SUPLEMENTO INFORMATIVO

PCI DSS v4.x: Guía para Controles Compensatorios y el Enfoque Personalizado

Versión: 1.0
Fecha: Junio de 2026
Autor: PCI Security Standards Council

Cambios en el Documento

Fecha	Versión	Descripción
Junio de 2026	1.0	Lanzamiento inicial

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.

Contenido

Cambios en el Documento ..... **i**
Descripción General **1**
Público Objetivo y Propósito 1
Opciones para Implementar y Validar los Controles PCI DSS v4.x 2
Comparación de Casos de Uso: Ejemplos de Controles Compensatorios y el Enfoque Personalizado **4**
Funciones de los Controles Compensatorios y el Enfoque Personalizado **5**
Función de la Entidad: Controles Compensatorios 5
Función del Asesor: Controles Compensatorios 5
Función de la Entidad: Enfoque Personalizado 7
Función del Asesor: Enfoque Personalizado 7
Documentación de los Controles compensatorios y el Enfoque Personalizado **10**
Independencia del Asesor **11**
Referencias y Materiales de Apoyo **12**
Apéndice: Ejemplos de Plantillas de Control Compensatorio y Enfoque Personalizado Completadas **13**
Ejemplo Completado para la Entidad: Ficha de Control Compensatorio 13
Ejemplo Completado para la Entidad: Matriz de Controles para el Enfoque Personalizado 16
Ejemplo Completado para la Entidad: Análisis de Riesgos Específico para un Enfoque Personalizado 19
Ejemplo Completado para el Asesor: Informe de Cumplimiento — Apéndice E Plantilla de Enfoque Personalizado 22

Descripción General

El Estándar Payment Card Industry Data Security Standard (PCI DSS) permite flexibilidad en la forma en que se cumplen los objetivos de seguridad. PCI DSS v4.x incluye dos enfoques para implementar y validar los controles PCI DSS: el enfoque definido y el enfoque personalizado. Estos dos enfoques difieren en intención, elementos, documentación y validación.

Este documento destaca cada enfoque y:

- Aborda el papel de las entidades evaluadas
- Aborda el papel de los asesores involucrados y
- Proporciona la documentación para estos enfoques y las respuestas a preguntas frecuentes.

Para las entidades evaluadas, este documento incluye ejemplos completados de:

- Una Ficha de Control Compensatorio,
- Una Matriz de Controles para un Enfoque Personalizado y
- Un Análisis de Riesgos Específico para un Enfoque Personalizado.

Para los asesores, este documento incluye un ejemplo completado de un Informe de Cumplimiento: Plantilla de Enfoque Personalizado del Apéndice E.

Público Objetivo y Propósito

Este documento está destinado para el uso de todas las entidades que desarrollan, operan, gestionan o evalúan controles compensatorios o un enfoque personalizado. Esto incluye a los asesores que realizan las evaluaciones PCI DSS y a las entidades que se someten a ellas.

El objetivo de este documento es proporcionar orientación práctica para respaldar el uso coherente de los controles compensatorios y el enfoque personalizado.

PCI Security Standards Council (PCI SSC) no es responsable de hacer cumplir las normas ni de determinar si una implementación particular es compatible. Las entidades deberán trabajar con las organizaciones que administran su programa de cumplimiento, como un adquirente (banco comercial), una marca de pago u otra entidad, para comprender las responsabilidades de validación y presentación de informes de cumplimiento de la entidad.

La orientación contenida en este documento no añade, amplía, reemplaza ni anula los requisitos PCI DSS ni de ningún otro estándar PCI SSC. En el momento de la publicación, la versión actual de PCI DSS es v4.0.1; sin embargo, los principios y prácticas generales que se ofrecen aquí también pueden aplicarse a versiones futuras.

Opciones para Implementar y Validar los Controles PCI DSS v4.x

El estándar PCI DSS v4.x ofrece dos maneras para que una entidad implemente y valide los requisitos PCI DSS: el enfoque definido y el enfoque personalizado.

El enfoque definido es el método tradicional para implementar y validar los controles de PCI DSS, que ha estado vigente desde la primera versión de PCI DSS. **Los controles compensatorios son una opción dentro del enfoque definido** para las entidades que tienen una restricción técnica o de negocios legítima y documentada que les impide cumplir con el requisito del enfoque definido tal como se indica. Los controles compensatorios, en general, se utilizan en situaciones en las que un sistema o proceso tradicional no se puede actualizar para cumplir el requisito.

El enfoque personalizado se centra en el objetivo de seguridad de cada requisito PCI DSS (si corresponde), lo que permite a las entidades implementar controles para cumplir con el Objetivo del Enfoque Personalizado establecido para el requisito, de una manera que no sigue estrictamente el requisito definido. Dado que cada implementación personalizada es diferente, no existen procedimientos de prueba definidos; en su lugar, el asesor debe elaborar procedimientos de prueba adecuados para la implementación específica, de modo que pueda validar que los controles implementados cumplan con el objetivo establecido.

¿El enfoque personalizado es una opción viable para todos los requisitos PCI DSS?

La mayoría de los requisitos PCI DSS pueden cumplirse utilizando el enfoque definido o el personalizado. Sin embargo, varios requisitos no tienen un objetivo de enfoque personalizado definido, lo que resulta en que no exista una opción de enfoque personalizado.

¿Para qué tipo de entidades está dirigido este enfoque personalizado?

El enfoque personalizado tiene como objetivo fomentar la innovación en las prácticas de seguridad, permitiendo a las entidades una mayor flexibilidad para demostrar cómo sus controles de seguridad cumplen con los objetivos de PCI DSS. Este enfoque se recomienda para entidades con un nivel de madurez en la gestión de riesgos que demuestren un enfoque sólido de gestión de riesgos en materia de seguridad, que incluye, entre otros, un departamento dedicado a la gestión de riesgos o un enfoque de gestión de riesgos para toda la entidad.

Se espera que los controles implementados y validados que utilizan el enfoque personalizado cumplan o superen la seguridad proporcionada por el requisito en el enfoque definido. Por consiguiente, el nivel de documentación y el esfuerzo necesarios para validar las implementaciones personalizadas también serán mayores que para el enfoque definido.

¿Las entidades que completan un SAQ pueden utilizar un enfoque personalizado?

El uso del enfoque personalizado no está contemplado en los Cuestionarios de Autoevaluación (SAQ). Las entidades que deseen realizar la validación utilizando el enfoque personalizado podrán usar la Plantilla del Informe de Cumplimiento (ROC) de PCI DSS para documentar los resultados de la evaluación. Las preguntas sobre el uso del enfoque personalizado, incluyendo si las entidades que reúnen los requisitos para un SAQ pueden, en su lugar, completar un ROC para utilizar un enfoque personalizado, siempre deben dirigirse a las organizaciones que gestionan los programas de cumplimiento, como las marcas de pago y las entidades adquirentes.

¿Cuál es la diferencia entre un control compensatorio y el enfoque personalizado?

Es importante tener en cuenta que los controles compensatorios tienen un propósito diferente al del enfoque personalizado. A diferencia de los controles compensatorios, que se utilizan cuando las organizaciones tienen una limitación y **no pueden** cumplir con el requisito tal como está establecido, el enfoque personalizado está destinado a entidades que **optan por cumplir con** el requisito de manera diferente a como está establecido. En este caso, la entidad debe cumplir con el Objetivo del Enfoque Personalizado establecido en lugar del requisito establecido. El enfoque personalizado resulta más eficaz cuando la entidad cuenta con procesos de seguridad sólidos y prácticas de gestión de riesgos robustas, así como con la capacidad de diseñar de manera efectiva la documentación, las pruebas y el mantenimiento de los controles de seguridad que cumplan con ese objetivo.

Tenga en cuenta que el Objetivo del Enfoque Personalizado de un requisito puede revisarse para comprender la intención del mismo, incluso cuando una entidad no esté implementando un enfoque personalizado para ese requisito.

¿Se pueden utilizar un control compensatorio y un enfoque personalizado para el mismo requisito?

