



**SEGURINFO**

VII Congreso Internacional de Seguridad de la Información

"La seguridad agrega valor"

10 y 11 de marzo de 2010 – SHERATON Buenos Aires - Argentina

**Tenemos que cumplir PCI...  
Ahora, ¿qué hacemos?**

organizado por:





**SEGURINFO**

VII Congreso Internacional de Seguridad de la Información

“La seguridad agrega valor”

10 y 11 de marzo de 2010 – SHERATON Buenos Aires - Argentina

**Presentada por:**

**Ing. María del Rosario ROMERO**

Jefe de Seguridad Informática  
Cencosud S.A.

**Ing. Claudio MEOLA**

Consultor Senior  
Cybsec



# Aclaración:



- © Usuaría, 2010. Todos los derechos reservados. No está permitida la reproducción parcial o total del material de esta sesión, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro u otros métodos, sin el permiso previo y por escrito de los titulares de los derechos. Si bien este Congreso ha sido concebido para difusión y promoción en el ámbito de la profesión a nivel internacional, previamente deberá solicitarse una autorización por escrito y mediar la debida aprobación para su uso.

# Agenda



- ◆ ¿Qué es PCI?
- ◆ ¿Quiénes Deben Validar Cumplimiento?
- ◆ PCI Data Security Standard (DSS)
- ◆ El Contexto de Cencosud
- ◆ Cencosud y PCI
- ◆ Reemplazando el Validador de Tarjetas
- ◆ Revisando los Otros Sistemas: La Foto Completa
- ◆ Puntos Claves

# ¿Qué es PCI?



- ◆ El *PCI-DSS (Payment Card Industry - Security Standards Council)* es un organismo internacional que *regula la industria de las tarjetas de pago*, con el fin de concentrar los esfuerzos para minimizar el riesgo de fraudes
- ◆ Se creó en 2006, soportado por las principales empresas de tarjetas de pago (Visa, MasterCard, AmEx, etc.)

# ¿Qué es PCI? (Cont.)



## ◆ Los objetivos del PCI-SSC son:

- Emitir nuevos estándares y administrar su ciclo de vida
- Fortalecer la seguridad en el manejo de cuentas de tarjetas
- Crear conciencia y dirigir la adopción de los estándares
- Fomentar la participación y recabar “feedback”
- Entrenar, testear y certificar
- Proveer una única voz a nivel global sobre la industria



# ¿Quiénes Deben Validar Cumplimiento?



## COMERCIOS

Nivel	VISA Inc	MasterCard	Requisitos
1	Con más de 6.000.000.- de transacciones anuales de VISA o comercios globales identificados como Nivel 1 por VISA fuera de USA	Comercios que procesen más de 6.000.000.- de transacciones MasterCard anualmente, aquellos que sean identificados como Nivel 1 por otra marca, o comercios que hayan experimentado algún compromiso de datos de tarjetas	<ul style="list-style-type: none"> <li>* Auditoría on site anual (QSA)</li> <li>* Escaneos trimestrales (ASV)</li> <li>* Formulario de Testimonio de Cumplimiento (VISA)</li> </ul>
2	Comercios que procesen de 1 a 6 millones de transacciones VISA anualmente	Comercios que procesen de 1 a 6 millones de transacciones MasterCard anualmente o comercios que sean calificados como Nivel 2 en otras marcas	<ul style="list-style-type: none"> <li>* Auditoría on site anual (QSA - MasterCard)</li> <li>* Escaneos trimestrales (ASV)</li> <li>* Formulario de Testimonio de Cumplimiento (VISA)</li> <li>* Cuestionario de Autoevaluación anual (VISA)</li> </ul>
3	Comercios que procesen 20.000 a 1 millón de transacciones VISA e-commerce anualmente	Comercios que procesen 20.000 a 1 millón de transacciones MasterCard e-commerce anualmente o comercios que sean identificados como Nivel 3 por otras marcas	<ul style="list-style-type: none"> <li>* Cuestionario de Autoevaluación anual</li> <li>* Escaneos trimestrales (ASV)</li> </ul>
4	Comercios que procesen menos de 20.000 transacciones VISA e-commerce anualmente, u otros comercios que procesen hasta 1 millón de transacciones VISA anualmente	Los demás comercios que procesen MasterCard	<ul style="list-style-type: none"> <li>* Cumplimiento a discreción del Adquiriente</li> <li>* Cuestionario de Autoevaluación recomendado (VISA)</li> <li>* Escaneos trimestrales realizados por un ASV recomendado (VISA)</li> </ul>

