# Gestión de Riesgos de Ciberseguridad

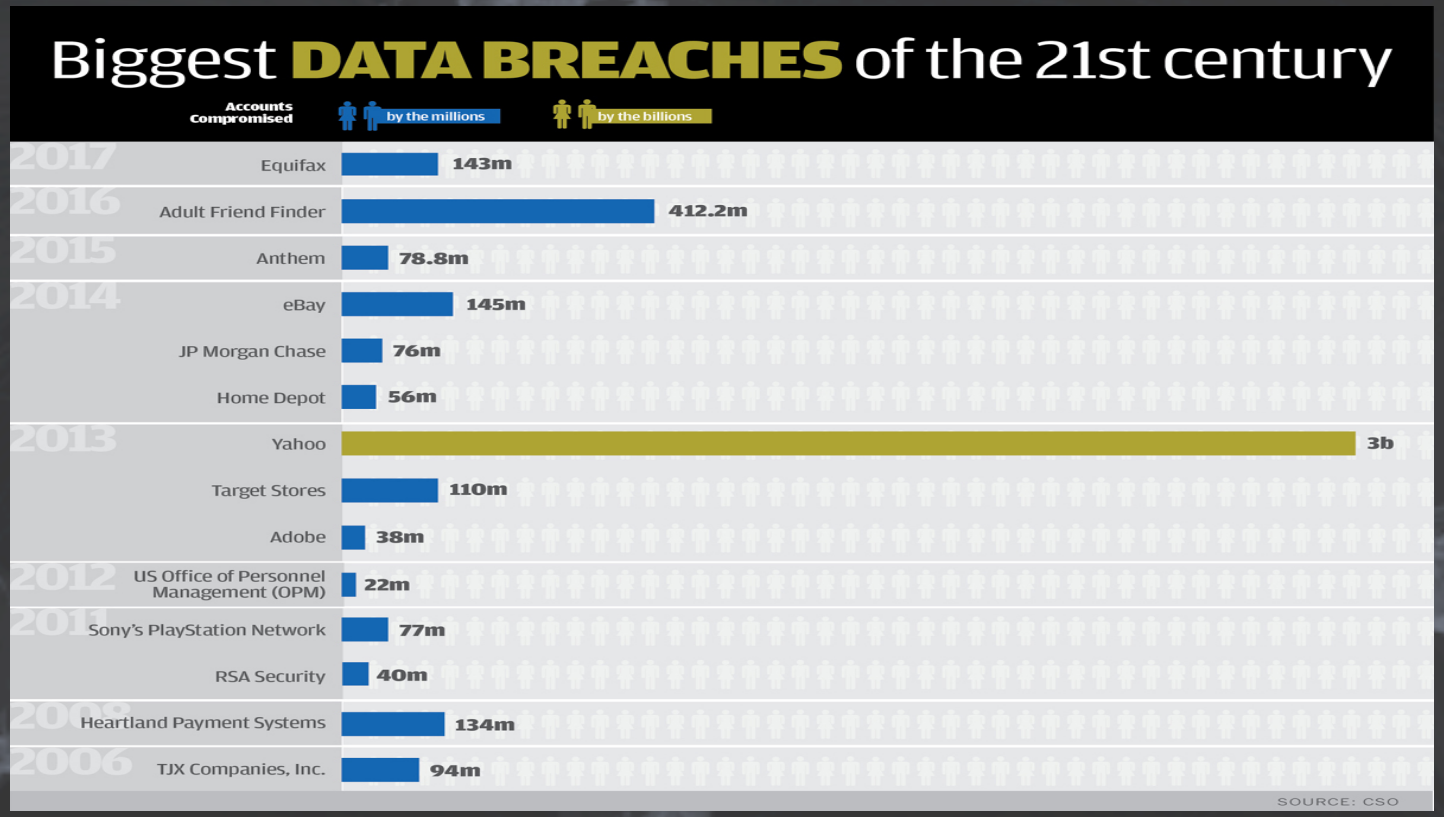

***Jacinto Cofiño***
***Presidente –***
***JC Payment Solutions***
***(jacintocofino@gmail.com)***


- ¿Que estamos tratando de resolver?
- Tendencias de compromisos de datos
- ¿Que y Quien es PCI?
- PCI DSS
- Conclusiones

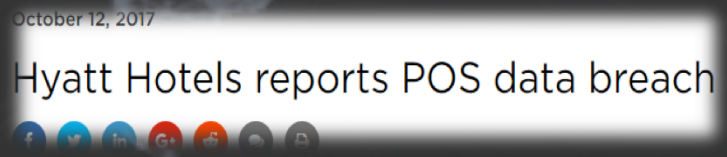
# ¿Que estamos tratando de resolver?