Sí. Una entidad puede utilizar controles compensatorios para ciertos componentes del sistema y un enfoque personalizado para cumplir con ese mismo requisito en otros componentes del sistema. Tomando como ejemplo el Requisito 5.3.1, una entidad podría utilizar un control compensatorio para cumplir con ese requisito para un determinado tipo de servidor, cuando exista una restricción de negocios legítima y documentada que impida que ese servidor cumpla con el requisito establecido. La entidad también puede optar por utilizar el enfoque personalizado para cumplir con ese mismo requisito en otros componentes del sistema, donde haya implementado un enfoque único para detectar y abordar las últimas amenazas de *malware*. La entidad también podría utilizar el enfoque definido, tal como se indica, para cumplir con ese mismo requisito en otro grupo de componentes del sistema.

Si una entidad diseña un enfoque personalizado que no cumple con el objetivo del enfoque personalizado, ¿puede la entidad utilizar un control compensatorio en su lugar para cumplir con el objetivo del enfoque personalizado?

No. Los controles compensatorios no son una opción para el enfoque personalizado. El enfoque personalizado está dirigido a organizaciones que optan por desarrollar sus propios controles que cumplan con el Objetivo del Enfoque Personalizado del requisito. Si una organización desarrolla un enfoque personalizado y luego tiene limitaciones técnicas o de negocios que le impiden cumplir el objetivo de dicho enfoque, esto significa que la organización diseñó un enfoque personalizado que no puede cumplir. Por eso, con este enfoque personalizado, los controles compensatorios no son una opción.

Si una entidad determina que no puede cumplir con un requisito PCI DSS con un enfoque personalizado, y tiene una restricción técnica o de negocios que le impide cumplir con el requisito del Enfoque Definido tal como está escrito, la entidad puede optar por implementar un control compensatorio basado en el requisito original del Enfoque Definido.

Comparación de Casos de Uso: Ejemplos de Controles Compensatorios y el Enfoque Personalizado

Estos ejemplos se proporcionan únicamente para diferenciar los casos de uso en los que se puede considerar un control compensatorio o un enfoque personalizado. Estos casos de uso no pretenden ilustrar implementaciones o controles reales que sean adecuados o recomendados para su uso en algún entorno específico. La entidad siempre debe confirmar con su asesor, y con la entidad a la que presentará la documentación de cumplimiento, la aceptabilidad y el uso de cualquier control compensatorio o control personalizado.

Abordado Mediante un Control Compensatorio	Abordado Mediante un Enfoque Personalizado
Requisito 3.3.1.2 Los datos SAD se almacenan después de la autorización porque la entidad no dispone de la tecnología necesaria para prohibir su almacenamiento.	*Este requisito no es elegible para el enfoque personalizado.*
Requisito 3.5.1 Debido a una limitación técnica, los PAN no se pueden cifrar ni hacer ilegibles de ninguna otra manera.	
Requisito 5.2.1 Las soluciones *anti-malware* no se pueden implementar en ciertos sistemas debido a limitaciones técnicas.	**Requisito 5.2.1** Existe un mecanismo que detecta todo el *software* malicioso e impide que se instale o ejecute.
Requisito 8.3.6 La herramienta del proveedor de servicios en la nube no permite modificar las configuraciones de contraseña y las configuraciones proporcionadas no cumplen con los requisitos PCI DSS. *Esto podría solucionarse mediante un Control Compensatorio o un Enfoque Personalizado, dependiendo del control implementado.*	
	Requisito 11.3.1 Las vulnerabilidades internas se identifican mediante un método distinto al escaneo interno de vulnerabilidades.
Requisito 11.3.2 Debido a un cambio pendiente en la herramienta ASV, el próximo análisis de vulnerabilidades externas no podrá realizarse a tiempo.	*Este requisito no es elegible para el enfoque personalizado.*
	Requisito 11.5.1 Para detectar el tráfico anómalo de la red se utiliza un mecanismo distinto a los IDS/IPS.

Funciones de los Controles Compensatorios y el Enfoque Personalizado

Función de la Entidad: Controles Compensatorios

Se espera que las entidades definan los controles compensatorios cuando los utilicen y documenten dichos controles compensatorios completando una o más Hojas de Trabajo de Controles Compensatorios (CCW). Las CCW de la entidad deben incluir:

- Restricciones técnicas o de negocios claramente definidas que impiden que la entidad cumpla con el requisito PCI DSS establecido.
- La definición de control compensatorio y la explicación de cómo el control aborda los objetivos del requisito original y cualquier riesgo aumentado: por ejemplo, en términos de las personas, los procesos, las políticas y/o las tecnologías que componen el control.
- El objetivo del control original:
  - La entidad puede, pero no está obligada a, utilizar el Objetivo de Enfoque Personalizado del requisito para este objetivo.
- El objetivo alcanzado por el control compensatorio:
  - Este puede ser, aunque no es obligatorio, el objetivo del enfoque personalizado establecido para el requisito PCI DSS.
- Una descripción de cualquier riesgo adicional que pueda suponer la falta del control original. La documentación debe reflejar la comprensión de este riesgo y cómo se aborda.
- Una explicación de cómo la entidad valida y prueba el control compensatorio.
- Una definición de los procesos y controles que la entidad ha implementado para mantener el control compensatorio.

En *el Apéndice C de PCI DSS v4.x se incluye un ejemplo de una CCW: Hoja de Trabajo de Control Compensatorio.* En el sitio web de PCI SSC, en la Biblioteca de documentos dentro del apartado PCI DSS, encontrará una plantilla para una *Hoja de Trabajo Adicional de Control Compensatorio.*

Función del Asesor: Controles Compensatorios

Los asesores deben evaluar minuciosamente las Hojas de trabajo de controles compensatorios (CCW) de la entidad durante cada evaluación anual de PCI DSS para confirmar que las CCW documenten y aborden de manera clara y efectiva los elementos del *Apéndice C: Ficha de Control Compensatorio*, mencionada anteriormente en “Función de la Entidad”.

En el caso de las limitaciones técnicas o de negocios legítimas documentadas de la entidad, no se espera que el asesor confirme que la limitación de negocios o técnica sea válida, sino solo que la entidad la haya documentado exhaustivamente. Sin embargo, se espera que el asesor pruebe los elementos de control implementados por la entidad para confirmar que el control compensatorio esté en funcionamiento y que opere de manera efectiva.

Se espera que el asesor:

- Incluya las CCW de la entidad en el Informe de Cumplimiento (ROC) o el Cuestionario de Autoevaluación (SAQ), según corresponda.
- Realice pruebas del control compensatorio, incluyendo el examen de la configuración, la revisión de la documentación, la observación de los procesos, etc., según corresponda al requisito y control relacionados que se estén revisando.
  - Los Procedimientos de Prueba del requisito pueden considerarse una guía sobre el tipo de prueba esperada para ese requisito.
- Al completar un ROC, por cada requisito PCI DSS cumplido con un control compensatorio:
  - Marque la casilla “Control Compensatorio”.
  - Incluya una descripción de cómo las pruebas y las evidencias del asesor demuestran que se cumple el requisito.
  - Documente las pruebas realizadas en los documentos de trabajo del asesor y almacene la evidencia junto con las demás evidencias de evaluación.

¿Puede utilizarse un control compensatorio para abordar un requisito que fue* omitido *en el pasado?

No. Para PCI DSS v4.x, Apéndice B: Se actualizó el apartado de Controles Compensatorios para aclarar que *los controles compensatorios no pueden utilizarse para abordar retroactivamente un requisito que se omitió en el pasado*. Nunca se pretendió que los controles compensatorios pudieran utilizarse de esta manera. Por ejemplo, una tarea que debería haberse realizado no se realizó, y en ese momento no se tomó ninguna medida para solucionarlo. Sin embargo, una entidad puede implementar un control compensatorio para abordar factores que puedan afectar el desempeño futuro de una tarea (por ejemplo, para anticipar el tiempo de inactividad programado del sistema o las vacaciones del personal).

¿Se puede utilizar un control compensatorio para cumplir con múltiples requisitos PCI DSS?

Sí. Se puede diseñar un control compensatorio para mitigar el riesgo de no cumplir con más de un requisito. Sin embargo, la forma en que cada requisito se cumple mediante ese control compensatorio debe documentarse por separado en Hojas de Trabajo de Controles Compensatorios individuales.

Deben abordarse todos los objetivos y riesgos asociados a cada requisito, y el control compensatorio debe validarse de forma independiente para cada requisito.

¿Es necesario utilizar un control compensatorio solo durante un tiempo limitado?

