



Informe global de investigación sobre PKI de 2026

PKI bajo presión: el punto de inflexión para la modernización

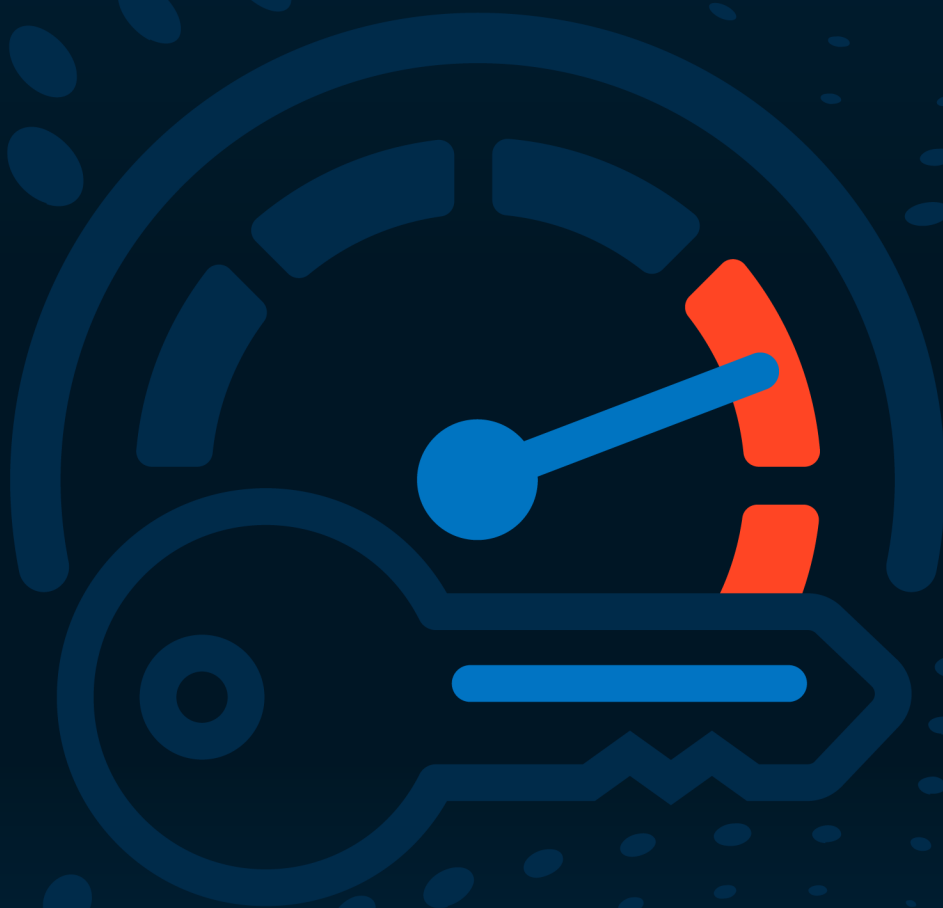


Tabla de contenido

Prólogo de Lakshmi Hanspal, directora de Confianza de DigiCert	3
Resumen ejecutivo	4
El desafío: PKI bajo presión	5
Visibilidad y riesgo	7
Complejidad y madurez	9
Inteligencia artificial y computación cuántica	14
La solución: modernizar la infraestructura de clave pública (PKI).	16
Metodología	17
Autores y colaboradores	18

Prólogo



Lakshmi Hanspal

Directora de Confianza | DigiCert

CIO y responsables de ciberseguridad, operaciones de TI, GRC y producto en todo el mundo. Lo que nos contaron fue a la vez esclarecedor y aleccionador.

La mayoría de las organizaciones comprenden lo que está en juego. Son muchas menos las que han convertido ese conocimiento en acciones concretas.

En DigiCert, no solo estudiamos este problema, sino que lo vivimos. A medida que nuestros entornos se expandían, nos enfrentábamos a las mismas duras realidades. Nuestros equipos tenían una visibilidad limitada de los activos criptográficos, al tiempo que lidiaban con la responsabilidades fragmentadas en la gestión de los certificados y la presión muy real de modernizar la infraestructura sin interrumpir el negocio que se ejecutaba sobre ella. La preparación para la era poscuántica añadió una urgencia que no podíamos ignorar.

