INFORMACIÓN COMPLEMENTARIA

PCI DSS v4.x: Guía para el Análisis de Riesgos Específicos

Fecha: Noviembre 2023
Autor: PCI Security Standards Council

Contenidos

DECLARACIONES: La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerarse, para todos los efectos, como la versión oficial de estos documentos y, si existe cualquier ambigüedad o inconsistencia entre este texto y el texto en inglés, el texto en inglés en dicha ubicación es el que prevalecerá.

Introduciendo el Análisis de Riesgos Específicos

PCI DSS v4.0 introdujo el concepto de análisis de riesgos específicos (TRA por sus siglas en inglés) e incluye dos diferentes tipos de TRA. En este documento se ofrece una descripción de cada uno de ellos, respuestas a las preguntas más frecuentes y una tabla que enumera los requisitos de PCI DSS que especifican la realización del TRA para definir la frecuencia con la cual se debe llevar a cabo una actividad.

Para cualquier requisito de PCI DSS que especifique un TRA para definir la frecuencia con la cual se debe realizar una actividad

El primer tipo de TRA, especificado en el requisito 12.3.1 del PCI DSS, se centra en aquellos requisitos del PCI DSS que le permiten a una entidad que tenga flexibilidad en cuanto a la frecuencia con la cual debe realizar un control determinado. Este TRA proporciona un marco para que la entidad defina una frecuencia adecuada basada en su evaluación del riesgo para su entorno.

Para estos TRA, las entidades identificarán los activos específicos, por ejemplo, archivos de registro o credenciales.que el requisito correspondiente pretende proteger, así como la o las amenazas o resultados de los cuales el requisito protege los activos, por ejemplo, malware, un intruso que no se haya detectado o el uso indebido de credenciales.. Los ejemplos de factores que podrían contribuir a la probabilidad y/o al impacto incluyen cualquiera que pueda aumentar la vulnerabilidad de un activo a una amenaza, por ejemplo, la exposición a redes que no son de confianza, la complejidad del entorno o la alta rotación de personal, así como la criticidad de los componentes del sistema o el volumen y la sensitividad de los datos que están siendo protegidos. El rendimiento de un TRA que incorpora estos factores asegura una evaluación sólida, integral y consistente de los riesgos para cada activo aplicable.

Todos los elementos que deben incluirse en un TRA para los requisitos de PCI DSS que permiten flexibilidad en relación a la frecuencia con la cual se realiza una actividad están documentados en la *Plantilla de Muestra* de *PCI DSS v4.x: Análisis de riesgos específicos para la frecuencia de las actividades,* puede encontrarse en la biblioteca de documentos del PCI SSC. Las entidades que documenten un TRA para definir la frecuencia de una actividad, aunque deben incluir todos los elementos especificados en este modelo, no están obligadas a utilizarlo ni a seguir su formato específico.

Para cualquier requisito de PCI DSS que la entidad cumpla con un enfoque personalizado

El segundo tipo de TRA, especificado en la condición 12.3.2, se relaciona con cualquier requisito que una entidad cumpla en relación con el enfoque personalizado. Este TRA apoya la implementación de una metodología del análisis de riesgos repetible y robusta específica para un enfoque personalizado y es una de las varias actividades que la entidad realizará para demostrar de qué forma cumple con el Objetivo del Enfoque Personalizado. El resultado de este tipo de TRA le permite a la entidad identificar los riesgos, evaluar el efecto sobre la seguridad si no se cumple con el requisito definido y describir cómo ha determinado la entidad que los controles cumplen el Objetivo de Enfoque Personalizado y proporcionan al

menos un nivel de protección equivalente al del requisito PCI DSS definido. El evaluador usa la documentación del enfoque personalizado proporcionada por la entidad, incluida en este TRA, para planificar y preparar la evaluación.

Todos los elementos que deben incluirse en un TRA para cualquier requisito de PCI DSS cuando una entidad cumple con el enfoque personalizado están documentados en el PCI DSS v4.x Ejemplos de Plantillas para Respaldar el Enfoque Personalizado (el cual incluye plantillas de muestra tanto para la Matriz de Controles como para el Análisis de Riesgos Específicos), que pueden encontrarse en la Biblioteca de Documentos del PCI SSC.

Nota: Las entidades que documentan cualquiera de los dos tipos de TRA, aunque deben incluir todos los elementos especificados en estas plantillas, no tienen que usar ninguna de las plantillas ni seguir el formato específico de cada una de ellas.