No. No existe ningún requisito que exija que un control compensatorio esté vigente únicamente por un período limitado; sin embargo, la entidad evaluada debe revisar sus controles compensatorios anualmente para confirmar que siguen siendo efectivos y necesarios. Por ejemplo, una nueva tecnología o sistema puede requerir un control compensatorio modificado para cumplir con el objetivo del requisito, o puede haber anulado la necesidad de un control compensatorio, de modo que ahora se pueda cumplir con el requisito PCI DSS original tal como se indicó.

Asimismo, se espera que el asesor revise anualmente los controles compensatorios de la entidad para confirmar que sigan siendo apropiados y necesarios para abordar el riesgo y cumplir con el requisito.

Función de la Entidad: Enfoque Personalizado

La entidad evaluada diseña, desarrolla, analiza, implementa y mantiene sus controles personalizados, incluyendo los siguientes pasos:

- Revisar la información sobre el enfoque personalizado que se indica en la sección Referencias y Materiales de Apoyo de este documento.
- Definir y documentar cada control personalizado, incluyendo una descripción de cómo el control cumple con el objetivo del requisito. Consultar la *Plantilla de Matriz de Controles de Muestra*[1] para una plantilla que se puede utilizar para documentar información sobre el control personalizado.
- Realice y documente un análisis de riesgo específico que demuestre que el control personalizado es suficientemente robusto para proporcionar al menos la protección equivalente al Requisito Definido. Consulte la *Ejemplo de Plantilla de Análisis de Riesgo Específico*[1] para una plantilla que puede utilizarse para documentar información sobre el control personalizado.
- Realice y documente pruebas que confirmen que cada control personalizado cumple con el objetivo del requisito eficazmente. Consulte la *Ejemplo de Plantilla de Matriz de Control* para documentar las pruebas realizadas y los resultados de las mismas.
- Describa cómo se supervisa y mantiene la eficacia de cada control con el paso del tiempo.
- Comuníquese con anticipación con su asesor sobre los planes para implementar un enfoque personalizado.
- Proporcione a su asesor toda la documentación relativa a todos los controles personalizados.

Para que la entidad evaluada pueda implementar y mantener sus controles personalizados eficazmente, es importante que internalice la responsabilidad y asuma la propiedad activa de dichos controles.

Función del Asesor: Enfoque Personalizado

Cuando se utiliza el enfoque personalizado, los asesores deben esperar recibir con anticipación la documentación del enfoque personalizado de la entidad para ayudarlos a realizar los siguientes pasos:

- Confirmar que el requisito PCI DSS en cuestión sea elegible para el enfoque personalizado.
- Revisar la documentación de la entidad para comprender completamente el control personalizado.
  - Confirmar que tanto la Matriz de Controles como el Análisis de Riesgos Específico se han completado y entregado.
- Confirmar que cada control personalizado esté suficientemente documentado, incluyendo lo siguiente:
  - La documentación incluye toda la información requerida, tal como se especifica en las plantillas de Matriz de Controles del Enfoque Personalizado y Análisis de Riesgos Específico.

[1] Se incluyen dos Plantillas en las Plantillas de Ejemplo: Enfoque Personalizado: 1) un Enfoque Personalizado - Ejemplo de Plantilla de Matriz de Control y 2) un Enfoque Personalizado - Ejemplo de Plantilla de Análisis de Riesgo. Este documento está disponible en el sitio web de PCI SSC, en la Biblioteca de Documentos, en el apartado de PCI DSS. Si bien no es obligatorio que las entidades sigan los formatos específicos de estas plantillas, la Matriz de Controles de Enfoque Personalizado y el Análisis de Riesgo Específico de la entidad deben incluir toda la información de estas plantillas, tal como se define en el Requisito PCI DSS 12.3.2.

  - La documentación describe cómo el control personalizado proporciona al menos la misma protección que el Requisito Definido.

- Revisar las pruebas que la entidad realizó del control personalizado y los resultados de las pruebas para determinar si las pruebas realizadas por la entidad fueron suficientes para evaluar los controles exhaustivamente.
- Diseñar procedimientos de prueba rigurosos que permitan realizar pruebas exhaustivas de cada control personalizado.
  - La documentación proporcionada por la entidad debe ser lo suficientemente detallada para que el asesor pueda comprender cómo funciona el control y derivar los procedimientos de prueba adecuados.
  - Si el asesor determina que las pruebas realizadas por la entidad proporcionaron una evaluación exhaustiva del control, el asesor puede, opcionalmente, utilizar las pruebas de la entidad para realizar sus propias pruebas de la eficacia del control. En este caso, el asesor deberá utilizar un conjunto de muestras diferente al utilizado por la entidad.
- Realizar pruebas independientes de cada implementación de control personalizada. No debe depender únicamente de los resultados de las pruebas realizadas por la entidad. El propósito de las pruebas del asesor es determinar si el control:
  - Cumple con el objetivo de Enfoque Personalizado del requisito,
  - Se le da mantenimiento para garantizar la eficacia continua y
  - Es suficiente para dar como resultado un resultado de "Vigente".
- Documente cada control personalizado en el Informe de Cumplimiento (ROC), tanto en el-requisito como en el *Apéndice E del ROC: Plantilla de Enfoque Personalizado*.
  - Durante una evaluación, el asesor completa este apéndice para cada caso en el que se utiliza un control personalizado para cumplir con un requisito PCI DSS.
  - Además de incluir información sobre el control personalizado de la documentación de la entidad, se espera que el asesor incluya detalles sobre los procedimientos de prueba elaborados, la evidencia revisada para confirmar que el control está implementado y funciona eficazmente, y los resultados de las pruebas realizadas.

En el caso del enfoque personalizado, ¿pueden las pruebas realizadas por la entidad sustituir las pruebas realizadas por el asesor?

No. Las pruebas realizadas por la entidad son necesarias como parte de la implementación y el mantenimiento del enfoque personalizado de la entidad para demostrar la eficacia del control, pero no reemplazan las pruebas realizadas por el asesor. El asesor debe realizar pruebas independientes y basar sus conclusiones de validación en los resultados de dichas pruebas. Si el asesor determina que las pruebas realizadas por la entidad proporcionaron una evaluación exhaustiva del control, puede utilizar la misma prueba, pero con un conjunto de muestras diferente al utilizado por la entidad.

¿Por qué se requiere más documentación para un enfoque personalizado que para un control compensatorio?

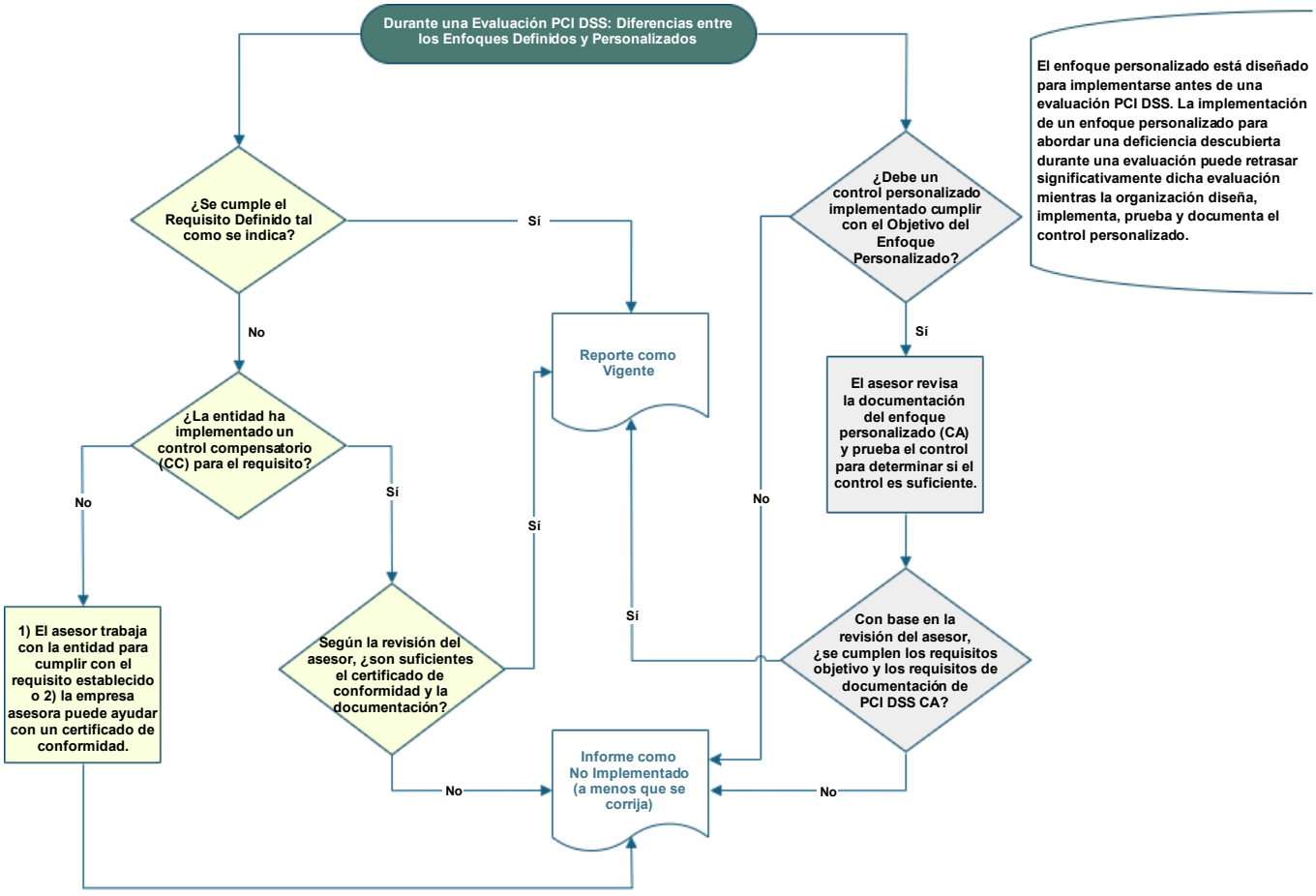
Las implementaciones personalizadas varían según el diseño y el entorno, y son diseñadas íntegramente por la entidad evaluada. Debido a que el control está diseñado por la entidad y, por lo tanto, no está definido en PCI DSS, tampoco existen procedimientos de prueba predefinidos. Por ello, es fundamental que la documentación de la entidad sea exhaustiva: debe definir en qué consiste el control, cómo se implementa,