1. Proteger la infraestructura y los ***bienes,*** de ***ataques internos*** y ***externos.***
2. Mantener la ***Confianza*** y la fortaleza de la ***Marca***
3. Crear una Fundación solida que te permita ***crecer tu negocio*** (ej, IOT)

# Tendencias de Compromisos de Datos


Fuente: CSO Online (Jan 2018)


**Chili's restaurants were hit by a data breach that exposed customers' credit-card information**

**Source: Businessinsider.com (5/14/18)**

# Tendencias de Compromisos de Datos

1. 73% perpetrado por actores externos
2. 28% involucró recursos internos
3. 76% fueron motivados por razones financieras
4. 50% fueron dirigidos por grupos criminales organizados
5. 69% de los consumidores de EEUU se preocupan del robo de los datos de medios de pago
6. **Mas del 97% de las entidades comprometidas son comercios pequeños (niveles 3 y 4, como los define las marcas)**
7. **Mas del 60% de los compromisos son causados por:**
   a. **Débil manejo de las claves**
   b. **Débil actualización de mejoras (“parches”)**
   c. **Débil manejo de accesos remotos**

**Fuentes: 2018 Verizon Report (1-4), Gallup (5) Visa public data (6), and PCI council (7)**

# Tendencias de Compromisos de Datos

## Citas notables de Compromisos de Datos…


**Amy Pascal**
Ex CEO de Sony Pictures
"Hubo este momento terrible, cuando me di cuenta que no había nada en lo absoluto que yo podía hacer" USA Febrero del 2015

**Stéphane Nappo**
Jefe Global de Seguridad de la Información en **Société Générale**
International Banking -2018 Global CISO of the year-
**"Toma 20 años el crear una reputación y en unos pocos minutos de un incidente de ciberseguridad arruinarlo"**

**Bryan Sartin**
Director General - Data breach response & forensics - Verizon - Abril 2015
"A menudo los actores claves en una empresa **subestiman** cuan complejo y abrumador puede ser manejar todas las personas auxiliares y grupos que deben manejar un rol en mitigar un compromiso grande, incluyendo **abogados** internos y externos, **investigadores** internos y externos, **agencias policiales**, **reguladores**, aseguradoras y muchos otros"

Fuente: http://www.cyberrescue.co.uk/library/quotes


HOME | ABOUT | SHIPPING/PRICES | CONTACT/ORDER | FEEDBACK

MasterCard VISA

SATISFACTION 100% GUARANTEE

WORLDWIDE SHIPPING

## We are offering top quality cards:

**All our cards come with PINs and instructions. You can use them at any ATM worldwide.**
**Our cards are equiped with magnetic strip and chip.**
**Once you purchase, we will email you a Full Guide on how to safely cash out.**

Us cards - available balance $2,500( minimum) and up to $5,000.
usage:
✓ ATM
✓ Stores
✓ Online

Eu cards - available balance 2,500 Euro(minimum) and up to 4,500 Euro.
usage:
✓ ATM
✓ Stores

Payment methods we accept:

