PCI DSS versión 4.0: Cronogramas previstos y últimas actualizaciones

Nuestro enfoque de PCI DSS versión 4.0 se basa tanto en los comentarios de la industria como en los cambios en los pagos, la tecnología y la seguridad. En las conversaciones con las partes interesadas de la industria, hemos recibido varias preguntas sobre PCI DSS versión 4.0. Enseguida entrevistamos a Lauren Holloway, directora de Normas de Seguridad, quien responde algunas preguntas clave sobre qué está sucediendo con PCI DSS versión 4.0.

Nota: *Todas las fechas mencionadas en este artículo se basan en revisiones actuales y están sujetas a cambios.*

¿En qué fase del proceso de elaboración se encuentran PCI DSS versión 4.0?

Lauren Holloway: La solicitud de comentarios (RFC) que tuvo lugar entre octubre y diciembre de 2019 generó más de 3,000 comentarios, y el PCI SSC está revisando y considerando cuidadosamente cada comentario recibido. Se prevé lanzar una nueva RFC entre septiembre y octubre de 2020. Esta RFC incluirá un borrador actualizado de PCI DSS versión 4.0, que estamos preparando con base en los comentarios recibidos en respuesta a la RFC de 2019.

Para mayor información sobre las próximas RFC y el proceso relacionado, consulte nuestra **Página de RFC.**

¿Cuándo se publicarán PCI DSS versión 4.0?

Lauren Holloway: Está previsto publicar la versión final de PCI DSS versión 4.0 a mediados de 2021.

Cabe señalar que el marco para elaborar esta actualización de PCI DSS es notablemente más largo que en las revisiones anteriores. Este marco ampliado tiene por objeto dar cabida a un mayor número de oportunidades para que las partes interesadas hagan comentarios durante el proceso de actualización.

Para mayor información, lea: Tres cosas que debe saber sobre la elaboración de PCI DSS versión 4.0

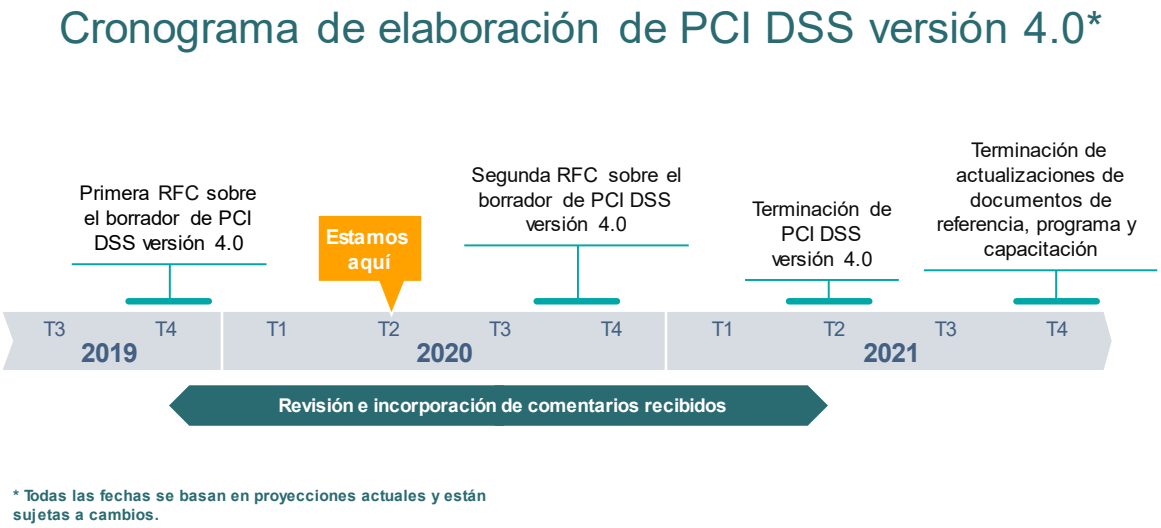
¿Se hará un análisis detallado de los comentarios recibidos en respuesta a la RFC de 2019?

