internet security auditors

PROBLEMÁTICAS DE PCI DSS EN CONTACT CENTERS & BPO

DAVID ANDRÉS GONZÁLEZ LEWIS

CISM, PCI QSA, PA QSA, PCIP, ISO 27001 IA

C. Santander, 101. Edif. A. 2º
E-08030 Barcelona (Spain)
Tel.: +34 93 305 13 18
Fax: +34 93 278 22 48

C. Arequipa, 1
E-28043 Madrid (Spain)
Tel.: +34 91 763 40 47
Fax: +34 91 382 03 96

Calle 90 # 12-28
110221 Bogotá (Colombia)
Tel: +57 (1) 638 68 88
Fax: +57 (1) 638 68 88

info@isecauditors.com
www.isecauditors.com

AGENDA

1. Brechas en los Contact Centers.
2. Principales requerimientos de PCI DSS a implementar.
3. Problemáticas en la implementación de los requerimientos.
4. Soluciones a las problemáticas.
5. Controles PCI DSS en pagos telefónicos.
6. Conclusiones.

BRECHAS DE SEGURIDAD EN CONTACT CENTERS

Caso AT&T:

- Robo de datos (PII y números seguro social) de 68.700.
- Efectuado en el proveedor de servicio de Contact Center.
- Afecto en México, Colombia y Filipinas.
- Falta de monitoreo sobre acceso y consulta de información sensible.
- Falla en el proceso de contratación de personal. (revisión de antecedentes)

Talk – Wipro:

- Robo de datos (PII y números de cuenta) de 157.000 clientes.
- Efectuado en el proveedor de servicio de Contact Center Wipro.
- Tres empleados encargados de la red.
- Falta de monitoreo sobre acceso y consulta de información sensible.
- Falla en el proceso de contratación de personal. (revisión de antecedentes).
- Falta de controles de acceso a segmentos de red sensibles.

BRECHAS DE SEGURIDAD EN CONTACT CENTERS

Contact Solutions:

- Robo de datos de los empleados.
- Ataque de phising dirigido a los empleados.
- Falta de concientización al personal.

Advanced Tech Support:

- Acceso no autorizado a equipos de asesores de llamadas inbound.
- Robo de cuentas e información de clientes.
- Mala configuración de seguridad en componentes perimetrales y equipos.

REQUERIMIENTOS DE PCI DSS – MAYORES RETOS

- No almacenar después de la autorización datos sensibles de autenticación (SAD): CAV2, CVC2, CVV2, CID. **Requerimiento 3.2.**
- Proteger datos de tarjetahabiente en almacenamiento (PAN). **Requerimiento 3.4.**
- Enmascarar PAN de acuerdo a la necesidad de conocer (1234********6789). **Requerimiento 3.3.**
- Limitar el trafico de entrada y salida al ambiente de datos de tarjetahabiente (CDE). **Requerimiento 1.3.**
- Asegurar componentes y mantenerlos actualizados con parches de seguridad(servidores, redes, equipos, etc.). **Requerimiento 2 y 6.1.**

PROBLEMATICAS AL IMPLEMENTAR REQUERIMIENTOS

Centrales Telefónicas:

- No se incluye seguridad en el diseño de la solución.
- Interfaces de administración no protegidas. Teléfonos SIP contraseñas débiles.
- PBX conectados a internet o con servicios no relacionados.

Grabación de llamadas:

- Información sensible dictada al asesor.
- Los tonos son incluidos en la grabación.

PROBLEMATICAS AL IMPLEMENTAR REQUERIMIENTOS (*)

Ambientes:

- Diferentes campañas sobre el mismo ambiente.
- Asesores con acceso a información sensible.
- Redes no segmentadas.
- Diferentes tecnologías y aplicaciones dependiendo de cada cliente.

Personal:

- Negocios con alta rotación de personal.
- Falta de capacitación y concientización en seguridad de la información dependiendo del cargo.
- Poca validación de antecedentes de empleados.