# ¿Quiénes Deben Validar Cumplimiento?(Cont.)



## PROVEEDORES DE SERVICIOS

Nivel	VISA Inc	MasterCard	Requisitos
1	Procesadores de VisaNet o cualquier proveedor de servicio que almacene, procese o transmita más de 300.000 transacciones anualmente	<ul style="list-style-type: none"> <li>* Todos los TPP (Third Party Processor)</li> <li>* Todos los DSE (Data Storage Entities) que almacenen, procesen o transmitan más de 300.000 transacciones anualmente combinadas entre MasterCard y Maestro</li> </ul>	<ul style="list-style-type: none"> <li>* Auditoría on site anual realizada por un QSA</li> <li>* Escaneos trimestrales realizados por un ASV</li> <li>* Formulario de Testimonio de Cumplimiento</li> </ul>
2	Cualquier proveedor de servicio que almacene, procese o transmita menos de 300.000 transacciones anualmente	Todos los DSE (Data Storage Entities) que almacenen, procesen o transmitan menos de 300.000 transacciones anualmente combinadas entre MasterCard y Maestro	<ul style="list-style-type: none"> <li>* Cuestionario de Autoevaluación anual</li> <li>* Escaneos trimestrales realizados por un ASV</li> <li>* Formulario de Testimonio de Cumplimiento</li> </ul>

# PCI Data Security Standard (DSS)



- ◆ Abarcan todas las áreas involucradas en la seguridad del procesamiento de transacciones con tarjetas de pago
  - Categoría 1: Construir y Mantener Redes Seguras
    - 1. Instalar y mantener configuraciones de “firewall” para proteger la información
    - 2. No usar contraseñas o parámetros de seguridad “por default”

# PCI Data Security Standard (DSS) (Cont.)



- Categoría 2: Proteger la Información del Titular de Tarjetas de Pago
  - ▣ 3. Proteger información almacenada
  - ▣ 4. Cifrar datos del titular de tarjetas e información sensible al enviarla por redes públicas
- Categoría 3: Establecer Programas de Pruebas de Vulnerabilidades
  - ▣ 5. Usar y actualizar regularmente soluciones anti-virus
  - ▣ 6. Desarrollar y mantener sistemas y aplicativos seguros

# PCI Data Security Standard (DSS) (Cont.)



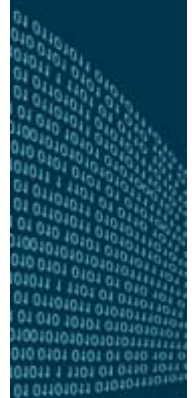
- Categoría 4: Implementar Medidas Fuertes de Control de Acceso
  - ▣ 7. Restringir acceso a información de acuerdo reglas de negocio
  - ▣ 8. Asignar IDs únicos para cada persona con acceso a sistemas
  - ▣ 9. Restringir acceso físico a la información de titulares de tarjetas de pago



# PCI Data Security Standard (DSS) (Cont.)



- Categoría 5: Monitorear y Probar Regularmente el Acceso a la Red
  - ▣ 10. Rastrear y monitorear todos los accesos a la red e información de titulares de tarjetas de pago
  - ▣ 11. Regularmente probar sistemas y procedimientos de seguridad
- Categoría 6: Mantener Políticas de Seguridad de la Información
  - ▣ 12. Establecer políticas dirigidas a la Seguridad de la Información



# El Contexto de Cencosud



## ◆ Quiénes somos?

Uno de los más grandes y prestigiosos conglomerados de retail en América Latina

## ◆ Presencia en:

Argentina, Brasil, Chile, Colombia y Perú



## ◆ Nuestros formatos:

Supermercados, Homecenters, Centros Comerciales, Tiendas por Departamento y Servicios Financieros



