PCI DSS v4.x Ejemplos de Plantillas para Respaldar el Enfoque Personalizado

Este documento contiene plantillas de muestra para la matriz de controles y el análisis de riesgos específicos, los cuales la entidad debe documentar como parte de su enfoque personalizado. Estas plantillas son ejemplos de los formatos que podrían usarse.

Nota: *Aunque no es obligatorio que las entidades sigan los formatos específicos que se proporcionan a continuación, la matriz de controles y el análisis de riesgos específicos de la entidad deben incluir toda la información de dichas plantillas, tal como está definido en el requisito 12.3.2 de PCI DSS v4.x.*

Enfoque Personalizado - Ejemplo de Plantilla de Matriz de Control

El siguiente es un ejemplo de la plantilla de matriz de control que puede ser utilizado por una entidad para documentar su implementación personalizada.

Como se describe en PCI DSS v4.x el *Anexo D: Enfoque Personalizado,* las entidades que utilizan el enfoque personalizado deben completar una matriz de control para proporcionar detalles de cada control implementado que explique qué se implementa, cómo ha determinado la entidad que los controles cumplen con el objetivo declarado de un requisito de PCI DSS, cómo el control proporciona al menos, el nivel de protección equivalente al que se lograría al cumplir con el requisito definido, y cómo la entidad tiene la seguridad sobre la eficiencia del control de forma continua.

El asesor utiliza la información dentro de cada matriz de control para planificar y prepararse para la evaluación.

Este ejemplo de plantilla de matriz de control incluye la información mínima que debe documentar la entidad y proporcionar al asesor para una validación personalizada. Si bien no se requiere el uso de esta plantilla específica, se requiere que la documentación del enfoque personalizado de la entidad incluya toda la información definida en esta plantilla, y que la entidad proporcione esta información exacta a su asesor.

La matriz de control no reemplaza la necesidad de que el asesor desarrolle de forma independiente procedimientos de prueba apropiados para validar los controles implementados. El asesor aún debe realizar las pruebas necesarias para verificar que los controles cumplan con el objetivo del requisito, sean eficientes y se mantengan de forma apropiada. La matriz de control tampoco reemplaza los requisitos de informes para validaciones personalizadas como se especifica en la plantilla ROC.

La matriz de control deberá incluir al menos la información de la siguiente tabla.

Ejemplo de Plantilla de Matriz de Control para los requisitos de PCI DSS cubiertos a través del Enfoque Personalizado Para ser completado por la entidad evaluada		
Identificador/Nombre de Control Personalizado	<La entidad define cómo quiere referirse a este control>	
Número de requisitos de PCI DSS y objetivos que se cumplen con este control.	Requisito #: Requisito #:	Objetivo: Objetivo:
Detalles del control		
¿Cuáles son los controles implementados?	<La entidad describe qué es el control y qué hace>	
¿Dónde se implementan los controles?	<La entidad identifica las ubicaciones de las instalaciones y los componentes del sistema donde se implementa y gestiona el control>	
¿Cuándo se realizan los controles?	<La entidad detalla con qué frecuencia se realiza el control; por ejemplo, se ejecuta continuamente en tiempo real o está programado para ejecutarse en NN horas y en XX intervalos>	
¿Quién tiene la responsabilidad general y la rendición de cuentas de los controles?	<La entidad incluye detalles del personal/funciones individuales con responsabilidad y rendición de cuentas para este control>	
¿Quién participa en la gestión, el mantenimiento y el monitoreo de los controles?	<La entidad incluye detalles del personal individual/funciones y/o equipos, según corresponda, que gestionan, mantienen y monitorean el control>	
Si corresponde, ¿cómo se consideran los controles como una mejora de otro control PCI DSS ya requerido para el elemento en revisión?	<La entidad describe cómo este control es una mejora de algún otro control PCI DSS requerido para el artículo bajo revisión>	

Ejemplo de Plantilla de Matriz de Control para los requisitos de PCI DSS cubiertos a través del Enfoque Personalizado Para ser completado por la entidad evaluada	
Para cada **requisito de PCI DSS para el cual se utilicen los controles personalizados, la entidad proporciona detalles de lo siguiente:**	
La entidad describe cómo los controles implementados cumplen con el ***Objetivo del Enfoque Personalizado*** establecido del requisito de PCI DSS.	<La entidad describe cómo el control cumple con el Objetivo del Enfoque Personalizado establecido del requisito de PCI DSS y resume los resultados relacionados>
La entidad describe las pruebas **que realizó** y los resultados de esas pruebas que demuestran que los controles cumplen con el objetivo del requisito aplicable.	<La entidad describe las pruebas que realizó para demostrar que el control cumple con el objetivo declarado del requisito de PCI DSS y resume los resultados relacionados>
La entidad describe brevemente los resultados del análisis de riesgo específico individual **que realizó** que explica los controles implementados y describe cómo los resultados verifican que los controles brindan al menos un nivel de protección equivalente al del enfoque definido por el requisito de PCI DSS aplicable. *Consulte el Enfoque Personalizado – Ejemplo de la Plantilla de Análisis de Riesgos Específicos para obtener detalles sobre cómo documentar este análisis de riesgos*.	<La entidad describe brevemente los resultados de su análisis de riesgo para este control, el cual se detalla por separado en el Análisis de Riesgo Específico>
La entidad describe las medidas **que ha implementado** para garantizar que se mantengan los controles y se garantice su eficiencia de forma continua. *Por ejemplo, cómo la entidad supervisa la eficiencia en el control, cómo se detectan y responden las fallas de control, y las acciones que se toman.*	<La entidad describe cómo asegura que se mantenga el control y cómo se asegura la eficiencia del control.>