SOLUCIONES A PROBLEMATICAS

Centrales Telefónicas:

- Proteger la interfaz administrativa y tener contraseñas fuertes en los teléfonos SIP.
- Diseño de solución incluyendo seguridad:
  - Reducir riesgos a nivel aceptable
  - Asegurar componentes
  - Diseño simple
- No exponerse a redes no confiables.
- Servidor dedicado.
- Componentes asegurados y actualizados.

SOLUCIONES A PROBLEMATICAS (*)

Grabación de Llamadas:

- Implementar sistemas IVR para capturar información sensible.
- No almacenar los tonos o implementar soluciones para enmascarar la información sensible en la grabación.

Ambientes:

- Separar las campañas dependiendo de la información que usa.
- Control de acceso a información sensible de acuerdo a la necesidad de conocer.
- Segmentar las redes del CDE.
- Configurar componentes de cliente de forma segura.

SOLUCIONES A PROBLEMATICAS (*)

Personal:

- Capacitar y concientizar en seguridad de la información al momento de la contratación y realizar refuerzos periódicamente.
- Definir accesos a componentes de acuerdo a la necesidad de conocer basado en funciones del cargo.
- Validar antecedentes y referencias de los empleados.

SOLUCIONES A PROBLEMATICAS (*)

Personal:

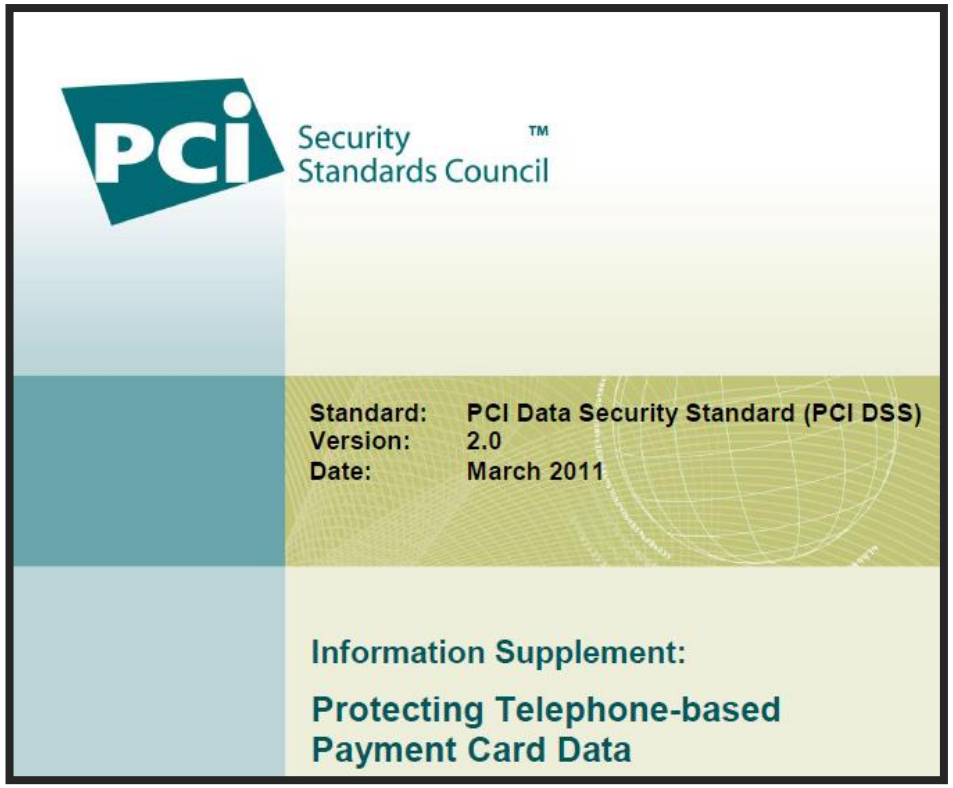
- No permitir el uso de papel.
- Controlar el uso de dispositivos electrónicos dentro de las áreas sensibles.
- Tecnologías para prevenir el uso de capturas de pantalla.
- No permitir correos salientes a destinatarios no controlados.
- CCTV.

