



# Administración de eventos y logs

## E-Global

Las empresas que manejan información de tarjetahabientes requieren cumplir con PCI, de ahí surge la necesidad de contar con herramientas que apoyen este proceso.

## Caso de Referencia

### Situación

E-Global opera las transacciones electrónicas de tarjetas de crédito para los principales bancos del país, por lo tanto maneja la información de los tarjetahabientes de dichas transacciones.

A nivel mundial existe un esfuerzo por parte de los principales proveedores de tarjetas como VISA, MASTERCARD, AMERICAN EXPRESS para proteger la información de los tarjetahabientes, este esfuerzo ha sido consolidado por medio de una regulación llamada PCI (Payment Card Industry Standard).

Dicha regulación exige a los bancos, a los operadores de transacciones y los retailers cumplir con ciertos mecanismos que mejoren la seguridad en la protección del ciclo de vida de la información de los tarjetahabientes.

Dado lo anterior E-Global requiere de tecnología para monitorear y correlacionar la actividad en su infraestructura tecnológica y generar las evidencias necesarias para el cumplimiento de la regulación de PCI.

### Proyecto

ARAME, empresa de Grupo SCANDA, ofreció una alternativa de solución de Administración de eventos y logs para la infraestructura de E-Global.

Por medio de esta tecnología E-Global tiene la capacidad de monitorear los logs y eventos de servidores, equipos de usuarios, infraestructura de red, infraestructura de seguridad y aplicaciones que están involucradas en el proceso de vida de la información de los tarjetahabientes. Gracias a esta funcionalidad se pueden detectar comportamientos fuera de políticas respecto al manejo de la información.

La herramienta integrada también brinda la facilidad de almacenar los logs para fines de auditoría por los periodos de tiempo que marca la regulación y los puede enviar a unidades de almacenamiento externo para futuras consultas.

Y algo muy importante es que esta solución maneja de forma pre configurada los reportes requeridos por PCI, lo cual facilita el trabajo de auditoría y de los administradores de sistemas.

### Perfil del Cliente

E-Global es el Swith de transacciones de medios de pago más grande en el mercado mexicano, la cual procesa las transacciones de tarjetas de crédito y débito de las principales Instituciones Financieras del País.

### Problemática

E-Global cuenta con servidores, equipos de computo, infraestructura de red, infraestructura de seguridad y aplicaciones que manejan información de tarjetahabientes, y dadas las funciones de la empresa requieren cumplir con la regulación de PCI.

PCI involucra 12 requerimientos para robustecer la seguridad y cumplir con la protección de datos de tarjetahabientes.

Para cumplir con estos requerimientos E-Global requiere de alguna herramienta que le permita el monitoreo de logs y eventos de la arquitectura de TI involucrada y el almacenamiento de los mismos por un periodo de tiempo específico.

También requiere generar las huellas y reportes necesarios para las auditorías de cumplimiento de la regulación de PCI

### Oferta

La solución implementada fue un appliance de administración y correlación de eventos y logs:

- RSA enVision

El equipo de RSA enVision brinda la facilidad de coleccionar los logs de cualquier dispositivo IP que se encuentre en la red, su arquitectura le permite funcionar sin la necesidad de instalar colectores en cada dispositivo a monitorear y maneja el almacenamiento de logs por medio de una tecnología propietaria (IPDB) que lo hace eficiente y rápido, a diferencia de soluciones que emplean bases de datos relacionadas para el almacenamiento.

RSA enVision maneja más de 20 reportes pre configurados respecto al cumplimiento de PCI, lo que facilita las funciones para administración y auditoría, también cuenta con la capacidad de almacenar los logs y enviarlos a un dispositivo externo de acuerdo a las políticas de ciclo de vida de la información que se le configuren.

### Beneficios

Colectión de logs—eventos de la infraestructura involucrada con información de tarjetahabientes de manera sencilla, esta incluye servidores, equipos de usuarios, firewalls, IPS y aplicaciones.

Emisión de reportes de operación y auditoría de manera automática.

Reducción de costos de operación y administración al no requerir de recursos dedicados al filtrado y revisión de logs y a la generación de reportes.

Apoyo en el Cumplimiento de los reportes de los requerimientos de PCI: 1,2,3, 4 y 5.

Apoyo en el Cumplimiento de seguimiento y monitoreo del requerimiento de 10 de PCI.

Ayuda para que el área de seguridad reduzca los tiempos de revisión y correlación de incidentes de seguridad.