Un panorama general sobre los comentarios recibidos respecto a la versión 4.0 del PCI DSS

El PCI SSC recientemente concluyó la revisión de más de los 3,000 comentarios recibidos el año pasado en respuesta a la primera RFC sobre PCI DSS versión 4.0. Esta RFC estableció un récord en cuanto al número de comentarios emitidos por la industria con respecto a un conjunto de normas del PCI SSC y fue la primera vez que la industria revisó un borrador de trabajo del PCI DSS. Se planea lanzar a fines de este año otra RFC sobre el borrador de la norma. Este enfoque colaborativo da a las partes interesadas una verdadera oportunidad de contribuir a la elaboración de la nueva versión.

Puede conocer más detalles del cronograma de elaboración de PCI DSS versión 4.0 en esta **publicación del blog**.

Comentarios relativos a las actualizaciones de requisitos propuestas
En el borrador de PCI DSS versión 4.0 para RFC de 2019 se propusieron nuevos requisitos y cambios en los existentes. La intención de las actualizaciones era abordar la evolución de los riesgos y amenazas relacionados con los datos de pago, brindar flexibilidad a las partes interesadas y reforzar la seguridad como un proceso continuo. A continuación, destacamos algunos de los temas que generaron un gran número de comentarios:

- Requisito 4: Proteja los datos del titular de la tarjeta (CHD) con una criptografía sólida durante la transmisión
  - Protección de todas las transmisiones de CHD
  - Uso de certificados auto firmados/internos
- Requisito 8: Identifique a los usuarios y autentique el acceso
  - Alineación de la longitud, el historial y la frecuencia de cambios de contraseñas con la guía de la industria
  - Comparación de nuevas contraseñas con una lista de contraseñas conocidas inseguras
  - Confirmación de todos los factores de autenticación multifactorial antes de cualquier indicación de éxito o falla de uno de ellos
  - Autenticación segura de las cuentas de aplicaciones y sistemas
- Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta
  - Ubicación de áreas confidenciales dentro de los entornos de datos de titulares de tarjetas
- Requisito 11: Probar periódicamente los sistemas y procesos de seguridad
  - Escaneo autenticado para análisis de vulnerabilidad
- Requisito 12: Refuerce la seguridad de la información con políticas y programas
  - Políticas de uso para proteger tecnologías críticas

- Evaluaciones de riesgos anuales
- Metodologías para la prevención de detección y fuga de datos

No es inusual que al responder a una RFC, organizaciones diferentes hagan comentarios contrapuestos sobre el mismo tema, y los recibidos durante el proceso de RFC sobre PCI DSS versión 4.0 no son una excepción. Se recibieron comentarios positivos y negativos con respecto a los temas arriba mencionados. Al evaluar estos comentarios, el PCI SSC considera una variedad de factores para determinar el mejor camino a seguir. Estos factores incluyen las percepciones específicas expresadas sobre un tema, los comentarios específicos y las soluciones sugeridas por los participantes para abordar los comentarios, y el total de comentarios sobre un determinado tema.

Las deliberaciones sobre estos temas han incluido la ponderación del valor del requisito desde el punto de vista de la seguridad y la forma de asegurar que el significado y la intención del requisito sean claros, así como que el requisito pueda aplicarse a todos los tipos de entornos y partes interesadas, y que brinde mayor flexibilidad para su cumplimiento. En la elaboración del borrador de PCI DSS versión 4.0 para la siguiente RFC, se están considerando los comentarios y su análisis subsiguiente.

Comentarios relativos a la nueva opción de enfoque personalizado
El borrador de PCI DSS versión 4.0 también incluyó el enfoque personalizado, que es un nuevo método para cumplir y validar los requisitos de PCI DSS. Este enfoque da a las organizaciones que usan diferentes tecnologías y metodologías de seguridad más flexibilidad para alcanzar el objetivo de los requisitos de estas normas. Puesto que es nuevo, recibimos muchos comentarios al respecto y los estamos utilizando para establecer guías adicionales, las cuales someteremos a revisión en la siguiente RFC.

Resumen de comentarios
El informe resumido sobre los comentarios en respuesta a la RFC de 2019 se presentará en el portal de PCI en septiembre/octubre de 2020, que será el periodo de la siguiente RFC. Este resumen mostrará todos los comentarios recibidos y cómo se abordó cada uno de ellos.

Preparación de la siguiente RFC
La siguiente RFC está programada para septiembre/octubre de 2020 y estará abierta a todas las organizaciones participantes y a la comunidad de asesores.
Las RFC del PCI SSC están abiertas a la industria a través de las organizaciones participantes. Si su organización desea participar en la siguiente RFC sobre las PCI DSS, debe registrarse como organización participante. Para obtener más información sobre el programa y los beneficios, **haga clic aquí**.

Encontrará más información sobre las próximas RFC y el proceso relacionado en nuestra página de **Solicitud de comentarios**.

Mayor información sobre PCI DSS versión 4.0