Enfoque Personalizado - Ejemplo de Plantilla de Análisis de Riesgo Específico

La siguiente es una muestra de una plantilla de análisis de riesgo específico que la entidad puede usar para su implementación personalizada. *Si bien no se requiere que la entidad siga este formato específico, la documentación de su enfoque personalizado debe incluir toda la información definida en esta plantilla.*

Como se describe en PCI DSS v4.x en el *Anexo D: Enfoque Personalizado, una entidad que utilice el enfoque personalizado debe proporcionar un análisis de riesgo específico detallado para cada requisito que la entidad cumpla con el enfoque personalizado.* El análisis de riesgo define el riesgo, y describe cómo la entidad ha determinado que los controles cumplen con el objetivo del enfoque personalizado, y como la entidad determinó que los controles brindan al menos un nivel de protección equivalente al proporcionado por el requisito de PCI DSS definido.

El asesor utiliza la información en el análisis de riesgo específico para planificar y prepararse para la evaluación.

Al completar un análisis de riesgo específico para un enfoque personalizado, es importante recordar que:

- El activo que se protege son los datos de tarjetahabiente que la entidad almacena, procesa o transmite.
- Los agentes amenazas están altamente motivados y capaces. La motivación y la capacidad de los agentes de amenazas tiende a aumentar en relación con el volumen de datos de tarjetahabiente que generará un ataque exitoso.
- La probabilidad de que una entidad sea atacada por agentes de amenazas aumenta a medida que la entidad almacena, procesa o transmite mayores volúmenes de datos de tarjetahabiente.
- El daño está directamente relacionado con el objetivo. Por ejemplo, si el objetivo es “el software malicioso no puede ejecutarse”, el daño es que el software malicioso se ejecute; si el objetivo es “se asignan responsabilidades diarias para realizar todas las actividades”, el daño es que no se asignan las responsabilidades.

***Nota**: El término “daño” tal como se usa en este análisis de riesgo específico (por ejemplo, en 1.3 en la tabla a continuación) se refiere a una ocurrencia o evento que afecta negativamente la postura de seguridad de la entidad. Ejemplos de esto lo constituyen la ausencia de una política, la falla en realizar un escaneo de vulnerabilidades o que se ejecute malware en el entorno de la entidad.*

Esta muestra de plantilla de análisis de riesgo específico incluye la información mínima que debe documentar la entidad y proporcionar al asesor para una validación personalizada. Si bien no se requiere el uso de esta plantilla específica, se requiere que la documentación del enfoque personalizado de la entidad incluya toda la información definida en esta plantilla, y que la entidad proporcione esta información exacta a su asesor.

El análisis de riesgos específico debe incluir al menos la información de la siguiente tabla.

Ejemplo de Análisis de Riesgo Específico para los requisitos de PCI DSS cumplidos a través del Enfoque Personalizado. Para ser completado por la entidad evaluada	
Ítem	**Detalles**
1. Identificar el requisito	
1.1 Identifique el requisito de PCI DSS tal como está escrito.	<La entidad identifica el requisito>
1.2 Identifique el objetivo del requisito de PCI DSS tal como está escrito.	<La entidad identifica el objetivo del requisito>
1.3 Describa el daño que el requisito pretendía impedir.	<La entidad describe el daño> <La entidad describe el efecto sobre su seguridad si la entidad no cumple con éxito el objetivo.> <La entidad describe qué fundamentos de seguridad cumplen, o qué podría hacer un agente de amenazas si la entidad no cumple con éxito el objetivo.>
2. Describa la solución propuesta	
2.1 Identificador/Nombre de Control Personalizado	<La entidad identifica el control personalizado como se documenta en la Matriz de Controles.>
2.2 ¿Qué partes del requisito tal como está escrito cambiarán en la solución propuesta?	<La entidad identifica qué elementos del requisito no se cumplirán con el enfoque definido y, por lo tanto, estarán cubiertos por el enfoque personalizado. Esto podría ser tan pequeño como cambiar la periodicidad de un requisito o la implementación de un conjunto de controles completamente diferente para cumplir el objetivo.>
2.3 ¿Cómo evitará el daño la solución propuesta?	<La entidad describe cómo los controles detallados en la Matriz de Controles evitarán los daños identificados en 1.3.>

