PCI-DSS v 3.0: Novedades de Seguridad en Tarjetas de Crédito

Desayuno de trabajo

28 de Octubre de 2014

AGENDA

- Repaso / Introducción
- PCI-DSS v 3.0 - DESTACADOS
- Proceso de Homologación
- Conclusiones

AGENDA

- Repaso / Introducción
- PCI-DSS v 3.0 - DESTACADOS
- Proceso de Homologación
- Conclusiones

¿QUÉ ES PCI-DSS?

Conjunto uniforme de requerimientos de seguridad de la información para todas las marcas de tarjetas.

PCI Security Standards Council™

VISA AMERICAN EXPRESS MasterCard JCB DISCOVER FINANCIAL SERVICES

BDO

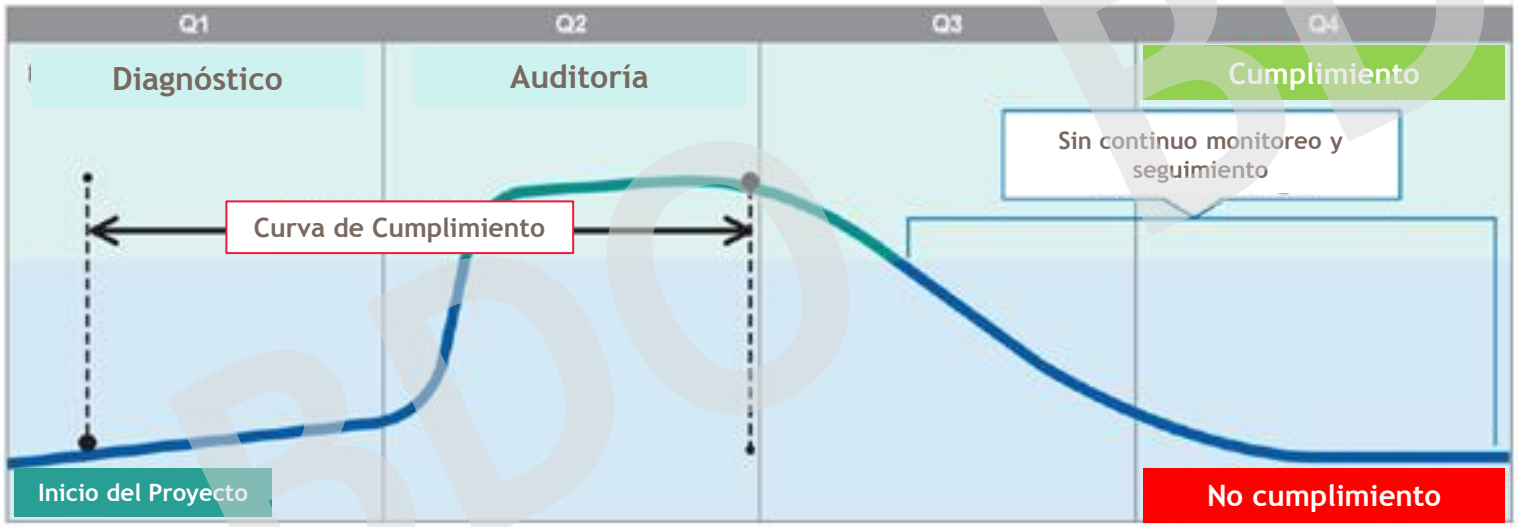
ULTIMA ACTUALIZACIÓN VIGENTE

Noviembre de 2013

¿Y AHORA? ¿QUÉ TENGO QUE HACER CON PCI 3.0?

La buena noticia es que si ya cumplían con la versión anterior de PCI-DSS está usted más cerca de cumplir con la versión 3.0.

Pero….¿Qué esta sucediendo?



(*)Información extraída de PCI_DSS_V3.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance

AGENDA

- Repaso / Introducción
- PCI-DSS v 3.0 – DESTACADOS
- Proceso de Homologación
- Conclusiones

PCI-DSS v 3.0 - DESTACADOS

OBJETIVOS DEL NUEVO ESTÁNDAR

Concientización/Educación: Establecer una cultura de seguridad a través de una mayor educación para mantener e impulsar el cumplimiento en toda la organización.

PCI «*Business as Usual*»: Nueva sección de «Mejores prácticas para la implementación de PCI» con el objetivo de convertirlo en un proceso continuo y no ante cada auditoría.

Responsabilidades compartidas: La nueva versión añade orientación a los proveedores y comerciantes para asegurar que existe una "responsabilidad compartida".

PCI-DSS v 3.0 - DESTACADOS

NUEVOS REQUERIMIENTOS

- Req. 8.2.3 - Complejidad y fortaleza de contraseña mínima combinados en un solo requisito, y el aumento de la flexibilidad en alternativas de igual solidez.

- Req. 8.5.1 (*) - Para los proveedores de servicio con acceso remoto a las instalaciones del cliente, utilice las credenciales de autenticación único para cada cliente.