Así pues, nos convertimos en nuestro propio cliente cero. Realizamos un inventario de nuestros activos criptográficos, detectamos los certificados no gestionados, automatizamos la gestión del ciclo de vida y comenzamos a reforzar los sistemas críticos para prepararlos para la criptografía resistente a la computación cuántica. Era necesario, y nos brindó una comprensión directa y práctica de lo que las organizaciones enfrentarán en cada etapa de este proceso.

Esto es algo que sé con certeza: no necesita un presupuesto perfecto, una hoja de ruta impecable ni una transformación radical para lograr un progreso real. Lo que necesita es un punto de partida claro, la visibilidad adecuada y el compromiso de dar el siguiente paso.

Este informe le proporciona los datos, los puntos de referencia y una visión honesta de la situación actual del sector. Le invito a utilizarlo, a iniciar la conversación, a fundamentar sus argumentos y a seguir adelante.

Las organizaciones que actúen ahora estarán mejor posicionadas para afrontar los desafíos actuales y, al mismo tiempo, desenvolverse en el panorama criptográfico en constante evolución del mañana.

*Lakshmi
Hanspal*

La modernización de la infraestructura de clave pública (PKI) y la preparación para la era poscuántica ya no son retos del futuro, sino realidades operativas del presente.

Los responsables de seguridad e infraestructuras se enfrentan a una confluencia de fuerzas. Las organizaciones se enfrentan a un mayor número de identidades de máquinas, sistemas más conectados, una mayor incertidumbre impulsada por la IA y plazos cada vez más reducidos para actuar antes de que las vulnerabilidades criptográficas se conviertan en riesgos para el negocio. Todo esto conlleva desafíos de complejidad en un momento en que las interrupciones relacionadas con los certificados y los fallos de confianza se están convirtiendo en una causa cada vez más frecuente de interrupciones del negocio. La agilidad criptográfica ya no es solo deseable: se está convirtiendo rápidamente en un requisito esencial para las operaciones diarias en todos los niveles.

Para comprender la situación actual de las organizaciones, encuestamos a más de 400 responsables de la toma de decisiones de TI y seguridad de alto nivel, incluidos CISO,

Resumen ejecutivo

Esta investigación revela un cambio cada vez más claro entre las organizaciones, que pasan de reconocer los desafíos de la infraestructura de clave pública (PKI) a abordarlos activamente para mejorar la resiliencia operativa.

La infraestructura de clave pública (PKI) está adquiriendo mayor importancia justo en el momento en que su gestión se está volviendo más compleja. La brecha entre la importancia y el nivel de preparación operativa es ahora lo suficientemente amplia como para requerir la atención de la dirección ejecutiva. Los líderes comprenden el riesgo. Lo que muchas organizaciones aún están desarrollando es la visibilidad, la gobernanza y la automatización necesarias para gestionar la infraestructura de clave pública (PKI) como un sistema empresarial en lugar de como un conjunto de soluciones puntuales.



El riesgo de PKI se comprende bien, pero no está bien controlado.

Adam Strange, Analista Principal de Seguridad de Datos en Omdia.

Los 3 desafíos de PKI de hoy

1

El grado de visibilidad determina la exposición al riesgo.

La falta de visibilidad del panorama completo de certificados es el mayor desafío al que se enfrentan las empresas. Solo el 34 % de las organizaciones afirma tener un inventario completo y actualizado de todos sus certificados digitales.

Existe una clara relación entre visibilidad y riesgo. El 73 % de las organizaciones están muy o extremadamente preocupadas por las interrupciones causadas por certificados caducados.

2

La complejidad y la madurez de la infraestructura de clave pública (PKI) dificultan la satisfacción de las crecientes necesidades empresariales.

El 74 % de las organizaciones están preocupadas por la proliferación de certificados, y el 52 % espera que la inversión en infraestructura de clave pública (PKI) aumente en los próximos tres años.

Sin embargo, aunque los profesionales de TI y seguridad reconocen las amenazas y la necesidad de modernizar la infraestructura de clave pública (PKI), muchos tienen dificultades para que las conversaciones sobre recursos y riesgos de PKI lleguen a los responsables de la toma de decisiones.