cuál es el riesgo, cómo se aborda dicho riesgo, cómo la entidad prueba el control, cómo el control cumple el objetivo establecido, cómo la entidad tiene la seguridad de que el control es eficaz de forma continua, etc.

Esta documentación permite al asesor comprender plenamente el control y su funcionamiento, de modo que pueda derivar los procedimientos de prueba adecuados y validar el control de forma independiente.

El siguiente diagrama ilustra cómo difieren el enfoque de los controles compensatorios y el enfoque personalizado durante una evaluación PCI DSS.

Figura 1: En qué se Diferencian el Enfoque Definido y el Enfoque Personalizado Durante una Evaluación PCI DSS.



Documentación de los Controles compensatorios y el Enfoque Personalizado

Se recomienda a las entidades que preparen documentación clara, completa y bien estructurada para sus controles compensatorios o personalizados. Una documentación exhaustiva proporciona a los asesores una base sólida para comprender y evaluar el control, el entorno y cómo el control cumple con la intención del requisito u objetivo de PCI DSS.

La calidad de la documentación de la entidad afecta directamente a la capacidad del asesor para validar los controles y llegar a una conclusión defendible.

Tanto para los controles compensatorios como para las implementaciones personalizadas, la documentación de la entidad debe:

- Ser completa, clara y comprensible para un lector independiente.
- Ser independiente sin depender de un contexto no documentado.
- Demostrar claramente cómo se cumplen los objetivos y se abordan los riesgos.
- Incluya evidencia de cómo la entidad confirmó que el control está funcionando eficazmente, incluyendo detalles sobre los procesos de la entidad y los resultados de validación, pruebas y aseguramiento continuo.

¿Se puede validar un control compensatorio o un enfoque personalizado si la documentación o las pruebas de la entidad son incompletas?

No. Si la documentación no es suficiente, es posible que el asesor no pueda validar que el control esté diseñado y funcione de manera efectiva. Si la entidad no proporciona pruebas suficientes al asesor, o si el asesor no tiene la certeza de que la documentación y los controles de la entidad sean suficientes, el asesor puede determinar si una conclusión de "No Implementado" es el resultado apropiado.

Independencia del Asesor

La independencia del asesor es un principio fundamental de las evaluaciones PCI DSS y se aplica por igual a la hora de validar los controles compensatorios y las implementaciones personalizadas. La entidad evaluada es responsable del desarrollo, la implementación y el mantenimiento de los controles compensatorios.

¿Pueden los QSA diseñar o implementar controles en nombre de una organización?

Si bien los empleados QSA pueden ayudar a las entidades con el diseño o la implementación de controles, las empresas QSA deben cumplir con los requisitos de independencia definidos en los *Requisitos de Calificación de QSA* y la *Guía del programa QSA*. Esto incluye contar con controles de separación de funciones para garantizar que los empleados de QSA que realicen o colaboren en una evaluación PCI DSS sean independientes y no estén sujetos a ningún conflicto de intereses.

Constituiría un conflicto de intereses que un empleado de QSA que haya participado en el diseño o la implementación de un control también pruebe, asesore o colabore en la evaluación de un control compensatorio o personalizado. Consulte *FAQ 1562*, Consulte la página de preguntas frecuentes de PCI SSC para obtener más información: "¿Un empleado de QSA que diseña, desarrolla o implementa controles específicos para un cliente también está autorizado a evaluar esos mismos controles?"

Específicamente para el Enfoque Personalizado

Si bien un empleado QSA puede brindar servicios de consultoría relacionados con el enfoque personalizado, una organización que necesita que un QSA diseñe o implemente sus controles personalizados puede no ser una buena candidata para el enfoque personalizado, ya que puede resultar difícil para la organización mantener ese control y garantizar que continúe funcionando de manera efectiva. Una organización con madurez en la gestión de riesgos, compromiso y los recursos necesarios para desarrollar, implementar y mantener sus propios controles personalizados tiene más probabilidades de lograr una eficacia de seguridad a largo plazo con dichos controles.

Cualquier participación de un asesor o de una empresa QSA en el desarrollo de controles compensatorios o personalizados debe documentarse en la Sección 1.4 del Informe de Cumplimiento (ROC).

Referencias y Materiales de Apoyo

Consulte las siguientes secciones y apéndices de PCI DSS v4.x, así como los siguientes documentos de orientación, plantillas y formularios:

Para el Enfoque Personalizado.

- La sección introductoria 8 de PCI DSS v4.x compara los controles compensatorios y el enfoque personalizado y proporciona descripciones generales de ambos enfoques.
- El Apéndice D de PCI DSS v4.x proporciona más detalles sobre el enfoque personalizado, incluyendo los elementos del análisis de riesgo específico requerido y las responsabilidades tanto de la entidad como del asesor.
- En PCI DSS v4.x, *la Figura 5 Comprensión de las Partes de los Requisitos* indica la ubicación dentro de cada requisito para el Requisito de Enfoque Definido y, cuando corresponda, el Objetivo del Enfoque Personalizado.
- El requisito 12.3.2, para un Análisis de Riesgo Específico (TRA) para cualquier requisito PCI DSS que se cumpla con un enfoque personalizado, define los elementos de un TRA para un enfoque personalizado.
- La Plantilla de Informe de Cumplimiento PCI DSS 4.x, la Plantilla de Enfoque Personalizado del Apéndice E.
- *Ejemplo de Plantilla: El Enfoque Personalizado* está disponible en el sitio web de PCI SSC, en la Biblioteca de documentos dentro del apartado de PCI DSS. Este documento incluye lo siguiente:
  - Enfoque personalizado - Ejemplo de Plantilla de Matriz de Control
  - Enfoque Personalizado - Ejemplo de Plantilla de Análisis de Riesgo
- *PCI DSS v4.x: La Guía de Análisis de Riesgos Específicos*: describe los dos tipos diferentes de análisis de riesgos específicos (TRA) incluidos en PCI DSS v4.x.

Para Controles Compensatorios

- Dentro de PCI DSS v4.x:
  - La Sección Introductoria 8 compara los controles compensatorios con el enfoque personalizado y ofrece una visión general de ambos enfoques.
  - *Apéndice B: Controles Compensatorios*, que proporciona la definición y los criterios básicos.
  - *Anexo C: Ficha de Control Compensatorio*, un ejemplo de la hoja de trabajo que las entidades utilizan para definir los controles compensatorios cuando se utilizan para cumplir con un requisito PCI DSS.
- Una *Ficha de Control Compensatorio Adicional*, para que las entidades la utilicen para documentar los controles compensatorios, está disponible en el sitio web de PCI SSC, en la Biblioteca de Documentos dentro del apartado PCI DSS.