SOLUCIONES A PROBLEMATICAS (*)

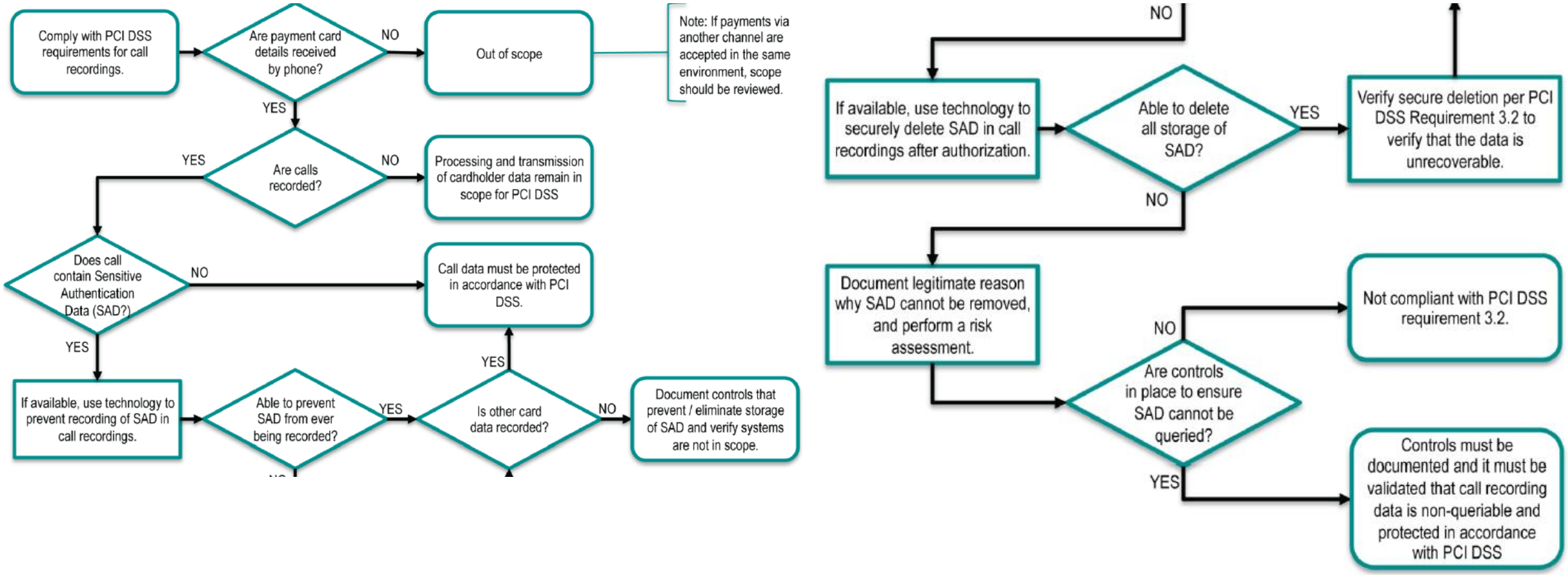
SI NO SE PUEDE CUMPLIR CON UN CONTROL ORIGINAL, SE PUEDE IMPLEMENTAR UN CONTROL COMPENSATORIO

- Monitoreo de repositorios.
- DLP.
- Multi-factor para consultas a información sensible.
- Firewalls locales en componentes.
- Aislamiento de áreas que tratan datos sensibles.

CONTROLES PCI DSS EN PAGOS TELEFÓNICOS



CONTROLES PCI DSS EN PAGOS TELEFÓNICOS (*)



CONTROLES PCI DSS EN PAGOS TELEFÓNICOS - TIPS

Asegurar políticas de retención:

- Almacenar datos de tarjetahabiente solo si es necesario y limitar el tiempo de almacenamiento de acuerdo a requerimientos de negocio.
- No almacenar SAD luego de la autorización.