3

Adaptarse a los rápidos cambios de la IA y a la creciente amenaza cuántica exige agilidad y planificación.

Más del 73 % de las organizaciones afirman que la infraestructura de clave pública (PKI) desempeñará un papel fundamental en el establecimiento de la confianza para los casos de uso de la IA.

La preparación ante la computación cuántica es deficiente, ya que solo el 22 % ha evaluado completamente los sistemas criptográficos para detectar futuras vulnerabilidades relacionadas con la computación cuántica.

La modernización de la infraestructura de clave pública (PKI) ofrece soluciones a estos desafíos.

La necesidad operativa de modernizar la infraestructura de clave pública (PKI) es cada vez más evidente, pero muchas organizaciones aún se encuentran en las primeras etapas de su implementación. Dado que la modernización puede ser compleja, la mayoría de las empresas adoptan un enfoque por fases. Estas organizaciones consideran que el éxito depende de la reducción de los procesos manuales, la mejora de la visibilidad y el acceso a los conocimientos especializados y al apoyo operativo necesarios.

El impacto de la modernización de PKI

Las organizaciones que han modernizado su infraestructura de clave pública (PKI) reportan una reducción del 60 % en las interrupciones del servicio.



Introducción

PKI bajo presión

La infraestructura de clave pública (PKI) está bajo presión porque el entorno operativo que dio forma al modelo operativo de ayer ya no es válido.

El volumen de certificados está aumentando, las identidades no humanas proliferan, los ciclos de vida de los certificados se acortan y el número de sistemas que dependen de la confianza criptográfica sigue creciendo. Al mismo tiempo, el cumplimiento normativo y las exigencias del sector están incorporando la infraestructura de clave pública (PKI) al ámbito de aplicación, responsabilizando a los líderes por resultados como el tiempo de actividad, la resiliencia y la gobernanza de la IA.

Esta combinación está transformando la infraestructura de clave pública (PKI) de una infraestructura de soporte a una capacidad estratégica cuya implementación, supervisión y gestión recaen directamente en los responsables de TI y seguridad.

Cómo utilizar este informe

Los datos de este informe se centran en el liderazgo en las operaciones diarias de PKI. Mediante una encuesta a los altos directivos que implementan la infraestructura de clave pública (PKI) en sus empresas, analizamos la situación actual de la PKI y lo que debe hacerse para que siga siendo eficaz en el futuro.

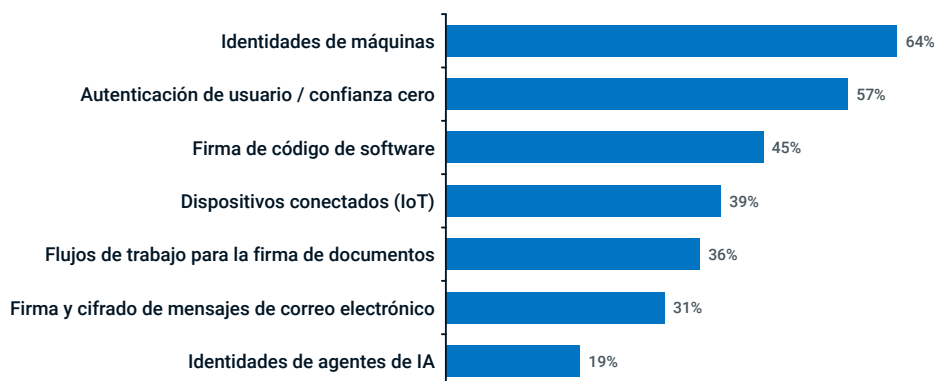
Los siguientes resultados le ayudarán a ver el estado actual de las operaciones de PKI, a comparar su organización con los promedios y a proporcionarle datos y consideraciones para su propia planificación, tanto internamente como con los responsables de la toma de decisiones en toda su organización.

Comprender la infraestructura de clave pública (PKI) empresarial actual.