Apéndice: Ejemplos de Plantillas de Control Compensatorio y Enfoque Personalizado Completadas

Ejemplo Completado para la Entidad: Ficha de Control Compensatorio

Tenga en cuenta que esto se proporciona únicamente como un ejemplo de una forma de completar una Ficha de Control Compensatorio y no pretende ser un ejemplo de un control real que sea adecuado o recomendado para su uso en ningún entorno específico.

Número y Definición del Requisito: Requisito PCI DSS 8.4.2: La autenticación múltiples factores (MFA) se implementa para todos los accesos al Entorno de Datos de Tarjetahabiente (CDE).

	Información Requerida	Explicación
1. Restricciones	Documente las limitaciones técnicas o de negocios legítimas que impiden la conformidad con el requisito original.	ABC Org opera una plataforma heredada de autorización de pagos (ID del sistema: PCIPAY-AUTH-01) ejecutándose en la versión UNIX propietaria 5.2. Esta plataforma no admite la integración con mecanismos modernos de autenticación múltiples factores (MFA), incluidos los módulos MFA basados en RADIUS, SAML o PAM. La plataforma cuenta con el respaldo del proveedor, pero no puede modificarse sin invalidar dicho respaldo y la integridad del sistema. La sustitución de este sistema está prevista en el marco del proyecto PCIPAY-MODERN-02, cuya finalización está programada para el cuarto trimestre de 2027.
2. Definición de Controles Compensatorios	Defina los controles compensatorios: explique cómo abordan los objetivos del control original y el aumento del riesgo si lo hay.	ABC Org ha implementado los siguientes controles compensatorios: **Aplicación de la Ley de Autenticación múltiples factores (MFA) del *Host* de *Jump*** El acceso a PAY-AUTH-01 está restringido a los *hosts* intermedios administrativos dedicados ubicados dentro del segmento de red VLAN-SEC-ADM. El acceso a los *hosts* intermedios requiere: ▪ ID de usuario único ▪ Autenticación de contraseña ▪ Token de autenticación basado en *hardware* (dispositivo validado por FIPS) ▪ Integración de Autenticación de Active Directory **Controles de Acceso a la Red** Las reglas del *firewall* restringen el acceso a PAY-AUTH-01 exclusivamente desde *hosts* intermedios. El acceso directo desde estaciones de trabajo de usuarios, conexiones VPN u

	Información Requerida	Explicación
		otros segmentos de red está técnicamente impedido. Referencia del conjunto de reglas del *firewall*: FW-RULE-SET-CDE-ADM-V3. **Supervisión y Registro de Sesiones** Todas las sesiones administrativas son: ▪ Registradas de forma centralizada ▪ Reenviadas a la plataforma SIEM empresarial (SecurityLog-SIEM-01) ▪ Almacenadas durante un mínimo de 12 meses. **Registro de la Sesión** Las sesiones administrativas de PAY-AUTH-01 se registran mediante la solución de gestión de acceso privilegiado (PAM) PAM-SEC-01. Los registros de las sesiones se almacenan con fines forenses y de supervisión. **Monitoreo y Alertas de Seguridad** El SIEM genera alertas para: ▪ Intentos de acceso no autorizados ▪ Acceso fuera de las ventanas administrativas definidas ▪ Intentos de escalada de privilegios Las alertas son revisadas por personal del SOC.
3. Objetivo	Defina el objetivo del control original.	Para garantizar una autenticación sólida para el acceso al CDE mediante el uso de factores múltiples de autenticación.
	Identifique el objetivo que cumple el control compensatorio. ***Nota**: Este puede ser, pero no es obligatorio que sea, el objetivo del enfoque personalizado indicado en PCI DSS para este requisito.*	El control compensatorio logra el objetivo del requisito al aplicar la autenticación múltiples factores (MFA) antes de otorgar acceso a PCIPAY-AUTH-01 e impedir el acceso directo al sistema.
4. Riesgo Identificado	Identifique cualquier riesgo adicional que suponga la falta del control original	Los riesgos asociados a la imposibilidad de implementar la autenticación múltiples factores directamente en PCIPAY-AUTH-01 incluyen: ▪ Posible vulneración de las credenciales de autenticación ▪ Acceso no autorizado a los sistemas de datos de tarjetahabiente. Los controles compensatorios implementados mitigan este riesgo al garantizar: ▪ La autenticación MFA se aplica antes del acceso. ▪ Que el acceso directo está prohibido. ▪ Que todos los accesos son monitoreados, registrados y revisados. Que el riesgo residual se considera Bajo.

	Información Requerida	Explicación
5. Validación de Controles Compensatorios	Defina cómo se validaron y comprobaron los controles compensatorios.	La entidad valida la efectividad del control compensatorio mediante: ▪ Revisiones trimestrales de las reglas del cortafuegos (Evidencia: Informes-Revisión de FW) ▪ Revisiones trimestrales de acceso privilegiado (Evidencia: Acceso-Revisión-Registros) ▪ Verificación trimestral del cumplimiento de la Ley de Asistencia al Usuario en los *hosts* intermedios. ▪ Verificación de la revisión mensual de alertas SIEM ▪ Auditoría interna anual de los controles de acceso privilegiado La entidad revisó esta evidencia de validación para confirmar que el control es efectivo: ▪ Configuraciones de *Firewall* ▪ Configuraciones de control de acceso ▪ Informes de alerta de SIEM ▪ Registros de grabación de sesión
6. Mantenimiento	Definir los procesos y controles establecidos para mantener los controles compensatorios.	La entidad mantiene la efectividad de los controles compensatorios mediante: ▪ Procedimientos de gestión de cambios que rigen los cambios de configuración del firewall y del *host* intermedio. ▪ Monitorización continua de SIEM ▪ Revisiones de acceso trimestrales ▪ Revisión anual de la aplicabilidad del control compensatorio Propietario de la revisión de control compensatorio: Director de Seguridad de la Información Frecuencia de revisión: Anual

Ejemplo Completado para la Entidad: Matriz de Controles para el Enfoque Personalizado

Nota esto se proporciona únicamente como un ejemplo de una forma de completar una Matriz de Controles para un enfoque personalizado y no pretende ser un ejemplo de un control real que sea adecuado o recomendado para su uso en algún entorno específico.

Plantilla de la Matriz de Controles para el Enfoque Personalizado – Ejemplo Completado **Debe ser completado por la entidad que está siendo evaluada**		
Nombre/identificador del control personalizado	Identificación y Autenticación por Voz	
Número de los de los requisitos y objetivos PCI DSS que se cumplen con estos controles	Requisito #: 8.2.8	Objetivo: Una sesión de usuario solo puede ser utilizada por el usuario autorizado.
Detalles del control		
¿**Cuáles** son los controles implementados?	La entidad opera un entorno “sin contacto” con fines de higiene operativa. En lugar de iniciar sesión mediante un teclado, los usuarios en un entorno particular solo emiten comandos verbales a su computadora. Al iniciar sesión por primera vez en un sistema, el usuario emite el comando de voz "Reconocer Nombre de Usuario", por ejemplo, "Reconocer a Alice". El sistema primero identifica y autentica al usuario mediante su huella de voz única y mediante una llamada al sistema de control de acceso físico, que valida que el usuario se encuentra físicamente en el entorno. A continuación, se le pedirá al usuario (por ejemplo, Alice) que repita tres palabras aleatorias que aparecen en la pantalla para anular la grabación previa y también se realizará una segunda comprobación de la huella de voz. En ese momento, el usuario ya ha iniciado sesión. El sistema escucha continuamente los comandos de voz. La sesión del usuario que ha iniciado sesión permanece activa mientras el usuario se encuentra en la zona física; finaliza una vez que el usuario utiliza su tarjeta de acceso para abandonar la zona. Cada vez que el usuario emite un comando, se valida su huella de voz. Si no coincide con la del usuario que ha iniciado sesión, se rechaza y se registra. Los registros son procesados por el SIEM. Si otro usuario intenta utilizar la terminal en la que el usuario ha iniciado sesión, la huella de voz no coincidirá y el sistema rechazará el comando. Por ejemplo, si Dave (que es un usuario autorizado del sistema, pero que no ha iniciado sesión en la terminal de Alice) o Mary (una atacante maliciosa) se acercan al sistema de Alice y dicen "Abre las puertas de la bahía de cápsulas",	