WESTERN UNION MONEY TRANSFERS

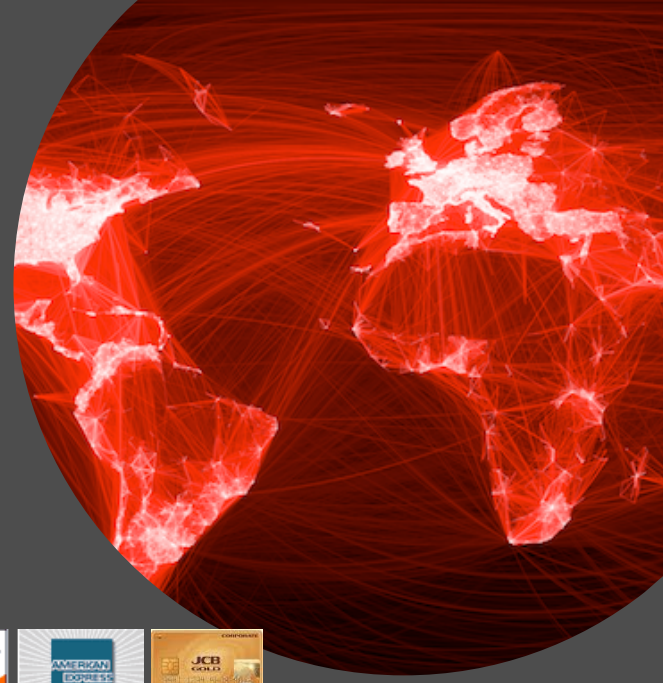
paysafecard

# Credit Card Emporium – Top Quality!

# ¿Que/Quien es PCI?

1. El Consejo de PCI (Payment Card Industry) de Estándares de Seguridad es una ***organización global y abierta***, formada a desarrollar, mejorar, diseminar, y asistir con el entendimiento de estándares de ***seguridad para los medios de pagos***.
2. El Consejo fue fundado en el **2006.**
3. Los miembros fundadores del Consejo son: **American Express, Discover Financial Services, JCB International, MasterCard, y Visa. Estas compañías forman el Comité Ejecutivo del Consejo (PCI SSC).**
4. La Junta de Asesores es formada por expertos de la Industria de Medios de Pago.
5. Los miembros fundadores del Consejo reconocen a los Asesores de Seguridad Calificados (**QSA - Qualified Security Assessors**) **y a los Proveedores Aprobados que ofrecen servicios de "scanning" (ASV - Approved Scanning Vendors).**

# Programa de Cumplimiento de PCI



## ¿Quien es responsable por el Cumplimiento de PCI?

Los estándares aplican a todas las entidades que ***almacenan*** , ***procesan*** o ***transmiten*** datos del tarjetahabiente