Lauren Holloway: Una vez que hayamos terminado de revisar los más de 3,000 comentarios recibidos y actualizado el borrador de PCI DSS versión 4.0, en el portal de PCI presentaremos un resumen de comentarios a los participantes en el proceso de RFC de 2019. Este resumen estará disponible para los participantes en la siguiente RFC sobre PCI DSS y explicará cómo se abordó cada comentario. Adicionalmente, mantendremos a la comunidad del Consejo de PCI al tanto de las decisiones adoptadas, por medio de nuestras difusiones web y nuestras reuniones comunitarias planificadas para finales de este año.

¿Cuándo se actualizarán los cuestionarios de autoevaluación (SAQ) y qué incluirán las actualizaciones?

Lauren Holloway: Las actualizaciones de los documentos de referencia, incluidos los SAQ, la plantilla para elaborar informes de cumplimiento (ROC), el Glosario de PCI DSS y el enfoque priorizado forman parte del ciclo de revisión siempre que se actualizan PCI DSS. A fines de este año, empezaremos a trabajar en las actualizaciones de toda la documentación justificativa para alinearla con PCI DSS versión 4.0 y presentaremos los avances. Prevemos tener estos documentos listos para su publicación pocos meses después de la de PCI DSS versión 4.0.

A continuación aparece el cronograma actual para la elaboración de PCI DSS versión 4.0, que incluye la RFC y la fecha de terminación de los materiales de dichas normas.



¿Cuánto tiempo tendrán las organizaciones para implementar la versión 4.0 una vez que se publique?

Lauren Holloway: Una vez que se publiquen PCI DSS versión 4.0, se otorgará a las organizaciones un periodo ampliado para la transición de la versión 3.2.1 a la versión 4.0. En apoyo de esta transición, la versión 3.2.1 permanecerá en vigor durante los 18 meses siguientes a la publicación de todos los materiales de la versión 4.0 — es decir, las actualizaciones de las normas, los documentos de referencia (incluidos SAQ, ROC y AOC), la capacitación y el programa.

Nota: *Se prevé finalizar la versión 4.0 seis meses antes de la publicación de las actualizaciones de la documentación justificativa, la capacitación y el programa requeridas para respaldar el uso de PCI DSS. Por lo tanto, la versión 4.0 estará disponible 2 años antes del retiro de la versión 3.2.1.*

Este periodo ampliado dará tiempo para que las organizaciones se familiaricen con los cambios efectuados en la versión 4.0, actualizar sus plantillas y formularios para la elaboración de informes, y planificar e implementar los cambios encaminados a cumplir los requisitos actualizados. Una vez que concluya el periodo de transición, la versión 3.2.1 se retirará y la 4.0 será la única versión vigente.

Aparte del periodo de 18 meses en que estarán vigentes a la vez las versiones 3.2.1 y 4.0, habrá un periodo definido para implementar los nuevos requisitos que se identifican en la versión 4.0 como “posfechados”.

¿Qué son los requisitos “posfechados” y cuándo entrarán en vigor?