Antes de analizar la infraestructura de clave pública (PKI) desde la perspectiva de los tres desafíos más importantes, primero veremos cómo se utiliza la PKI en las organizaciones actuales. Los datos demuestran que la infraestructura de clave pública (PKI) se ha expandido mucho más allá de los certificados web públicos. La identidad de las máquinas, la autenticación de usuarios y las iniciativas de confianza cero son componentes importantes de la infraestructura de clave pública (PKI) en más de la mitad de los encuestados, con una cobertura significativa en otros casos de uso no web, como la firma de código, el IoT y de contenido.

Estos hallazgos demuestran por qué las organizaciones están sumamente preocupadas por las interrupciones del servicio, ya que la infraestructura de clave pública (PKI) proporciona cifrado, identidad, autenticación y mucho más a una amplia gama de infraestructuras empresariales críticas, mucho más allá de los servidores web de acceso público.

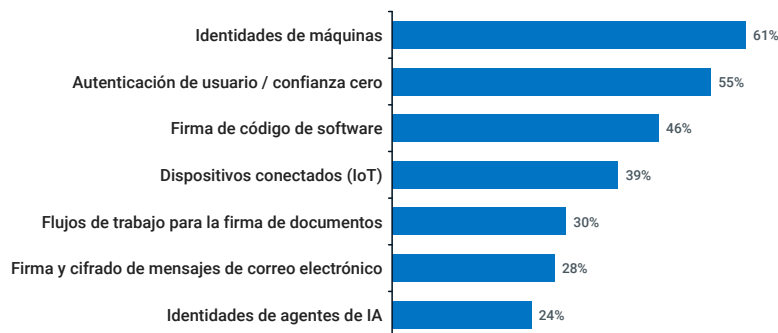
¿Cuál de las siguientes opciones cubre su infraestructura PKI actual?



Prioridades para la modernización de la infraestructura de clave pública (PKI)

Como era de esperar, encontramos una correlación entre el uso de la infraestructura y las prioridades de modernización de la PKI. Casi tres cuartas partes de los encuestados están muy preocupados por las interrupciones causadas por certificados caducados y la proliferación de certificados. Los profesionales comprenden las consecuencias del fracaso y establecen fases de modernización que se corresponden con las áreas de mayor necesidad y mayor riesgo.

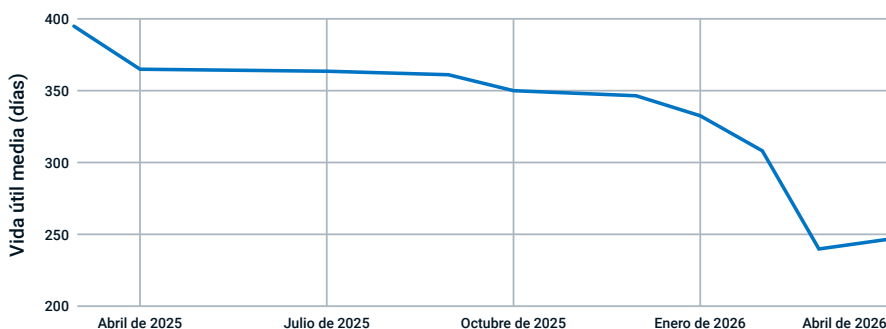
¿Qué áreas ha priorizado su organización para la modernización de la infraestructura de clave pública (PKI)?



La reducción de los ciclos de vida aumenta la presión.

A pesar del aumento de la complejidad, el número de conexiones, identidades y casos de uso, el ciclo de vida de los certificados públicos se está acortando. El sector avanza hacia un período máximo de validez de 47 días para los certificados TLS públicos a partir de marzo de 2029. Esto deja aún menos margen de maniobra para los equipos que todavía dependen de la instalación manual, la propiedad poco clara o las hojas de cálculo como sistema de registro. En muchas organizaciones, la infraestructura de clave pública (PKI) se ha convertido en un ecosistema que se fragmenta más rápido de lo que los equipos pueden integrarlo y gestionarlo.

Mediana mensual de la vida útil de los certificados (2025-2026)



La IA y la computación cuántica complican aún más un sistema ya de por sí complejo.