Preguntas Frecuentes acerca de TRA

1. **¿Cómo sabe una entidad cuándo se deben realizar los TRA para determinar la frecuencia de una actividad?**

   Los TRA para determinar la frecuencia de una actividad sólo se exigen cuando se indican explícitamente en un requisito; cada uno de estos requisitos especifica que el TRA debe "realizar de acuerdo con todos los elementos especificados en el requisito 12.3.1".

   Al final de este documento se encuentra la lista de requisitos que especifican un TRA para determinar la frecuencia de las actividades, junto a las frecuencias recomendadas.

2. **¿Con qué frecuencia debe una entidad realizar un TRA para determinar la frecuencia de una actividad?**

   La entidad lleva a cabo inicialmente el ejercicio del análisis de riesgos y prepara el TRA para definir la frecuencia con la cual debe realizarse la actividad en función del riesgo de la entidad. A continuación, la entidad realiza la actividad de acuerdo con el TRA. A partir de entonces, la entidad revisa anualmente el TRA para determinar si los resultados siguen siendo válidos y actualiza el TRA de ser necesario. La revisión de los resultados de estos TRA al menos una vez cada 12 meses, y de los cambios que podrían afectar el riesgo al medio ambiente, permite a la organización garantizar que los resultados de los análisis de riesgos se mantengan actualizados con los cambios organizacionales y las amenazas, tendencias y tecnologías en evolución, y que las frecuencias establecidas aún responden adecuadamente al nivel de riesgo de la entidad.

3. **¿Existe una plantilla de muestra para que el TRA defina la frecuencia de una actividad periódica, similar a las plantillas de muestra proporcionadas para el enfoque personalizado?**

   Sí. La *Plantilla de muestra de PCI DSS v4.x: Análisis de riesgos específicos para la frecuencia de las actividades* se puede encontrar en la Biblioteca de Documentos del PCI SSC, usando el filtro "PCI DSS". Aunque usar esta plantilla no es obligatorio, todos los elementos incluidos en ella, tal y como se

describen en el requisito 12.3.1, deben documentarse en los TRA que definan la frecuencia de la actividad.

4. **¿En qué se diferencia el TRA del requisito 12.3.1 de PCI DSS v4.0 de la evaluación anual de riesgos, exigida en el requisito 12.2 de PCI DSS v3.2.1?**

   El objetivo del requisito 12.3.1 de PCI DSS v4.0 es centrarse en determinadas áreas de riesgo específicas de los requisitos de PCI DSS, mientras que PCI DSS v3.2.1 exigía una evaluación de riesgos general, que muchas organizaciones cumplían con una evaluación de riesgos de toda la empresa que podía no haber sido específica respecto a los datos de las cuentas de pago.

   Puede establecerse un proceso de evaluación de riesgos para toda la empresa como parte del programa general de gestión de riesgos de una entidad, y la información de esa evaluación de riesgos podría aportarles datos a los procesos del TRA. Tenga en cuenta que se recomienda realizar una evaluación de riesgos para toda la empresa, pero no es obligatoria para PCI DSS v4.0. Entre los ejemplos de las metodologías de evaluación de riesgos para las evaluaciones de riesgos en toda la empresa se incluyen, entre otros, ISO 27005 y NIST SP 800-30.

5. **¿Puede una entidad realizar un *Análisis de Riesgos Específicos para la Frecuencia de las Actividades* si quieren realizar una actividad con *menos* frecuencia de la establecida en el requisito de PCI DSS?**

   No. Este tipo de TRA no puede usarse con este fin. Si el requisito establece que una actividad debe realizarse con una frecuencia específica, una organización debe realizar la actividad al menos con la frecuencia definida para cumplir con el requisito tal y como se establece. Si la organización realiza una actividad con menos frecuencia de lo indicado por el requisito, no está cumpliendo con ese requisito de PCI DSS.

   Alternativamente, la organización puede decidir cumplir el Objetivo del Enfoque Personalizado del requisito, siempre que la entidad diseñe, implemente, pruebe y documente un control personalizado que cumpla con el Objetivo del Enfoque Personalizado para ese requisito. Tenga en cuenta que se requiere un TRA para el enfoque personalizado, y la realización de un TRA para el enfoque personalizado es una de las varias actividades que la entidad llevará a cabo para demostrar cómo cumple con el Objetivo del Enfoque Personalizado. Consulte el anexo D de PCI DSS v4.0 para obtener información detallada acerca del enfoque personalizado.

6. **¿Debe una entidad realizar un *Análisis de Riesgos Específicos para la Frecuencia de las Actividades* si desea realizar la actividad con una frecuencia *superior* a la establecida según un requisito de PCI DSS?**

   No. Si la organización desea realizar una actividad con más frecuencia de lo que establece el requisito, puede hacerlo sin realizar el TRA.