# El Contexto de Cencosud (Cont.)



## ◆ Nuestros locales en Argentina:

-  250
-  46

## ◆ Escenario tecnológico:

- Complejo, de gran volumen y variados tipos de equipamientos y aplicaciones

## ◆ Operamos con todas las marcas de tarjetas de crédito, además de la tarjeta propia (Tarjeta Más)

# Cencosud y PCI

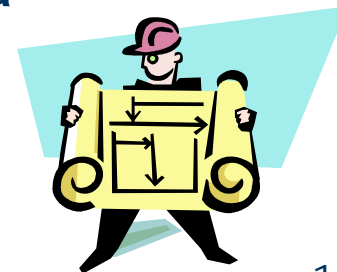


- ◆ Nos encontramos con PCI en dos situaciones diferentes:
  - Reemplazo de la solución de validación de tarjetas (software y plataforma)
  - Auditoría PCI
  
- ◆ En ambos casos utilizamos un enfoque de solución *similar*, pero atendiendo a las *características propias de cada contexto*

# Reemplazando el Validador de Tarjetas



- ◆ Incorporamos PCI en la etapa de Diseño. Se consideró para:
  - La definición de la arquitectura
  - Las parametrizaciones de seguridad de los componentes
  - La construcción de interfaces seguras
  - Adecuado almacenamiento de la información de los propietarios de datos de tarjetas



# Reemplazando el Validador de Tarjetas (Cont.)



◆ Como última fase, previa al cierre del proyecto, se realizó un Gap Analysis:

- Se identificaron desvíos en la implementación para corregir los mismos
- Permitted certificar de manera interna la alineación de la nueva aplicación y su arquitectura a PCI

◆ Lo más importante: ¡un sistema menos por el cual preocuparse!



# Revisando los Otros Sistemas: La Foto Completa



## ◆ Validar PCI en un *contexto complejo*:

- Diversas soluciones para las distintas UNs
- Diferentes tecnologías
- Arquitectura tecnológica con limitantes

## ◆ Primer Paso: *Realizar un Gap Analysis*

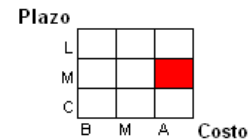
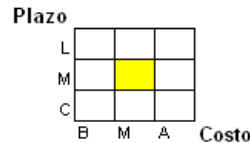
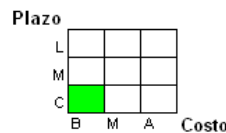
- Nos permitió conocer en qué situación nos encontrábamos
- Identificamos puntos a corregir, ponderando su criticidad



# Revisando los Otros Sistemas: La Foto Completa (Cont.)



- ◆ Segundo Paso: *Clasificar cada ítem según el esfuerzo de corrección en dos dimensiones: plazo y costo*



- ◆ Tercer Paso: *Presentación de los resultados al Negocio priorizados*
- ◆ Cuarto Paso: *Armar un plan de acción y ejecutar el mismo*

# Puntos Claves



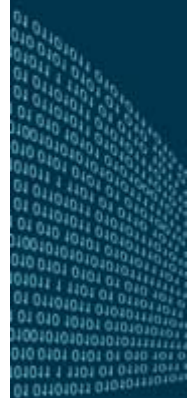
- ◆ Incorporar PCI desde el inicio del proceso: *¡el mejor de los mundos!*
- ◆ Aprovechar las *oportunidades*
  - Oportunidad para regularizar aspectos normativos y procedimentales
  - Implementación de mejoras con el aval del Negocio (obtención de recursos)
  - Buscar sinergia, extendiendo las correcciones a otros ambientes



# Puntos Claves (Cont.)



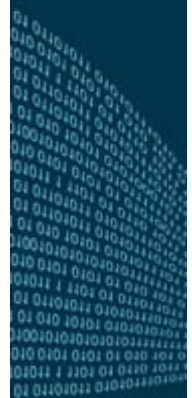
- ◆ La *regularización* de los sistemas existentes suele ser *compleja*, pero hay que tener perseverancia para dar *continuidad* al plan
- ◆ Buscar en PCI un "*aliado*" para poder implementar el cambio y buscar un ambiente más controlado de manera integral



# Gracias por asistir a esta sesión...



## Preguntas y Respuestas...



# Para mayor información:



**Ing. María del Rosario Romero**

rosario.romero@cencosud.com.ar



**Ing. Claudio Meola**

cmeola@cybsec.com

**Para descargar esta presentación visite  
[www.segurinfo.org](http://www.segurinfo.org)**

Los invitamos a sumarse al grupo “Segurinfo” en **LinkedIn**®