Enmascarar el PAN:

- Acceso al PAN completo debe garantizarse basado en la necesidad de conocer.
- Segmentar operaciones de las campañas para que solo pocos agentes puedan ingresar el PAN,
- Implementar soluciones en las que el agente no tenga acceso al PAN. (IVR). De no ser posible, enmascarar el PAN luego de ingresarlo en la aplicación.

CONTROLES PCI DSS EN PAGOS TELEFÓNICOS – TIPS (*)

Almacenamiento del PAN:

- El PAN debe almacenarse ilegible mediante:
  - Tokenización
  - Hashing
  - Truncado
  - Cifrado
- Proteger el PAN en Grabaciones, en caso de tenerlo no reproducir las grabaciones

Cifrado de datos en redes públicas:

- Utilizar protocolos de cifrado fuerte como TLS 1.2, SSH, IPSec.
- No enviar CHD por tecnologías de usuario final (SMS, email).

CONTROLES PCI DSS EN PAGOS TELEFÓNICOS – TIPS (*)

Autenticación adecuada para el personal:

- Restringir accesos a grabaciones, y bases de datos con datos de tarjetahabiente.
- Implementar control de acceso multi-factor para conexiones remotas.
- No usar cuentas compartidas.

Política de Seguridad:

- Implementar procedimientos operacionales.
- Políticas de uso de tecnologías.
- Concientizar en seguridad a los empleados (incluidos los remotos) y validar los antecedentes y referencias.
- Prohibir a empleados remotos copiar o mover información a equipos locales.

CONTROLES PCI DSS EN PAGOS TELEFÓNICOS – TIPS (*)

Se deben cumplir todos los requerimientos de PCI DSS, incluidos:

- Autenticación fuerte a sistemas que almacenan información de tarjetahabientes.
- No conexiones a internet entre componentes que almacenan CHD e internet.
- Asegurar que los sistemas mantengan configuraciones seguras, actualizados y sean probados en contra de vulnerabilidades.
- Equipos de personal remoto y portátiles tenga firewall personal instalado.
- Equipos de personal remoto cuente con antivirus instalado.
- Solo se deben utilizar componentes autorizados.

CONCLUSIONES

- Se debe tener especial cuidado con el tratamiento de datos de tarjetahabiente por las diferentes fuentes en las que se puede recibir el dato.
- En las grabaciones no se debe tener el PAN almacenado.
- Hay que tener especial cuidado con el personal dado que es un eslabón débil.
- Se debe cumplir con PCI DSS inclusive si se es utilizado componentes del cliente.
- Los CC y BPOs son proveedores de servicio, deben estar en cumplimiento pero son

internet
security
auditors

C. Santander, 101. Edif. A. 2º
E-08030 Barcelona (Spain)
Tel.: +34 93 305 13 18
Fax: +34 93 278 22 48

C. Arequipa, 1
E-28043 Madrid (Spain)
Tel.: +34 91 763 40 47
Fax: +34 91 382 03 96

Calle 90 # 12-28. Bogotá
(Colombia)
Tel: +57 (1) 638 68 88
Fax: +57 (1) 638 68 88

info@isecauditors.com
www.isecauditors.com

internet
security
auditors

C. Santander, 101. Edif. A. 2º
E-08030 Barcelona (Spain)
Tel.: +34 93 305 13 18
Fax: +34 93 278 22 48

C. Arequipa, 1
E-28043 Madrid (Spain)
Tel.: +34 91 763 40 47
Fax: +34 91 382 03 96

Calle 90 # 12-28. Bogotá
(Colombia)
Tel: +57 (1) 638 68 88
Fax: +57 (1) 638 68 88

info@isecauditors.com
www.isecauditors.com