La IA aumenta la demanda de una mayor seguridad en cuanto a identidad, integridad, procedencia y aplicación de políticas en todo el contenido, los modelos y los agentes. La transición a la criptografía poscuántica aumenta la importancia de la visibilidad y la agilidad en todo el entorno. En conjunto, estos factores demuestran que la modernización de la infraestructura de clave pública (PKI) es una respuesta natural a un problema de confianza que se avecina.

Conclusión clave

La presión sobre la infraestructura de clave pública (PKI) no proviene de una sola fuente. Se trata del efecto acumulativo del crecimiento de la identidad de las máquinas, la reducción de los ciclos de vida de los certificados, la necesidad de una gobernanza de la IA y la preparación para la computación cuántica, que llegan simultáneamente, especialmente cuando la previsión de Gartner sobre el Día Q¹ coincide con el inicio del mandato de un ciclo de vida de certificados de 47 días en 2029.

¹ Resumen de Gartner Insights: Cómo mitigar los riesgos criptográficos que plantea la computación cuántica

Visibilidad y riesgo

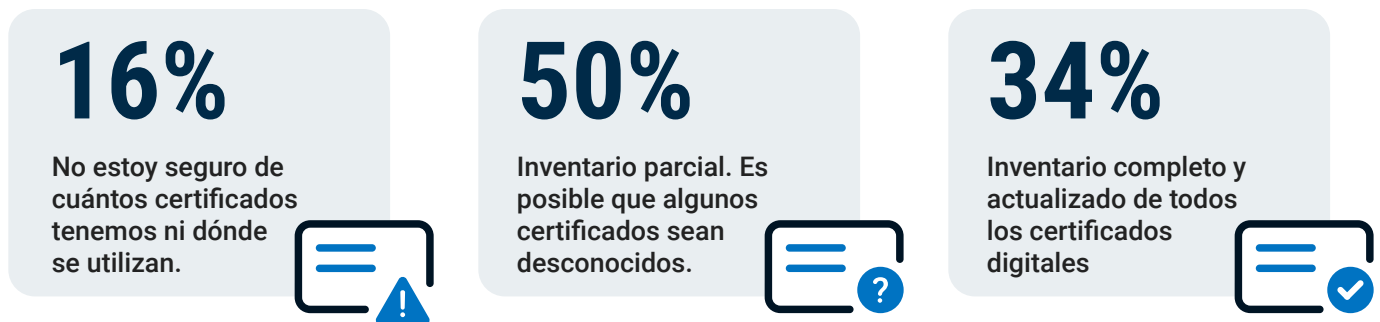
Cuando las organizaciones aumentan la visibilidad, el riesgo disminuye.

Solo un inventario completo del despliegue y el estado de cada certificado en la empresa proporciona la información necesaria para evitar deficiencias, fallos y omisiones.

La visibilidad previene interrupciones y ataques.

El estudio deja clara una cuestión: las organizaciones no pueden gestionar eficazmente el riesgo de los certificados sin visibilidad. Los resultados muestran que solo el 34 % de las organizaciones afirma tener un inventario completo y actualizado de todos sus certificados digitales. Esto significa que dos tercios de las organizaciones solo tienen un inventario parcial, ningún inventario o no tienen una visión clara de su entorno de certificados. El hecho de que un solo certificado caducado pueda paralizar toda una aplicación empresarial explica por qué el riesgo es tan alto cuando los inventarios están incompletos.

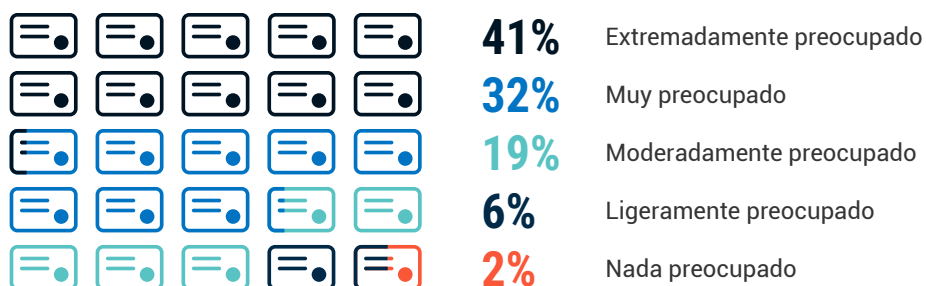
¿Qué describe mejor el conocimiento y el seguimiento que su organización hace de los certificados digitales que utiliza actualmente?



