A través de la utilización de la técnica de **SQL Injection** se consigue sacar información de sus bases de datos desde su sitio web.

# A QUE ESTAMOS EXPUESTOS

- Casos mas renombrados de perdida de información


U.S. Department of Veterans Affairs

**Descripción**

*Mayo 2006*. El departamento de Veteranos de Guerra reporta un incidente de perdida de información valiosa entre la que se encuentra nombres, números de seguridad social, fechas de nacimiento y algunas limitantes físicas de sus registrados y esposas.

**Impacto**

Perdida de Información sensible de **26 millones** de registros de ciudadanos americanos y sus esposas. **20 millones USD** en costos legales

**Brecha**

El envío a reparación de un **disco duro** dañado y **sin cifrar** deja expuesta esta información

# A QUE ESTAMOS EXPUESTOS

- Casos mas renombrados de perdida de información

Banco TD

**Descripción**

*Marzo 2012.* Información de clientes del **Banco TD** en Estados Unidos y Canadá se ve comprometida por la **perdida de cintas de respaldo**.

**Impacto**

Perdida de Información sensible de **267.000 clientes** (información personal, información de sus cuentas, y números de seguridad social) de clientes en Estados Unidos y Canadá

**Brecha**

La perdida de cintas de respaldo (Tape Backup) **sin cifrar** deja expuesta esta información

# A QUE ESTAMOS EXPUESTOS

- Casos mas renombrados de perdida de información

DigiNotar
Internet Trust Services

Entidad Certificadora de Holanda

**Descripción**

*Julio 2011*. La compañía Diginotar, dedicada a la emisión de certificados digitales a nivel mundial, se ve involucrada en un incidente de seguridad que permite el **robo de información** de usuarios conectados a **Google** desde Iran.

**Impacto**

Robo de Información sensible de **millones** de usuarios (acceso a cuentas de correo, servicios de aplicaciones, búsquedas, videos, etc) de ciudadanos en Iran.

**Brecha**

La emisión de **certificados digitales fraudulentos** por una entidad certificadora reconocida, permtiendo un ataque “Man in the middle”.

# Índice

- A qué estamos expuestos
- **Mecanismos para asegurar la información.**
- Y como se hubiera podido evitar.
- Asegurar no significa Obstaculizar.
- Preguntas y Respuestas

# Mecanismos para asegurar la informacion

## En el puesto de trabajo

- Herramientas de protección de **end-point** (Antivirus, Antimalware, IPS).
- **Cifrado** de **disco**, cifrado de **medios extraíbles.**
- Herramientas de **Respaldo y Cifrado**.

## En la red

- **Cifrado** de **comunicaciones** (VPN o Tunneling).
- Herramientas de **DLP** (Data Loss Prevention) en red.
- Herramientas de **Respaldo y Cifrado**.

# Mecanismos para asegurar la informacion

## En los servidores

- Herramientas de protección de server (Antivirus, Antimalware, IPS).
- Herramientas de DLP (Data Loss Prevention) en servers
- Cifrado de comunicaciones (VPN o Tunneling).
- Herramientas de Respaldo y Cifrado.
- Uso de **certificados digitales**.

## En la nube

- Herramientas de DLP (Data Loss Prevention) en red.
- Cifrado de comunicaciones (VPN o Tunneling).
- Herramientas de **Respaldo y Cifrado**.

# Índice

- A qué estamos expuestos
- Mecanismos para asegurar la información.
- **Y como se hubiera podido evitar.**
- Asegurar no significa Obstaculizar.
- Preguntas y Respuestas