Ejemplo de Análisis de Riesgo Específico para los requisitos de PCI DSS cumplidos a través del Enfoque Personalizado. Para ser completado por la entidad evaluada						
Ítem	**Detalles**					
3. Analice cualquier cambio en la PROBABILIDAD de que ocurra el daño, lo que lleva a una brecha de la confidencialidad de los datos de tarjetahabiente.						
3.1 Describa los factores detallados en la Matriz de Control que afectan la probabilidad de que ocurra el daño.	La entidad describe: • Qué tan exitosos serán los controles para prevenir el daño • Cómo los controles detallados en la Matriz de Control reducen la probabilidad de que ocurra el daño					
3.2 Describa las razones por las que el daño puede seguir ocurriendo después de la aplicación del control personalizado.	La entidad describe: • Las razones típicas por las que falla el control, la probabilidad de que esto ocurra y cómo podría evitarse • ¿Qué tan resilientes son los procesos y sistemas de la entidad para detectar que los controles no están operando normalmente? • ¿Cómo un agente de amenazas podría eludir este control? - ¿Qué pasos deberían tomar? ¿qué tan difícil es, se detectaría al agente de amenazas antes de que fallara el control? ¿Cómo se ha determinado esto?					
3.3 ¿En qué medida los controles detallados en el enfoque personalizado representan un cambio en la probabilidad de ocurrencia del daño en comparación con el requisito de enfoque definido?	El daño es más susceptible de ocurrir	☐	No hay cambios	☐	El daño es menos susceptible de ocurrir	☐
3.4 Proporcione el razonamiento de su evaluación del cambio en la probabilidad de que ocurra el daño una vez que se implementen los controles personalizados.	La entidad provee: • La justificación de la evaluación documentada en 3.3. • Los criterios y valores utilizados para la evaluación documentada en 3.3.					

Ejemplo de Análisis de Riesgo Específico para los requisitos de PCI DSS cumplidos a través del Enfoque Personalizado. Para ser completado por la entidad evaluada				
Ítem	**Detalles**			
4. Analice cualquier cambio en el IMPACTO del acceso no autorizado a los números de cuenta principales (PAN)				
4.1 Para el alcance de los componentes del sistema que cubre esta solución, ¿qué volumen de los números de cuenta principales (PAN) estarían en riesgo de acceso no autorizado si la solución fallara?	**4.1.1** Número de datos PAN almacenados	*Máximo en cualquier momento*	**4.1.2** Número de datos PAN procesados o transmitidos durante un período de 12 meses	*Total*
4.2 Descripción de cómo los controles personalizados serán direccionados: • Reducirán la cantidad de datos PAN individuales comprometidos si un agente de amenazas tiene éxito, y/o • Permitirán una notificación más rápida de los datos PAN comprometidos con las marcas de tarjetas.	El impacto en el ecosistema de pago está directamente relacionado con la cantidad de cuentas comprometidas y con qué rapidez el emisor de la tarjeta puede bloquear cualquier dato PAN que haya quedado comprometido. La entidad describe cómo los controles personalizados logran lo siguiente, para cada uno de los controles personalizados: • Reduce el volumen de datos de tarjetahabiente que se almacenan, procesan o transmiten y, por lo tanto, reduce los elementos disponibles para que un agente de amenazas tenga éxito, y/o • Reduce el tiempo de detección, notificación de cuentas comprometidas y contención del agente de amenazas.			

Ejemplo de Análisis de Riesgo Específico para los requisitos de PCI DSS cumplidos a través del Enfoque Personalizado. Para ser completado por la entidad evaluada	
Ítem	**Detalles**
5. Aprobación y revisión de riesgos	
5.1 He revisado el análisis de riesgos anterior y acepto que el uso del enfoque personalizado propuesto como se detalla proporciona al menos un nivel de protección equivalente al enfoque definido para el requisito de PCI DSS aplicable.	Un miembro de la dirección ejecutiva debe revisar y aceptar el enfoque personalizado propuesto. <Un miembro de la gerencia ejecutiva de la entidad firma que revisó y aceptó el enfoque personalizado documentado aquí.>
5.2 Este análisis de riesgos debe revisarse y actualizarse a más tardar:	El análisis de riesgos debe revisarse al menos cada doce meses, y con mayor frecuencia si el enfoque personalizado en sí tiene un límite de tiempo (por ejemplo, porque hay un cambio planificado en la tecnología) o si otros factores dictan un cambio necesario. En caso de una revisión de riesgo no programada, detalle el motivo por el cual se realizó la revisión. <La entidad indica la fecha en que se revisó y actualizó el análisis de riesgo específico.>

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.