(*) Mejor practica hasta el 30 de junio de 2015.

PCI-DSS v 3.0 - DESTACADOS

NUEVOS REQUERIMIENTOS

- Req. 8.6 – Contar con otros mecanismos de autenticación (por ejemplo, tokens de seguridad físicos o lógicos, tarjetas inteligentes, certificados, etc.) estos deben ser vinculados a una cuenta individual y garantizan sólo el usuario previsto pueda tener acceso.

- Req. 9.3 - Controlar el acceso físico a las áreas sensibles para el personal, incluyendo un proceso para autorizar el acceso, y revocar el acceso inmediato a la terminación.

PCI-DSS v 3.0 - DESTACADOS

NUEVOS REQUERIMIENTOS (cont.)

- Req. 9.9 (*) - Proteger contra alteración y sustitución a los dispositivos que capturan datos de la tarjeta de pago a través de interacción física directa con la tarjeta.

- Req. 11.3 (*) y 11.3.4 – Requisito para aplicar una metodología de pruebas de penetración internas/externas. Asimismo, si la segmentación se utiliza para aislar el entorno de datos de titulares de tarjetas de otras redes, realizar pruebas de penetración para verificar los métodos de segmentación.

(*) Mejor practica hasta el 30 de junio de 2015.

PCI-DSS v 3.0 - DESTACADOS

NUEVOS REQUERIMIENTOS (cont.)

- Req. 11.5.1 - Proceso para responder a todas las alertas generadas por el mecanismo de detección de cambios (reemplaza a la monitorización de integridad de archivos).

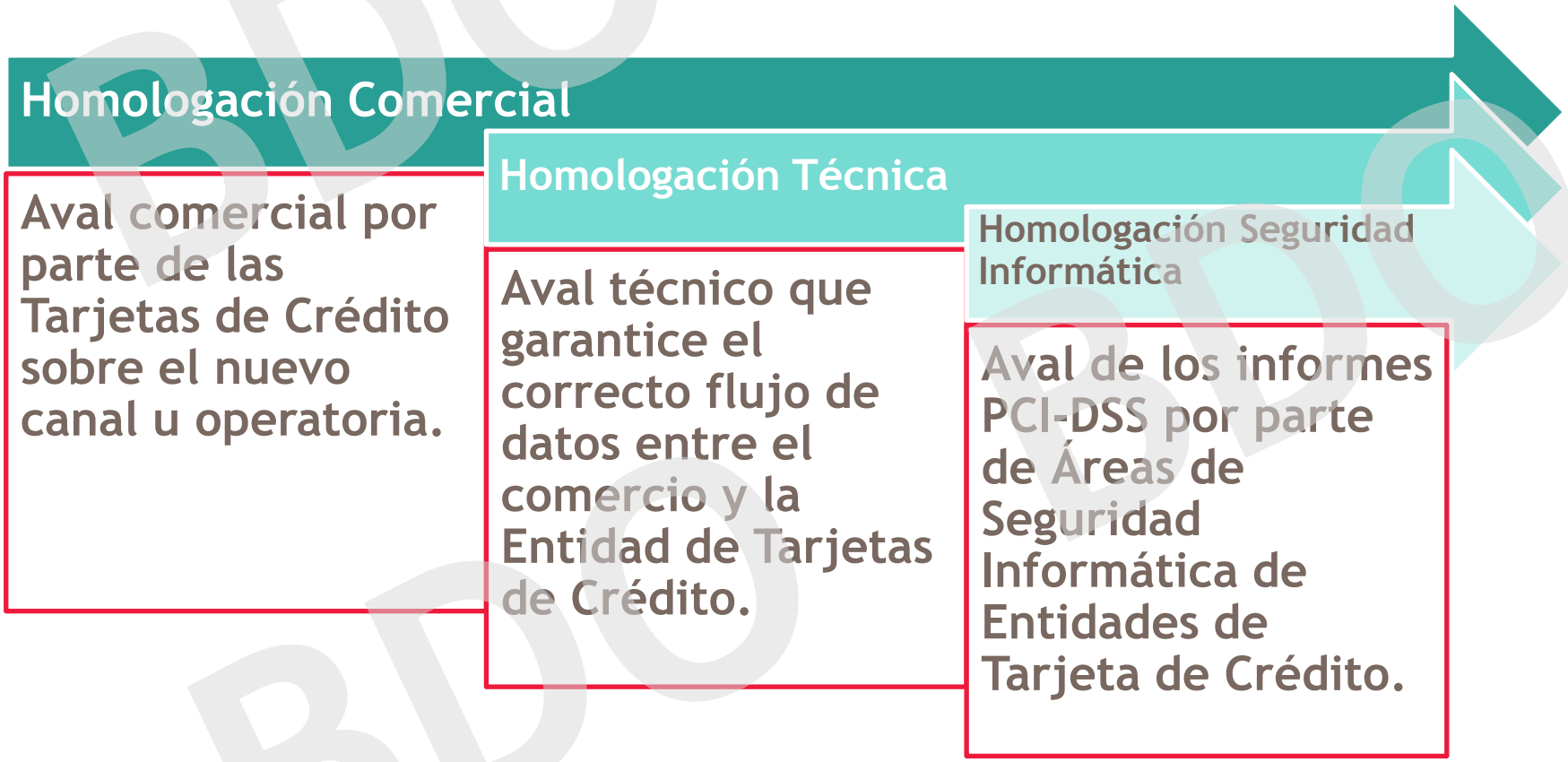
- Req. 12.9 (*) - Para proveedores de servicios; proporcionan el reconocimiento/acuerdo escrito a sus clientes, como se especifica en el requisito 12.8.2.