Plantilla de la Matriz de Controles para el Enfoque Personalizado – Ejemplo Completado Debe ser completado por la entidad que está siendo evaluada	
	el ordenador reconocerá que la orden no ha sido emitida por Alice y dirá "Me temo que no puedo hacer eso", y también registrará un intento de acceso no autorizado. Además, las interfaces USB y Bluetooth están desactivadas en los sistemas, por lo que el sistema de reconocimiento de voz no se puede desactivar manualmente.
¿**Dónde** se implementan los controles?	Instalación de producción 17. Nevada.
¿**Cuándo** se realizan los controles?	Cada vez que se analiza una solicitud de voz.
¿**Quién** tiene la responsabilidad general y rinde cuentas de los controles?	La Jefatura de Seguridad de la Información
¿**Quién** participa en la gestión, el mantenimiento y el monitoreo de los controles?	El departamento de registro de operaciones seguras es responsable de la incorporación de nuevos usuarios del sistema, lo que incluye la capacitación de los usuarios y la obtención de suficientes muestras de voz para establecer una huella de voz confiable. La gestión y el mantenimiento del sistema se subcontratan a Acme Voiceprint Security Technologies, que se gestiona de acuerdo con el requisito 12.8 y también proporciona esta tecnología a muchas instituciones financieras líderes para la detección y validación de fraudes, y el acceso a la información del cliente en los centros de contacto.
Para cada **requisito PCI DSS para el cual se utilicen los controles, la entidad proporciona detalles de lo siguiente:**	
La entidad describe cómo los controles implementados cumplen con el ***objetivo*** del requisito PCI DSS.	Solo el usuario que ha iniciado sesión puede usar una sesión, ya que el usuario se vuelve a autenticar (mediante biometría de huella de voz) cada vez que se emite un comando. Otros usuarios autorizados y no autorizados no pueden utilizar la sesión iniciada.
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.	Se encargó una evaluación de seguridad a Acme Secure Testing Services para validar el funcionamiento del sistema e intentar obtener acceso no autorizado a la sesión de un usuario. No lograron hacerlo. Por otra parte, la misma empresa llevó a cabo un ejercicio de equipo rojo y tampoco pudo vulnerar el sistema ni obtener acceso no autorizado haciéndose pasar por un usuario autorizado que utiliza la voz.
La entidad describe brevemente los resultados del análisis de riesgos independiente **que realizó,** el cual explica los controles implementados y describe cómo los resultados verifican que los controles proporcionen al menos un nivel de protección equivalente al enfoque definido para el requisito PCI DSS aplicable. Consulte la Plantilla de	Con el control de requisitos definido, un usuario que haya iniciado sesión podría abandonar su estación de trabajo y un atacante no autorizado tendría 15 minutos para acceder a ella antes de que se cierre la sesión. Con este control, la sesión permanece siempre activa cuando el usuario se encuentra físicamente en el entorno, y la huella de voz de

Plantilla de la Matriz de Controles para el Enfoque Personalizado – Ejemplo Completado Debe ser completado por la entidad que está siendo evaluada	
Análisis de Riesgos Específicos para obtener detalles sobre cómo documentar este análisis de riesgos.	cada comando se válida para comprobar que proviene del usuario que ha iniciado sesión antes de que se ejecute. Por lo tanto, el sistema aborda un nivel de riesgo mayor que el control de validación definido.
La entidad describe las medidas que ha implementado para garantizar que los controles se mantengan y que su eficacia esté asegurada de forma continua. *Por ejemplo, la forma en la que la entidad supervisa la eficiencia en el control, la forma en la que se detectan y responden las fallas de control, y las acciones que se toman.*	Mensualmente, un miembro del equipo GRC intentará tomar el control de la sesión de un usuario emitiendo comandos de voz en las instalaciones y utilizando grabaciones de voz pregrabadas. Este ejercicio sigue un procedimiento documentado y el sistema graba los resultados en audio. El responsable de Gobernanza, Riesgo y Cumplimiento revisa las grabaciones de audio y los registros de procedimientos después de cada prueba. Existe un procedimiento para informar sobre incidentes sospechosos. Si un usuario sospecha que el sistema respondió a una voz que no pertenecía a una persona registrada, tiene un procedimiento que seguir. Todos los usuarios han recibido capacitación sobre el uso de este procedimiento y han completado un informe de incidentes ficticio. El uso de este procedimiento está incluido en la capacitación anual de seguridad del usuario. Hasta ahora, no se han reportado incidentes.

Ejemplo Completado para la Entidad: Análisis de Riesgos Específico para un Enfoque Personalizado

Nota esto se proporciona únicamente como ejemplo de una forma de completar un Análisis de Riesgo Específico para un enfoque personalizado, y no pretende ser el ejemplo de un control real que sea adecuado o recomendado para su uso en algún entorno específico.

Análisis de Riesgo Específico para el Enfoque Personalizado – Ejemplo Completado Debe ser completado por la entidad que está siendo evaluada	
Artículo	**Detalles**
1. Identificar el requisito	
1.1 Identifique el requisito PCI DSS tal como está escrito.	8.2.8 Si la sesión de un usuario ha estado inactiva durante más de 15 minutos, el usuario debe volver a autenticarse para reactivar la terminal o la sesión.
1.2 Identifique el objetivo del requisito PCI DSS tal como está escrito.	Una sesión de usuario solo puede ser utilizada por el usuario autorizado.
1.3 Describa el problema que se pretende evitar con este requisito.	Un atacante, ya sea interno o externo, puede tomar el control de la sesión desatendida de un usuario legítimo. El atacante podría realizar actividades, acceder a datos y emitir comandos, que se atribuirían erróneamente al usuario que ha iniciado sesión. Podría producirse un acceso no autorizado a los sistemas y a los datos. Los archivos de registro serían inexactos, ya que registrarían la identidad del usuario que ha iniciado sesión para actividades que este no realizó.
2. Describa la solución propuesta	
2.1 Identificador/nombre de control personalizado	Identificación y Autenticación por Voz
2.2 ¿Qué partes del requisito, tal como está escrito, cambiarán en la solución propuesta?	El sistema en uso no distingue específicamente entre estados activos e inactivos, por lo que no tiene la capacidad de detectar si una sesión ha estado "inactiva" durante 15 minutos. En cambio, un usuario que ha iniciado sesión puede dar un comando de voz al sistema en cualquier momento después de haberse autenticado e iniciado sesión; sin embargo, cada comando emitido se verifica para asegurar que fue dado por el usuario que ha iniciado sesión. Solo se aceptan los comandos emitidos por el usuario que ha iniciado sesión.
2.3 ¿Cómo evitará el daño la solución propuesta?	Dado que cada comando de voz se verifica antes de ejecutarse, cualquier comando emitido por alguien que no sea el usuario que ha iniciado sesión no aprobará la verificación y el sistema no lo procesará. Esto impide, por lo tanto, que un atacante, ya sea interno o externo, pueda tomar el control de la sesión desatendida de un usuario legítimo.

Análisis de Riesgo Específico para el Enfoque Personalizado – Ejemplo Completado Debe ser completado por la entidad que está siendo evaluada						
Artículo	**Detalles**					
3. Analice cualquier cambio en la PROBABILIDAD de que ocurra el daño, lo que lleva a una violación 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.	Cada comando recibido por el sistema se válida para comprobar que ha sido emitido por el usuario que inició sesión. Esto reduce la probabilidad de que un atacante se apodere de una sesión iniciada. Con el requisito definido, un atacante dispone de un lapso de 15 minutos para acceder físicamente a una sesión autenticada no supervisada y tomar el control de la misma. En los controles implementados, no existe alguna posibilidad de que un atacante pueda emitir comandos durante la sesión de un usuario que haya iniciado sesión.					
3.2 Describa las razones por las que el daño puede seguir ocurriendo después de la aplicación del control personalizado.	El sistema ha sido sometido a pruebas exhaustivas y no se ve superado por soluciones tecnológicas como la síntesis de voz y la reproducción de grabaciones, y se prevé que incluso los intentos de este tipo serían detectados por el usuario que inició sesión, quien debe estar físicamente presente en el entorno para mantener su sesión iniciada. Un atacante podría eludir el control mediante la intimidación física del usuario que inició sesión; sin embargo, el sistema está equipado con un monitor de estado de emergencia que no proporciona ninguna indicación de activación al usuario, pero alerta al personal de seguridad. En las pruebas y evaluaciones de seguridad, el sistema no ha podido ser vulnerado por un atacante simulado.					
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?	Es más probable que ocurran eventos maliciosos	☐	No haya cambios	☐	Es menos probable que ocurran eventos maliciosos	☒
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.	El lapso de 15 minutos permitido por el requisito de que un atacante tome el control de la sesión del usuario que ha iniciado sesión se reduce a cero minutos, ya que cada comando se valida como proveniente del usuario conectado.					

