REQUISITO 6 DE PCI DSS: “DESARROLLO SEGURO DE LOS SISTEMAS Y APLICACIONES”

Te presentamos los errores más comunes que afectan al cumplimiento del requisito 6 del estándar PCI DSS, y recomendaciones para asegurarlo.

A modo de contextualización, a continuación, se hace mención, de manera general, de los controles comprendidos en el requisito 6 sobre el Desarrollo Seguro:

• CONTROLES REQUISITO 6

- Desarrollar aplicaciones de software internas y externas de manera segura de acuerdo con PCI DSS, basadas en las normas o en las mejores prácticas de la industria.
- Incorporar la Seguridad de la Información durante todo el ciclo de vida del desarrollo del software.
- Revisar el código personalizado antes de enviarlo a producción.
- Separar los entornos de desarrollo/prueba de producción.
- Capacitar a los desarrolladores en técnicas de desarrollo seguro.
- Desarrollar aplicaciones basadas en directrices de codificaciones seguras (por ejemplo, OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.)

Con relación a los controles determinados precedentemente, se identifican los siguientes como los errores más comunes que cometen las empresas en el cumplimiento del requisito 6 son:

• ERRORES

- No incorporar la Seguridad de la Información desde la definición de requisitos y el diseño de la aplicación.

- No contar con evidencia de que la Seguridad de la Información ha sido considerada durante todo el ciclo de vida del desarrollo.
- Adquirir aplicaciones de terceros que no han sido desarrolladas de manera segura acorde a lo que establece PCI DSS o PA DSS.
- Las personas a cargo del desarrollo de la aplicación desconocen de buenas prácticas de codificación segura.
- Las personas a cargo de las revisiones de código carecen de conocimientos suficientes de prácticas de codificación segura.
- El desarrollo de la aplicación se pasa al ambiente de producción sin haber revisado que el código haya sido desarrollado siguiendo las directrices de codificación segura.
- La aplicación pasa al ambiente de producción sin haber resuelto las vulnerabilidades detectadas durante la revisión de código seguro.
- Los datos de producción se usan en el entorno de desarrollo/prueba.
- Al realizar un cambio significativo en la aplicación, no se identifican ni se implementan todos los requisitos pertinentes de PCI DSS.

Frente a esto, son considerados factores claves de éxito para cumplir con el Requisito 6:

• FACTORES CLAVE DE CUMPLIMIENTO

- Establecer un marco de gobierno de desarrollo seguro de las aplicaciones que comprende: políticas, estrategias, métricas, procedimiento de desarrollo seguro según estándares internacionales aceptados por la industria.
- Considerar los requisitos de seguridad desde la definición y el diseño de la aplicación. Es muy importante realizar la evaluación de riesgos y revisar la arquitectura de seguridad.
- Establecer procesos en que se incluya la Seguridad de la Información en todo el ciclo de vida del desarrollo.
- En caso de adquirir aplicaciones de terceros se debe asegurar de que se encuentre en cumplimiento de PCI DSS y PA DSS o PCI SSF (evolución del PA DSS). Estos dos últimos

estándares aplican generalmente para software que se vende e instala “en forma estándar” sin demasiada personalización.

- Mantener evidencias (Sistema de tickets, correos, actas, formatos de requerimientos, plantillas de pruebas, informes, reportes de herramientas, etc.) que permitan acreditar que la Seguridad de la Información se incluye en todo el ciclo de vida de desarrollo.

- Realizar pruebas de seguridad o ethical hacking, que incluyan la verificación de las vulnerabilidades de codificación comunes, cuando la aplicación se encuentre en la fase de prueba; aunque, también sería recomendable realizarla durante la fase de desarrollo.

- Revisar que el código de la aplicación cumpla con las directrices de codificación segura; por ejemplo, OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.

- Capacitar al personal a cargo del desarrollo y a los responsables de la revisión de código en “codificación de desarrollo seguro” con la finalidad de que puedan identificar y solucionar los problemas relacionados con las vulnerabilidades de codificación comunes u otras que pueden ser aprovechadas por un atacante.

Obtenido de: https://www.pcihispano.com/errores-comunes-y-factores-claves-de-exito-en-el-cumplimiento-del-requisito-6-de-pci-dss-desarrollo-seguro/