(*) Mejor practica hasta el 30 de junio de 2015.

AGENDA

- Repaso / Introducción
- PCI-DSS v 3.0 - DESTACADOS
- Proceso de Homologación
- Conclusiones

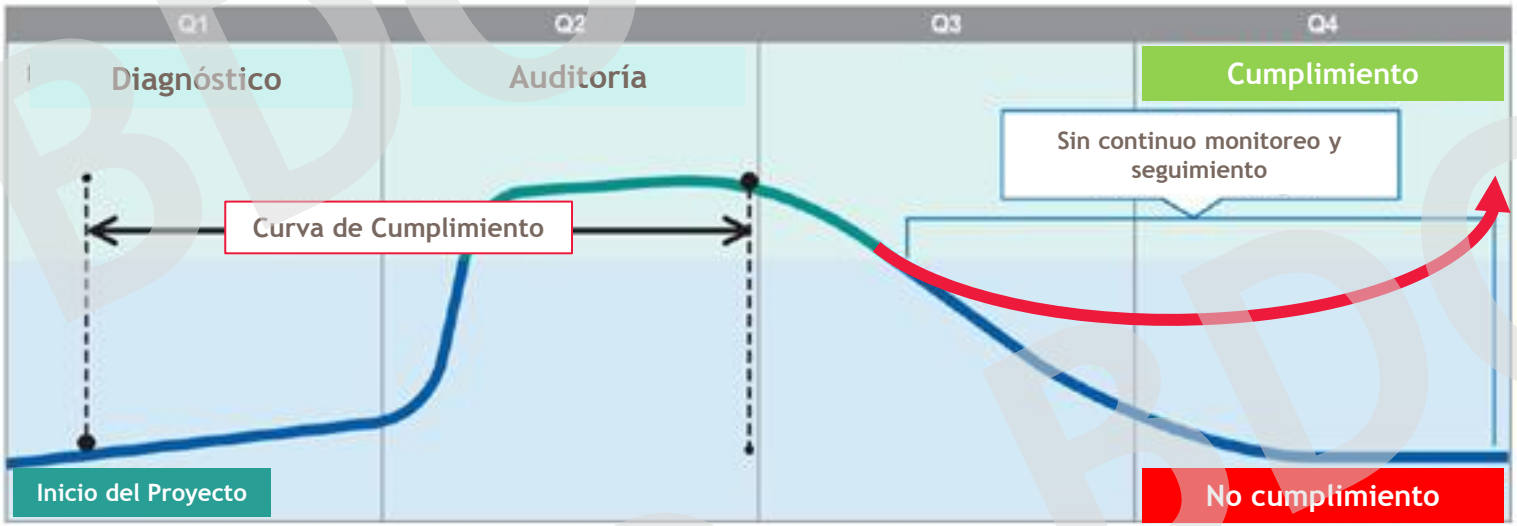
PROCESO DE HOMOLOGACIÓN



AGENDA

- Repaso / Introducción
- PCI-DSS v 3.0 - DESTACADOS
- Proceso de Homologación
- Conclusiones

CONCLUSIONES



CAMBIAR Y MANTENER LA CURVA DE CUMPLIMIENTO DEMANDA ESFUERZOS:

+ procesos operativos/de control
+ recursos
+ inversión

CONCLUSIONES

- Determinar los **sistemas/datos/comunicaciones involucrados** en el flujo y operación con tarjetas;
- Determinar la mejor forma de **limitar/acotar el entorno** de tarjetas;
- Realizar Planes de Remediación realistas y priorizando **temas críticos.**
- **MONITOREO CONTINUO**

¿DUDAS? ¿PREGUNTAS?

¡MUCHAS GRACIAS!

Pablo Silberfich
psilberfich@bdoargentina.com

Leandro Bauso
lbauso.ext@bdoargentina.com

Maipú 942 1° piso
C1006ACN Buenos Aires, Argentina
Tel.: 54 11 4106 7000
Fax: 54 11 4106 7255

www.bdoargentina.com