PCI Security Standards Council

**Responsable por manejar varios programas de PCI y la certificación de los QSAs**

VISA MasterCard DISCOVER NETWORK AMERICAN EXPRESS JCB GOLD

**Responsables por supervisar el cumplimiento de PCI DSS de todas las entidades y comercios**

**PCI Security & Compliance**

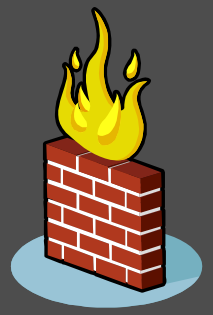
### Bancos Adquirentes

**Comunicar y educar a los comercios. Proveer a las marcas prueba de cumplimiento de sus comercios**

### Comercios y Proveedores de Servicios

**Responsables por proteger los datos de las tarjetas y cumplir con PCI DSS**

# Los 12 Controles de PCI DSS

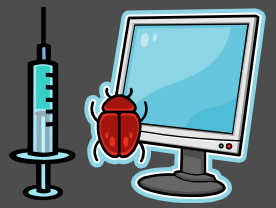


1. Instalar un Firewall

2. Cambiar la configuracion default

3. Almacenar datos de una manera segura

4. Transmitir datos de una manera segura

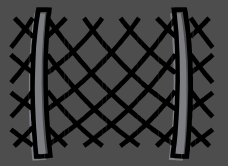


5. Usar Antivirus

6. Mantener los Sistemas y Aplicaciones Seguros

7. Definir usuarios autorizados

8. Utilizar autenticacion fuerte



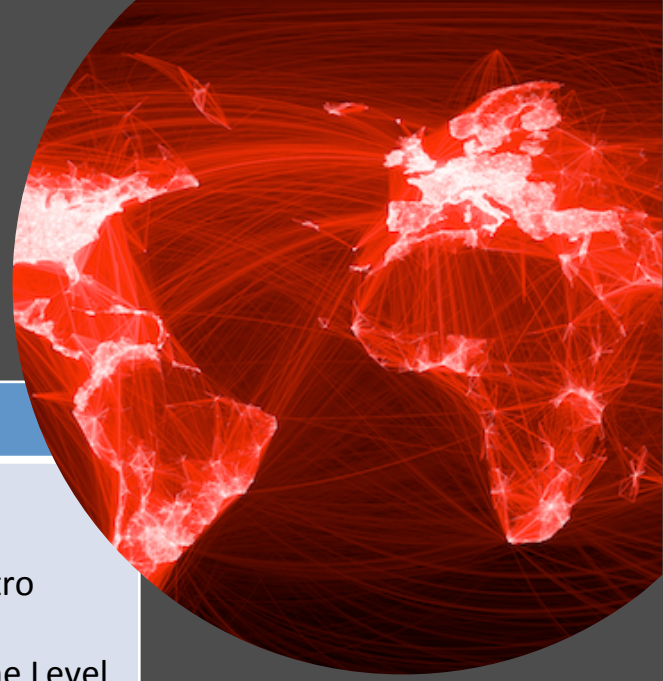
9. Restringir Acceso físico

10. Monitorer cada sistema

11. Probar los sistemas de vulnerabilidades

12. Mantener políticas de seguridad

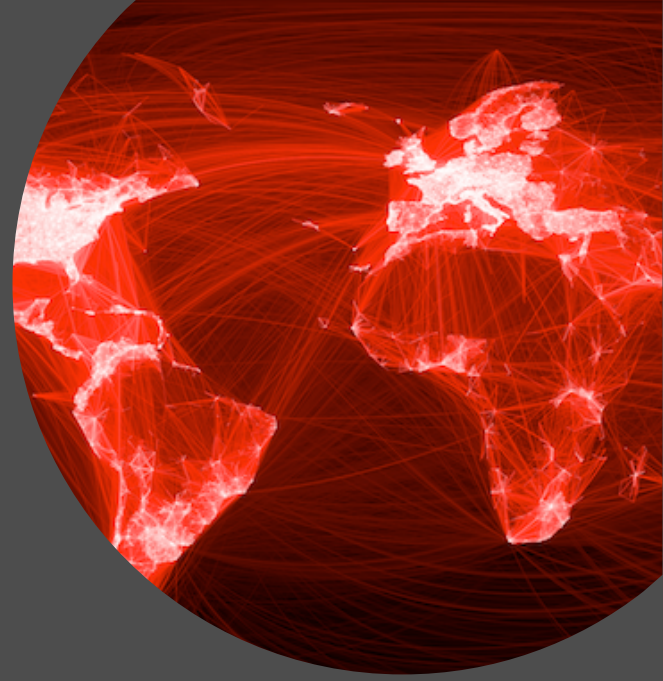
# Niveles de los Comercios



## Niveles de acuerdo a Visa & MasterCard

| Niveles | Criterios |
|---|---|
| 1 | • Any merchant that **has suffered a hack** or an attack that resulted in an account data compromise<br>• Any merchant having more than **six million** total combined Visa, MasterCard and Maestro transactions annually<br>• Any merchant that Visa or MasterCard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system |
| 2 | • Any merchant with more than **one million but less than or equal to six million** total combined Visa, MasterCard and Maestro transactions annually |
| 3 | • Any merchant with more than 20,000 combined Visa, MasterCard and Maestro **e-commerce** transactions annually but **less than or equal to one million** total combined MasterCard and Maestro e-commerce transactions annually |
| 4 | • All other merchants |

# Requerimientos de los Comercios



## Requerimentos de validación – VISA & MC

| Niveles | Validación | Validado por |
|---|---|---|
| 1 | • Annual Onsite Assessment<br>• Quarterly Network Scan | • Qualified Security Assessor (QSA) |
| 2 | • Annual Self-Assessment<br>• Onsite Assessment at Merchant Discretion<br>• Quarterly Network Scan | • Qualified Security Assessor (QSA)<br>• Internal Auditor (ISA) |
| 3 | • Annual Self-Assessment<br>• Quarterly Network Scan | • Merchant or QSA |
| 4 | • Annual Self-Assessment<br>• Quarterly Network Scan | • Merchant or QSA |

# Conclusiones

1. Los “hackers” están atacando a los ***comercios pequeños***
2. El crear ***conciencia*** de la relevancia de la seguridad de los datos (cumplimiento de PCI) ***es un reto*** para los comercios pequeños y medianos
3. Los compromisos fueron dirigidos por grupos criminales organizados con un fin lucrativo
4. La seguridad a veces es percibido como un gasto en vez de una inversión
5. La mayoría de los compromisos pueden ser prevenidos mediante controles sencillos:
   - **manejo de las claves**
   - **actualización de mejoras (“parches”)**
   - **manejo de accesos remotos**
6. **El cumplimiento con PCI *se puede lograr* / el precio de no cumplir es muy alto**
7. La Seguridad de Datos es un ***pilar importante para el crecimiento del negocio***

***“Toma 20 años el crear una reputación..y en unos pocos minutos de un incidente de ciberseguridad arruinarlo..”***

# Gestión de Riesgos de Ciberseguridad


***Jacinto Cofiño***
***Presidente –***
***JC Payment Solutions***
***(jacintocofino@gmail.com)***