7. **Si la entidad tiene una limitación técnica o empresarial legítima que le impide cumplir la frecuencia establecida en un requisito de PCI DSS, ¿se requiere un TRA?**

   No. Si existe una restricción empresarial o técnica documentada que le impida a la organización cumplir con la frecuencia especificada del requisito, se puede documentar e implantar un control compensatorio para mitigar el riesgo asociado al incumplimiento del requisito de PCI DSS según lo establecido.

8. **¿Cuál es el papel del evaluador en la revisión del TRA de una entidad para determinar la frecuencia de la actividad?**

   La función del evaluador es asegurarse de que todos los elementos especificados en el requisito 12.3.1 estén documentados en el TRA de la entidad, incluyendo el que la entidad justifique con qué frecuencia debe realizarse la actividad y cómo esta frecuencia aborda el riesgo de la entidad.

Requisitos y Recomendaciones de Frecuencia del PCI DSS v4.x TRA

La siguiente tabla enumera todos los requisitos de PCI DSS que especifican la realización del TRA para definir la frecuencia con la cual se realiza la actividad, junto a una guía sobre las frecuencias recomendadas para las actividades relacionadas.

Tenga en cuenta que incluso cuando se siga la frecuencia sugerida en la tabla siguiente, se requerirá del TRA para documentar y respaldar la frecuencia seleccionada. Todos los componentes requeridos deben estar incluidos en el TRA, tal y como se especifica en el requisito 12.3.1 de PCI DSS v4.0.

Requisito de PCI DSS v4.0[1]	Frecuencia Sugerida[2]
5.2.3.1 La frecuencia de las evaluaciones periódicas de los componentes del sistema identificados como sin riesgo de malware se define en el análisis de riesgos específicos de la entidad.	Al menos una vez cada seis meses
5.3.2.1 Si se realizan análisis periódicos de malware para cumplir el requisito 5.3.2, la frecuencia de las exploraciones se define en el análisis de riesgos específicos de la entidad.	Al menos una vez al día / diariamente
7.2.5.1 Todos los accesos a las cuentas de aplicaciones y sistemas y los privilegios de acceso correspondientes se revisan periódicamente (con la frecuencia definida en el análisis de riesgos específico de la entidad).	Al menos una vez cada seis meses
8.6.3 Las contraseñas / frases de acceso de las cuentas de aplicaciones y sistemas se cambian periódicamente (con la frecuencia definida en el análisis de riesgos específico de la entidad).	Como mínimo una vez cada tres meses
9.5.1.2.1 La frecuencia de las inspecciones a los dispositivos POI y el tipo de inspección que se realice se define en el análisis de riesgos específico de la entidad.	Al menos una vez al mes / mensualmente
10.4.2.1 La frecuencia de las revisiones periódicas de los registros para todos los demás componentes del sistema (no definido en el Requisito 10.4.1) se define en el análisis de riesgos específicos de la entidad.	Al menos una vez cada siete días / semanalmente
11.3.1.1 Todas las demás vulnerabilidades aplicables (aquellas que no se clasifican como de alto riesgo o críticas (según las clasificaciones de riesgo de vulnerabilidad de la entidad definidas en el Requisito 6.3.1) se gestionan en función del riesgo definido en el análisis de riesgos específicos de la entidad.	Mediano: En tres meses Bajo: En seis meses Informativo: Monitorear regularmente

[1] Esta columna representa extractos resumidos de los requisitos para centrarse en los elementos del TRA de cada uno. Consulte PCI DSS v4.0 para que conozca todos los requisitos.

[2] La columna de la frecuencia sugerida incluye recomendaciones de referencia que las entidades pueden considerar como aporte a su proceso de toma de decisiones a la hora de evaluar el riesgo y determinar una frecuencia de la actividad adecuada para su entorno. Cada entidad debe usar sus resultados específicos de TRA para determinar las frecuencias mínimas necesarias para abordar el riesgo de la entidad y proteger mejor su entorno.

Requisito de PCI DSS v4.0[1]	Frecuencia Sugerida[2]
11.6.1 Se despliega un mecanismo de detección de cambios y manipulaciones para detectar las modificaciones no autorizadas en los encabezados HTTP y en el contenido de las páginas de pago, y las funciones del mecanismo se realizan al menos una vez cada siete días O periódicamente con la frecuencia definida en el análisis de riesgos específico de la entidad.	Como mínimo una vez cada siete días
12.10.4.1 La frecuencia de la capacitación periódica del personal de respuesta a incidentes se define en el análisis de riesgos específicos de la entidad.	Al menos una vez al año y al iniciar la relación laboral