Cumplimiento de PCI DSS

8 Mar 2025 / JORGE MACARIO

Complete

Score	1 / 1 (100%)	Flagged items	1	Actions	0

Fecha	08.03.2025 15:16 CST
Realizado por:	JORGE MACARIO
Ubicación	7A Avenida 15-46, Cdad. de Guatemala, Guatemala (14.6327592, -90.5139319)

Flagged items

1 flagged

Inspección / Seguridad del sistema de punto de venta (Ask POS Vendor)

¿Se han cambiado las configuraciones y contraseñas predeterminadas en los sistemas y bases de datos que forman parte del sistema POS?

No

Inspección	1 flagged, 1 / 1 (100%)
Fallas comunes de control de PCI DSS	
Almacenamiento de datos de autenticación confidenciales (SAD), como datos de seguimiento, después de la autorización. **¿Su sistema almacena estos datos? Si es así, ¿está al tanto de ello?**	Si
¿Se cambiaron las configuraciones y contraseñas predeterminadas del sistema cuando se instaló el sistema?	No
¿Se eliminaron o aseguraron servicios innecesarios e inseguros cuando se instaló el sistema?	Si
¿Se han comprobado aplicaciones web mal codificadas que podrían provocar inyecciones de SQL y otras vulnerabilidades que permitan el acceso a la base de datos que almacena los datos del titular de la tarjeta directamente desde el sitio web?	No
¿Ha comprobado si hay parches de seguridad faltantes o desactualizados?	Si
¿Se han comprobado los protocolos de registro adecuados?	No
¿Se verificó que la supervisión sea adecuada (a través de revisiones de registros, detección/prevención de intrusiones, análisis de vulnerabilidad trimestrales y sistemas de supervisión de integridad de archivos)?	Si
Seguridad del sistema de punto de venta (Ask POS Vendor)	1 flagged
¿Se han cambiado las configuraciones y contraseñas predeterminadas en los sistemas y bases de datos que forman parte del sistema POS?	No
¿Accede a mi sistema POS de forma remota?	Si
Si es así, ¿ha implementado controles adecuados para evitar que otros accedan a mi sistema POS, como utilizar métodos de acceso remoto seguros y no utilizar contraseñas comunes o predeterminadas?	No
¿Se han eliminado todos los servicios innecesarios e inseguros de los sistemas y bases de datos que forman parte del sistema POS?	Si
¿Mi software POS está validado según el Estándar de Seguridad de Datos de Aplicaciones de Pago (PA-DSS)?	No

¿Mi software POS almacena datos de autenticación confidenciales, como datos de seguimiento o bloqueos de PIN?	Si

Si es así, este almacenamiento está prohibido: ¿con qué rapidez pueden ayudarme a eliminarlo?

Se debe de realizar el procedimiento el vo.bo del jefe de operaciones

¿Mi software POS almacena números de cuenta principales (PANs)?	Si

Si es así, es necesario proteger este almacenamiento: ¿cómo protege el POS estos datos?

Si con el cifrado.

¿Documentarías la lista de archivos escritos por la aplicación con un resumen del contenido de cada archivo para verificar que los datos prohibidos mencionados anteriormente no se almacenen?	Si
¿Mi software POS aplica contraseñas complejas y únicas para el acceso de todos los usuarios?	No
¿Puede confirmar que no utiliza contraseñas comunes o predeterminadas para acceder a mi sistema y a otros sistemas comerciales que admite?	Si
¿Todos los sistemas y bases de datos que forman parte del sistema POS han sido parcheados con todas las actualizaciones de seguridad aplicables?	No
¿Está activada la capacidad de registro para los sistemas y bases de datos que forman parte del sistema POS?	No
Si las versiones anteriores de mi software de punto de venta almacenaban datos de autenticación confidenciales, ¿se ha eliminado esta función durante las actualizaciones actuales del software de punto de venta? ¿Se utilizó una utilidad de borrado seguro para eliminar estos datos?	No

Datos del titular de la tarjeta

1 / 1 (100%)

Las reglas de marca de pago permiten el almacenamiento del número de cuenta principal (PAN), la fecha de vencimiento, el nombre del titular de la tarjeta y el código de servicio.

¿Es absolutamente necesario el almacenamiento de estos datos para la empresa y su finalidad? Indique por qué se deben almacenar o eliminar los datos.

No es necesario.

¿Vale la pena el riesgo de que los datos se vean comprometidos y el esfuerzo de almacenarlos?	Si

¿Valen la pena los controles PCI DSS adicionales que deben aplicarse para proteger los datos a fin de continuar almacenándolos?	Si
¿Valen la pena los esfuerzos de mantenimiento continuos para seguir cumpliendo con PCI DSS a lo largo del tiempo el almacenamiento continuo de estos datos?	Si
Los datos del titular de la tarjeta que NECESITAN almacenarse se consolidan y aíslan adecuadamente mediante una segmentación de red adecuada.	☑

Aprobación del oficial de cumplimiento	
Nombre completo y firma del Oficial de Cumplimiento a cargo	Ernesto Ramirez