Análisis de Riesgo Específico para el Enfoque Personalizado – Ejemplo Completado Debe ser completado por la entidad que está siendo evaluada				
Artículo	**Detalles**			
4. Analice cualquier cambio en el IMPACTO del acceso no autorizado a los datos del titular de la tarjeta				
4.1 Para el alcance de los componentes del sistema que cubre esta solución, ¿qué volumen de datos del titular de la tarjeta estaría en riesgo de acceso no autorizado si la solución fallara?	**4.1.1** Número de los PAN almacenados	Ninguno. La entidad no almacena el PAN.	**4.1.2** Número de PAN procesados o transmitidos durante un período de 12 meses	32 millones
4.2 Descripción de cómo los controles personalizados directamente: Reducirán la cantidad de datos PAN individuales vulnerados si un agente de amenazas tiene éxito, y/o Permitirán una notificación más rápida de los datos PAN vulnerados con las marcas de tarjetas.	Los controles implementados no reducen el impacto del acceso no autorizado a los datos del titular de la tarjeta.			
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 PCI DSS aplicable.	[Firma]			
5.2 Este análisis de riesgos deberá revisarse y actualizarse a más tardar el:	[Fecha]			

Ejemplo Completado para el Asesor: Informe de Cumplimiento — Apéndice E Plantilla de Enfoque Personalizado

Tenga en cuenta que esto se proporciona únicamente como un ejemplo de una forma de completar el Informe de Cumplimiento y no pretende ser el ejemplo de un control real que sea adecuado para, o recomendado para su uso en algún entorno específico.

Número y Definición del Requisito: Requisito PCI DSS 8.2.8: Si una sesión de usuario ha estado inactiva durante más de 15 minutos, se requiere que el usuario vuelva a autenticarse para reactivar la terminal o la sesión.

Informe de Cumplimiento Plantilla para el Enfoque Personalizado – Ejemplo completado **Debe ser completado por el asesor**	
Identifique el nombre/identificador de control personalizado en cada control utilizado para cumplir con el objetivo del enfoque personalizado. *(**Nota**: utilice el nombre del Control Personalizado de la matriz de controles de la entidad evaluada.)*	Identificación y Autenticación por Voz
Describa cada control utilizado para cumplir el objetivo del enfoque personalizado. *(**Nota**: Consulte los Requisitos y Procedimientos de Prueba del Estándar Payment Card Industry Data Security Standard (PCI DSS) para el Objetivo del Enfoque Personalizado.*	Objetivo: Una sesión de usuario solo puede ser utilizada por el usuario autorizado. 1. Los usuarios inician sesión en el sistema utilizando únicamente comandos verbales. El sistema primero identifica y autentica al usuario mediante su huella de voz única y mediante una llamada al sistema de control de acceso físico, que valida que el usuario se encuentra físicamente en el entorno. A continuación, el sistema le pide al usuario que repita tres palabras aleatorias que aparecen en la pantalla para anular la pregrabación y realiza una segunda comprobación de la huella de voz. 2. El sistema escucha continuamente comandos de voz. La sesión del usuario que inició sesión permanece activa mientras el usuario se encuentra en la zona física; finaliza una vez que el usuario utiliza su tarjeta de acceso para abandonar la zona. 3. Cada vez que el usuario emite un comando, se valida su huella de voz. Si no coincide con la del usuario que ha iniciado sesión, se rechaza y se registra. Los registros son procesados por el SIEM. 4. Si otro usuario intenta usar la terminal en la que el usuario ha iniciado sesión, la huella de voz no coincidirá y el sistema rechazará el comando. 5. Las interfaces USB y Bluetooth están deshabilitadas en los sistemas, por lo que el sistema de reconocimiento de voz no se puede omitir manualmente.

Informe de Cumplimiento Plantilla para el Enfoque Personalizado – Ejemplo completado Debe ser completado por el asesor	
Describa cómo los controles cumplen con el objetivo del enfoque personalizado.	Objetivo del Enfoque Personalizado: Una sesión de usuario solo puede ser utilizada por el usuario autorizado. Solo el usuario que inició sesión puede usar dicha sesión, ya que el usuario se vuelve a autenticar (mediante biometría de huella de voz) cada vez que se emite un comando. Otros usuarios autorizados y no autorizados no pueden utilizar la sesión iniciada.
Identifique la documentación de la Matriz de Controles revisada que respalda un enfoque personalizado para este requisito.	Doc-10 – Matriz de Controles de Enfoque Personalizados
Identifique la documentación del Análisis de Riesgos Específico que se revisó y que respalda el enfoque personalizado para este requisito.	Doc-11 – Enfoque Personalizado TRA
Identifique el nombre o los nombres de los asesores que certifican que: La entidad completó la Matriz de Controles incluyendo toda la información especificada en la Plantilla de Matriz de Controles en PCI DSS v4.x: En el sitio web de PCI SSC se encuentran disponibles Plantillas de Ejemplo para Respaldar un Enfoque Personalizado, y los resultados de la Matriz de Controles respaldan dicho enfoque para este requisito. La entidad completó el Análisis de Riesgos Específico, incluyendo toda la información especificada en la Plantilla de Análisis de Riesgos Específico en PCI DSS v4.x: Plantillas de Ejemplo para Respaldar el Enfoque Personalizado en el sitio web de PCI SSC, y que los resultados del análisis de riesgos respaldan el uso del enfoque personalizado para este requisito.	Josephine, Asesora
Describa los procedimientos de prueba derivados y realizados por el asesor para **validar que los controles implementados cumplen con el objetivo del enfoque personalizado;** por ejemplo, si los controles personalizados son suficientemente robustos para proporcionar al menos un nivel de protección equivalente al proporcionado por el enfoque definido. ***Nota 1**: Siempre que sea posible y apropiado, se deben realizar revisiones técnicas (por ejemplo, revisar la configuración, la eficacia operativa, etc.).* ***Nota 2**: Agregue filas adicionales para cada procedimiento de prueba elaborado por el asesor, según sea necesario. Asegúrese de que todas las filas a la derecha del "Procedimiento de prueba derivado del asesor" se copien para cada procedimiento de prueba derivado del asesor que se agregue.*	