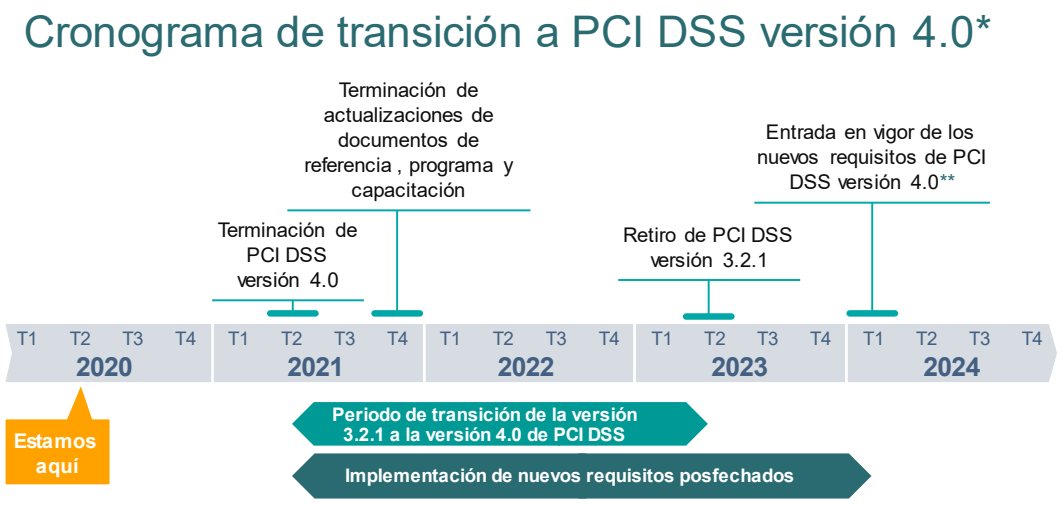
Lauren Holloway: En PCI DSS, los nuevos requisitos a veces se designan con una fecha futura a fin de dar a las organizaciones más tiempo para terminar de implementarlos. Estos requisitos se consideran como mejores prácticas hasta esa fecha futura. Mientras tanto, las organizaciones no tienen que validarlos. Aunque no es obligatorio, a las organizaciones que han implementado controles para cumplir los nuevos requisitos y están listas para someterlos a evaluación antes de la fecha futura establecida, se les alienta a hacerlo. Todos los requisitos posfechados entran en vigor a partir de esa fecha.

Prevemos que PCI DSS versión 4.0 contendrán varios nuevos requisitos posfechados; sin embargo, no sabremos su número hasta que se finalicen las normas.

Si bien la fecha futura de entrada en vigor de estos nuevos requisitos no se confirmará hasta que estén listas para publicación PCI DSS versión 4.0, las organizaciones tendrán tiempo suficiente para planificar e implementar los nuevos controles y procesos de seguridad necesarios para cumplirlos. La fecha futura dependerá del impacto general que los nuevos requisitos tengan en las normas. Según el borrador actual, se

prevé que la fecha futura se fije más allá del periodo de transición, posiblemente entre dos y medio y tres años después de la publicación de PCI DSS versión 4.0.

Enseguida se presenta el cronograma previsto para la transición y la implementación de los requisitos posfechados.



*** Todas las fechas se basan en proyecciones actuales y están sujetas a cambios.**

** Se refiere a los nuevos requisitos posfechados de PCI DSS.
La fecha de entrada en vigor se determinará una vez que se confirmen todos los nuevos requisitos.

Para mayor información, lea: Cómo los comentarios de la industria están configurando el futuro de PCI DSS

¿Se publicará un borrador de PCI DSS versión 4.0 antes de que se finalicen?

Lauren Holloway: Los borradores de las normas se presentan a las partes interesadas para que los revisen y comenten. El borrador siguiente de PCI DSS se someterá a la revisión y los comentarios de las empresas QSA y ASV y las organizaciones participantes durante el próximo periodo de RFC, que será en septiembre/octubre de este año.

Me gustaría participar en la siguiente RFC de PCI DSS versión 4.0. ¿Cómo puedo participar?

Lauren Holloway: Cualquier organización es elegible para participar. Las organizaciones participantes, además de hacer comentarios sobre las normas de seguridad de PCI pueden proponer, votar y participar en grupos de interés especial, asistir a las reuniones comunitarias anuales del PCI SSC con dos pases de cortesía y demostrar a sus clientes y socios de negocios su compromiso con la seguridad de pagos. Para obtener más información sobre los beneficios y **cómo ser una organización participante, haga clic aquí.**

¿Cómo puede prepararse nuestra organización para PCI DSS versión 4.0?

Lauren Holloway: Aunque PCI DSS versión 4.0 todavía están en proceso de elaboración, alentamos a todas las entidades a que sigan implementando con diligencia los controles de seguridad previstos en la versión 3.2.1. Esto no solo les ayudará a mantener la seguridad, sino también les facilitará la transición a la versión 4.0.

Se insta enfáticamente a las organizaciones que han tenido acceso a los primeros borradores a que no intenten implementar ningún requisito nuevo o actualizado antes de que se publiquen PCI DSS versión 4.0 definitivas. Las versiones de la RFC *solo son borradores*, y la versión final de las normas será diferente.

Mayor información sobre PCI DSS versión 4.0