# Y como se hubiera podido evitar

- **Caso 1 (Sony) “Lo que sucedió”**


**Sql Injection**
**anything' OR 'x'='x**

√

**Servidor Web**

**Atacante**

**Internet**

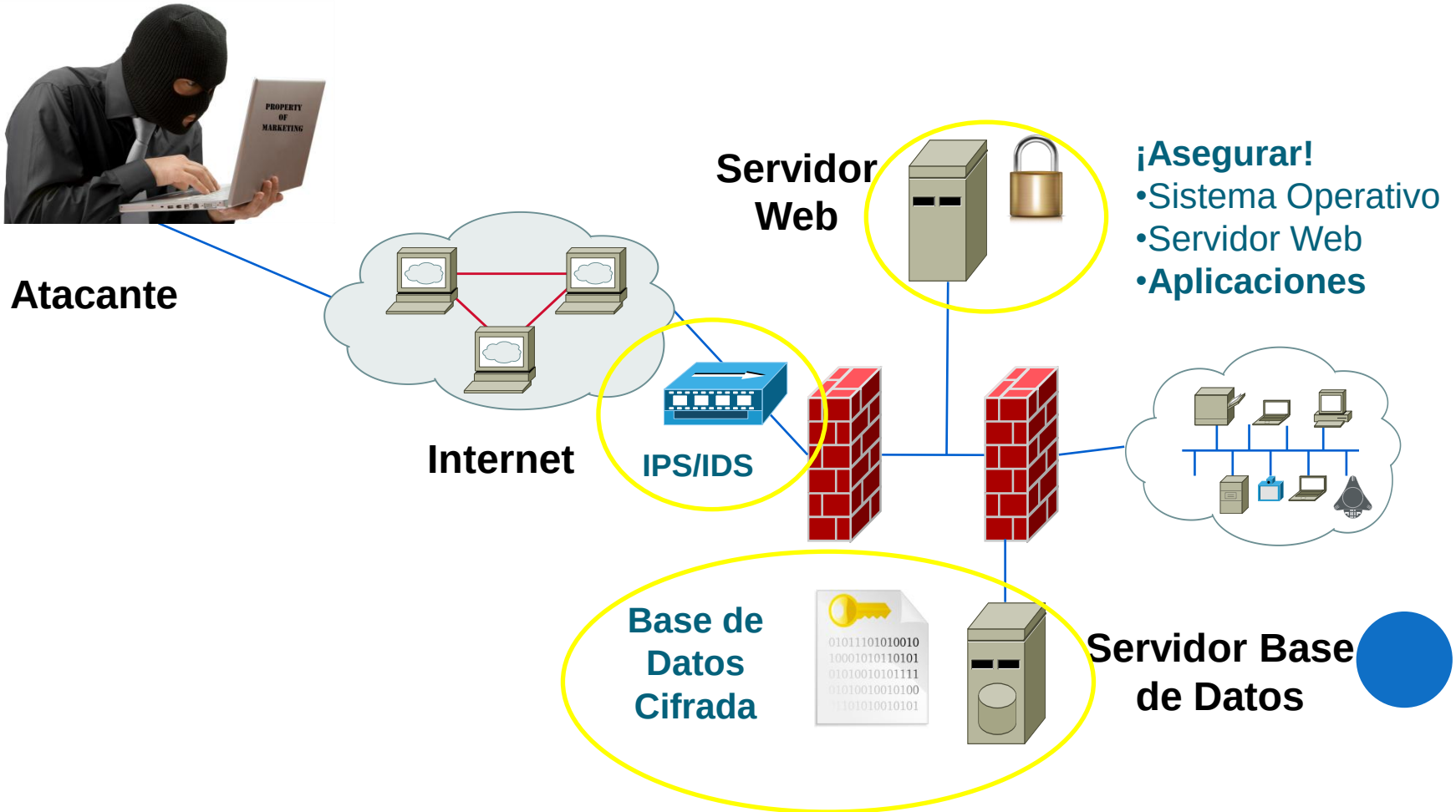
**FW Perímetro**

**Servidor Base de Datos**

**User:** Bob
**password:** 123456
**email:** bobus@mail.com

# Y como se hubiera podido evitar

- **Caso 1 (Sony) “Los controles para evitarlo”**



# Y como se hubiera podido evitar

- Recomendaciones Generales para el aseguramiento de información.

## Tunneling (Comunicaciones Cifradas)

- **Sitios web** que expongan **información sensible** de usuarios en internet, deben estar publicadas usando **protocolos seguros** (SSL) de cifrado .
- Enlaces de **comunicaciones** (LAN/WAN) que transmitan **información sensible** deben estar **cifradas usando protocolos seguros** (IPSEC).


## Almacenamiento en la nube

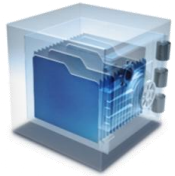
- **No almacenar información Corporativa** en **plataformas abiertas basadas en nube** (DropBox)
- **Información** importante **que se requiera almacenar en la nube**, preferiblemente **debe estar cifrada** antes de transmitirla.

# Y como se hubiera podido evitar

- Recomendaciones Generales para el aseguramiento de información.

**Cifrado de Almacenamiento (Medios Cifrados)**

- Medios externos (**Cintas, discos externos**) con data **importante, debe** utilizar **cifrado con algoritmos fuertes (AES, RSA,etc)**
- Medios **removibles** (USB, Teléfonos Móviles) de **altos directivos** debe preferiblemente **estar cifrados y asegurados**.
- **Laptops corporativas** con **información sensible**, deben tener capacidades de **cifrado con herramientas centralizadas**, que permitan el control de **medios extraíbles**.



**Sistemas de Respaldo (Medios Cifrados)**

- Siempre usar una **herramienta de respaldo** tanto para **data personal como corporativa.**
- **Usar capacidades de cifrado** en los respaldo ofrecidos tanto por las **unidades de Backup** como por las **herramientas**.

# Índice

- A qué estamos expuestos
- Mecanismos para asegurar la información.
- Y como se hubiera podido evitar.
- **Asegurar no significa Obstaculizar.**
- Preguntas y Respuestas

# Asegurar no significa obstaculizar

| Mito | vs | Realidad |
| --- | --- | --- |
| Las medidas de **seguridad obstaculizan** los procesos de negocio. | | Un proceso de negocio **que expone información** sensible, puede ser el **obstáculo del crecimiento** de la compañía. |
| El uso de **medios encriptados dificulta la recuperación** ante incidentes. | | La **recuperación** de data desde un medio encriptado requiere un **proceso técnico serio**, con herramientas acordes la **criticidad de la información** almacenada |
| **El aseguramiento** de plataformas tecnológicas aumenta la **Confidencialidad** e **Integridad** de la información, pero disminuye la **Disponibilidad**. | | Las **medidas de seguridad** aplicadas a una plataforma **aumentan su disponibilidad,** si se tiene en cuenta un **ataque como riesgo** que afecta la misma. |

# Preguntas y Respuestas.

**Q & A**

**Victor Mora Escobar**
**vmora@indracompany.com**