Informe de Cumplimiento Plantilla para el Enfoque Personalizado – Ejemplo completado Debe ser completado por el asesor		
Introduzca aquí el procedimiento de evaluación elaborado por el asesor: 1.a) Después de obtener acceso al entorno, intente iniciar sesión en el sistema a través del teclado proporcionado, si está disponible. 1.b) Después de obtener acceso al entorno, intente iniciar sesión en el sistema mediante el comando de voz requerido. 1.c) Después de que el usuario autorizado inicie sesión en el sistema, repita las tres palabras aleatorias que se muestran en la pantalla. 1.d) Después de que el usuario inicie sesión en el sistema, pida a otro usuario autorizado que repita las tres palabras aleatorias que aparecen en la pantalla. 2.a) Con el usuario autorizado presente en la sala, emita una orden de voz con la voz del asesor. 2.b) Después de que el usuario autorizado haya utilizado su tarjeta de acceso para salir del área, emita un comando de voz al sistema, utilizando una grabación de la voz del usuario emitiendo un comando. 3.a) Revise los registros del SIEM para obtener los resultados de las pruebas 1 y 2.	**Identifique qué se evaluó** (por ejemplo, personas entrevistadas, componentes del sistema revisados, procesos observados, etc.) ***Nota**: todos los artículos analizados deben estar identificados de forma unívoca.*	Se realizaron pruebas con la asistencia de Int-1, Int-2 e Int-3 dentro del entorno de la instalación de producción 17 Nevada en *ConsoleA* y *ConsoleB*, donde el Control de Aproximación Personalizado está activo. Hablé con Int-10 para verificar que se detectaron y revisaron las anomalías ocurridas durante las pruebas 1 y 2.
	Identifique todas las pruebas examinadas para este procedimiento de análisis.	Se revisó el documento Doc-22 - registro SIEM para el período de las pruebas 1 y 2.
	Describa los resultados de las pruebas realizadas por el asesor para este procedimiento de prueba y cómo estos resultados verifican que los controles implementados cumplen con el Objetivo del Enfoque Personalizado.	El asesor siguió a un usuario autorizado hasta los entornos que contenían *ConsoleA* y *ConsoleB*. Prueba 5.a) Primero, el asesor revisó las consolas para verificar que las interfaces USB y las capacidades Bluetooth del sistema no estuvieran disponibles. Prueba 1.a) Luego, el asesor observó que no había teclados disponibles para iniciar sesión en ninguna de las consolas. Prueba 1.b) A continuación, el asesor intentó iniciar sesión en el sistema mediante el comando de voz requerido. El sistema mostró un mensaje de error indicando que el asesor no era un usuario autorizado y no podía iniciar sesión. Prueba 1.c) Luego, el asesor observó mientras Int-1 iniciaba sesión en cada consola, tomando nota del uso de un comando de voz que fue aceptado por cada consola. A continuación, el asesor repitió las tres palabras que aparecían en la pantalla de cada consola y observó que el sistema no registraba al usuario y mostraba un error que indicaba que no se reconocía la respuesta de voz del usuario. Prueba 1.d) El asesor observó mientras el participante 2 repetía las tres palabras aleatorias que aparecían en la pantalla. El sistema se negó a permitir que Int-2 accediera al sistema y emitió un aviso de que la huella de voz no coincidía.

Informe de Cumplimiento Plantilla para el Enfoque Personalizado – Ejemplo completado Debe ser completado por el asesor		
3.b) Hable con el personal responsable de revisar el registro SIEM para determinar si registraron alguna anomalía durante las pruebas 1 y 2. 4.a) Probado en 2.b. 5.a) Examine el sistema para comprobar si tiene interfaces USB y capacidades Bluetooth.		Prueba 2.a) Una vez que Int-1 inició sesión correctamente en el sistema, y el sistema pareció responder a los comandos de Int-1 para abrir el archivo xyz, el asesor emitió un comando al sistema para abrir el archivo xyz. El sistema se negó a abrir el archivo y emitió un mensaje de advertencia indicando que la huella de voz no coincidía con la del usuario autorizado. Prueba 2.b y Prueba 4.a) El asesor observó mientras el usuario registrado utilizaba su tarjeta de acceso para salir del entorno. Después de que la persona que había iniciado sesión abandonara el entorno, el asesor intentó enviar un comando al sistema utilizando una grabación del usuario anterior que había enviado un comando al sistema. El sistema rechazó ejecutar el comando y emitió una respuesta indicando que el usuario había cerrado sesión. Prueba 3.a.) El asesor obtuvo los registros SIEM generados durante las pruebas y verificó que el sistema registrara correctamente los intentos fallidos de acceso y de comandos. Prueba 3.b) El asesor entrevistó a Int-10 para verificar que recibió una alerta por el intento de acceso al sistema. El asesor determinó que el control, tal como fue diseñado, funciona según lo previsto y que el diseño parece ser eficaz para limitar la sesión de un usuario únicamente al usuario que obtuvo acceso autorizado.
Documentar los procedimientos de prueba elaborados y realizados por el asesor para **validar que los controles se mantienen para garantizar su eficacia continua**; por ejemplo, cómo la entidad supervisa la eficacia de los controles y cómo se detectan, se responde y se toman las medidas que se toman en caso de fallos en los controles. ***Nota 1:*** *Siempre que sea posible y apropiado, se deben realizar revisiones técnicas (por ejemplo, revisar la configuración, la eficacia operativa, etc.).* ***Nota 2:*** *Agregue filas adicionales para cada procedimiento de prueba elaborado por el asesor, según sea necesario. Asegúrese de que todas las filas a la derecha del "Procedimiento de prueba derivado del asesor" se copien para cada procedimiento de prueba derivado del asesor que se agregue.*		

Informe de Cumplimiento Plantilla para el Enfoque Personalizado – Ejemplo completado Debe ser completado por el asesor		
Introduzca aquí el procedimiento de evaluación elaborado por el asesor: 1) Revise el procedimiento documentado del GRC para probar los controles mensualmente. 2) Revise la fecha y la hora de los resultados de los últimos 12 meses para verificar que las pruebas se realizan mensualmente. 3) Seleccione dos resultados de pruebas registrados para verificar que los controles funcionaron como se esperaba y que el Jefe de GRC revisó los resultados. 4) Revise el procedimiento documentado para informar sobre incidentes sospechosos y verifique que el procedimiento describe suficientemente lo que el personal debe hacer en caso de que el sistema responda a la voz de una persona que no ha iniciado sesión. 5) Revise los materiales de la capacitación anual en seguridad para verificar que todos los usuarios hayan recibido capacitación sobre el uso del procedimiento. 6) Seleccione aleatoriamente cinco informes de incidentes ficticios y revíselos para comprobar que estén completos.	**Identifique qué se evaluó** (por ejemplo, personas entrevistadas, componentes del sistema revisados, procesos observados, etc.). ***Nota**: todos los artículos analizados deben estar identificados de forma unívoca.*	Procedimientos GRC (Doc-3) y resultados de las pruebas de los últimos 12 meses (Doc-4), Entrevisté a Int-1 y revisé los resultados de las pruebas de marzo de 2025 y agosto de 2025 (Doc-16, Doc-17). Se revisó el procedimiento documentado para informar sobre incidentes sospechosos con Int-1. Se revisaron los materiales de capacitación anual en seguridad con los agentes Int-1, Int-2 e Int-3. Se revisaron los informes de incidentes ficticios completados por los investigadores Int-10 a Int-14. Se verificó que no se ha producido ningún incidente en los últimos 12 meses.
	Identifique todas las pruebas examinadas para este procedimiento de análisis.	Prueba 1: Documento-3 Prueba 2: Documento-4 Prueba 3: Documento-16, Documento-17, Intervalo-01 Prueba 4: Documento-20 Prueba 5: Documento-23 Prueba 6: Documentos 50, 51, 52, 53, 54

Informe de Cumplimiento Plantilla para el Enfoque Personalizado – Ejemplo completado Debe ser completado por el asesor		
7) Si se ha producido un incidente verificado, revise el informe de incidentes. Revise todos los informes de incidentes verificados.	**Describa los resultados** de las pruebas realizadas por el asesor para este procedimiento de prueba y cómo estos resultados verifican que los controles implementados se mantienen para garantizar una eficacia continua.	Los procedimientos de GRC para probar los controles mensualmente parecen ser claros y eficaces para determinar que los controles de comandos de voz funcionan según lo previsto. El GRC realizó las pruebas mensualmente, las cuales se registraron según lo descrito en los procedimientos. Los resultados parecían estar adecuadamente documentados, incluyendo la hora de realización, quién realizó la prueba y los resultados de las mismas. Los procedimientos para informar sobre incidentes sospechosos parecen ser claros y adecuados. Los requisitos de presentación de informes incluyen un formulario (Informe de incidentes) que debe ser utilizado por el personal de TI en la instalación de producción 17. Nevada. Se confirmó que todo el personal de Informática en la planta de producción 17. Nevada ha recibido capacitación revisando el registro de capacitación obtenido del departamento de Recursos Humanos. Además, se seleccionaron cinco informes de incidentes ficticios aleatoriamente de los registros de recursos humanos y se comprobó que se habían completado siguiendo los procedimientos establecidos. Se revisó el registro de incidentes obtenido de Int-1 correspondiente a los últimos 12 meses con Int-1. Aunque se registraron incidentes en el registro, ninguno parecía estar relacionado con el control por comandos de voz. Se ha confirmado con Int-1 que no ha habido incidentes relacionados con el control. Por lo tanto, parece que el mantenimiento del control garantiza la eficacia continua de limitar la sesión de un usuario al usuario autorizado que inició sesión en el sistema.