

# **Necesitas implantar PCI, ¿Te dijeron qué hacer?**

**Alejandro Bedini G.**

[abedini@nexussa.cl](mailto:abedini@nexussa.cl)



**OWASP**

The Open Web Application Security Project




**OWASP**  
LATIN AMERICA  
TOUR 2012





- Alejandro Bedini G.

[abedinio@nexussa.cl](mailto:abedinio@nexussa.cl)

- Jefe Departamento SPQA 
- Ingeniero y master en Ingeniería Informática con especialización Ingeniería de Software de la UTFSM.
- Postgrado en Management Financiero de la Universidad de Buenos Aires





# Temario

Orientado: GENERAL, SIMPLE,  
FACIL DE COMPRENDER, NO  
ABURRIDO e INTERACTIVO

- Ruta o qué hacer
- Matriz de costo
- Preguntas

# ¿ Qué es PCI-SDI ?



- En particular, el estándar PCI DSS (*Payment Card Industry Data Security Standard*), un estándar de protección de datos del tarjetahabiente establecido por la industria de pagos, exige a toda organización que procese, transmita o almacene datos de tarjeta a cumplir con una serie de requisitos de seguridad en su ambiente. Esto incluye comercios, bancos adquirentes, procesadores de pago y bancos emisores.



# PCI versus OWASP



**OWASP**

The Open Web Application Security Project








Levels	Level 1	Level 2	Level 3	Level 4
<b>Description</b>	<p>Any merchant - regardless of acceptance channel - processing more than 6,000,000 Visa transactions per year</p> <p>Any merchant that has suffered a hack or an attack that resulted in an account data compromise</p> <p>Any merchant identified by any card association as Level 1</p>	<p>1 million - 6 million Visa or MasterCard transactions per year</p>	<p>20,000 - 1 million Visa or MasterCard e-commerce transactions per year</p>	<p>Less than 20,000 Visa or MasterCard e-commerce transactions per year, and all other merchants processing up to 1 million Visa or MasterCards transactions per year</p>
<b>Solutions</b>	<p>For Level 1 merchants, our Compliance Validation Solution (CVS) is comprehensive in scope from document collection and analysis to vulnerability scanning and penetration testing to the final production of the Report on Compliance (ROC). Our PCI DSS validation for Level 1 review includes an on-site evaluation as required by PCI DSS.</p>	<p>For Level 2 and Level 3 merchants, PCI DSS validation includes a SAQ and vulnerability scanning through our on-demand portal, TrustKeeper. In addition, Trustwave assigns a security consultant to work with a retailer after the initial questionnaire and scan are completed.</p>		<p>For Level 4 merchants, Trustwave's TrustKeeper provides the SAQ, vulnerability scanning, if necessary, and remediation services. Sponsored programs have access to Trustwave's Security Policy Advisor, online education and help references and Security Awareness Training.</p>



- **Tarjetas de crédito sufrieron robo de datos en EE.UU**
- Visa y Mastercard confesaron *tremendo hoyo* en seguridad de tarjetas de crédito gringas.
- Tarjetas de crédito, Mastercard y Visa confesaran que hubo un hoyo de seguridad en un periodo de casi un mes que pudo provocar el robo de datos de al menos **10 millones de personas.**

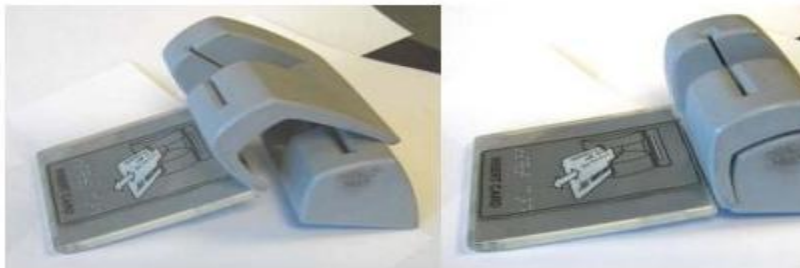
# La Cuarta



- Mastercard derribado por seguidores de Assange, creador de WikiLeaks fuente 



La ranura de lectura de tarjeta real    El dispositivo de captura



El corte lateral no es visible cuando se encuentra en el cajero automático

KNOWLEDGE IS FREE.  
WE ARE ANONYMOUS  
WE ARE LEGION.  
WE DO NOT FORGIVE.  
WE DO NOT FORGET.  
EXPECT US!





## Foco principales



The Open Web Application Security Project



# Justificación



## OWASP

The Open Web Application Security Project



Caso de  
Negocio



Normativa

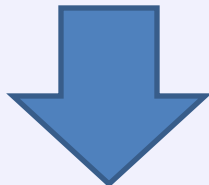


Competencia

Inversión + mantenimiento

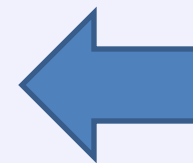


# ¿Qué se hace primero?



Proyecto

Mantenición







# Normalmente qué se hace “Ruta PCI en tu empresa”





### Servidores

- Hardening, parches seguridad, segmento, monitoreo, scan vulnerabilidades, si va almacenar n° de tarjetas.....

### SW

- Encriptación de datos, revisión de código (OWASP) , arquitectura de seguridad.....

### Procesos

- Políticas , normas y procesos de seguridad
- Habilitación de **SO & QSA**, Panel de control de seguridad, Liderar certificación PCI
- .....

# Matriz de costo



ITEM HW	ITEM SW	PROCESOS
Servidores	Revisión de código (manual y/o automático)	Consultor PCI
Segmentos de red “especiales”	Cumplimiento arquitectura de seguridad	SO
Firewalls	Licencias BD encriptación	Gestión del cambio
Antispam	Antispam	Verificación cumplimiento norma
Accesos de seguridad física	Antivirus	Establecer normas de seguridad
Monitoreo de info sensible		
Destrucción de info sensible		
<b>Defina</b>	<b>Defina</b>	<b>Defina</b>

# Preguntas



**OWASP**

The Open Web Application Security Project



- **Alejandro Bedini G.**

- » [www.bedinialejandro.com](http://www.bedinialejandro.com)

- » [abg@bedinialejandro.com](mailto:abg@bedinialejandro.com)