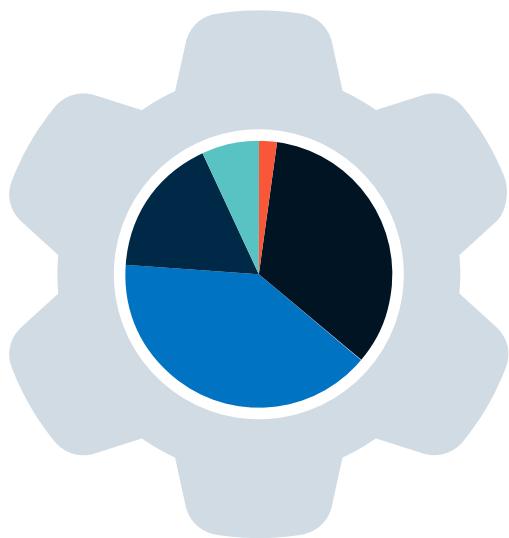
Esta preocupación no pasa desapercibida para los líderes. Casi tres cuartas partes de los encuestados están muy o extremadamente preocupados por las interrupciones del servicio debidas a certificados caducados, y casi la misma proporción está muy o extremadamente preocupada por la proliferación de certificados. En conjunto, estos hallazgos describen una tensión empresarial común: las organizaciones comprenden las consecuencias de un fallo en un certificado, pero muchas aún carecen de la visibilidad necesaria para prevenirlo de forma sistemática.

Además, aproximadamente la mitad de los encuestados también mencionan soluciones aisladas que son difíciles de gestionar, y el 47 % señala el seguimiento mediante hojas de cálculo, propenso a errores. En otras palabras, la brecha de visibilidad no se trata solo de un descubrimiento incompleto. También es el resultado de herramientas fragmentadas, propiedad fragmentada y procesos fragmentados.

¿Hasta qué punto le preocupa la proliferación de certificados en su organización a medida que aumenta el número de sistemas/identidades?



¿Hasta qué punto le preocupa la proliferación de certificados en su organización a medida que aumenta el número de sistemas/identidades?



40% Extremadamente preocupado

34% Muy preocupado

17% Moderadamente preocupado

6% Ligeramente preocupado

2% Nada preocupado

4100 millones

certificados públicos emitidos en 2025

Esto supone un aumento del 55 % con respecto al año anterior, cuando se emitieron 2.600 millones de certificados a nivel mundial a lo largo de 2024, según los registros de transparencia pública. Se están emitiendo certificados internos a un ritmo mucho mayor.



Las herramientas y los procesos adecuados aumentan la visibilidad al tiempo que reducen el riesgo.

A pesar de la variabilidad en la implementación de la modernización, los encuestados fueron claros sobre lo que constituye una mejor infraestructura de clave pública (PKI). Una mejor monitorización y un mayor control sobre los certificados, una visibilidad centralizada, el ahorro de tiempo y una menor cantidad de interrupciones se traducen en una gestión más sencilla y eficaz con menor riesgo. Observamos que la visibilidad centralizada y una vista unificada siguen consolidándose como prioridades principales para las organizaciones que gestionan la complejidad de la infraestructura de clave pública (PKI).

Por eso, el detección y el inventariado deben considerarse el primer paso en la modernización. Un inventario fiable es la forma en que las organizaciones pasan de las suposiciones a las pruebas. Permite a los equipos asignar responsabilidades, identificar las dependencias de renovación, priorizar la automatización y comprender dónde será más difícil lograr la agilidad criptográfica. Sin esa visibilidad, cualquier otro esfuerzo de modernización se basa en información parcial.

Conclusión clave

La visibilidad ayuda a abordar los riesgos de las interrupciones relacionadas con los certificados y sienta las bases para la modernización de la infraestructura de clave pública (PKI).

Complejidad y madurez

La complejidad y la baja madurez son las principales causas de los problemas de visibilidad y del riesgo.

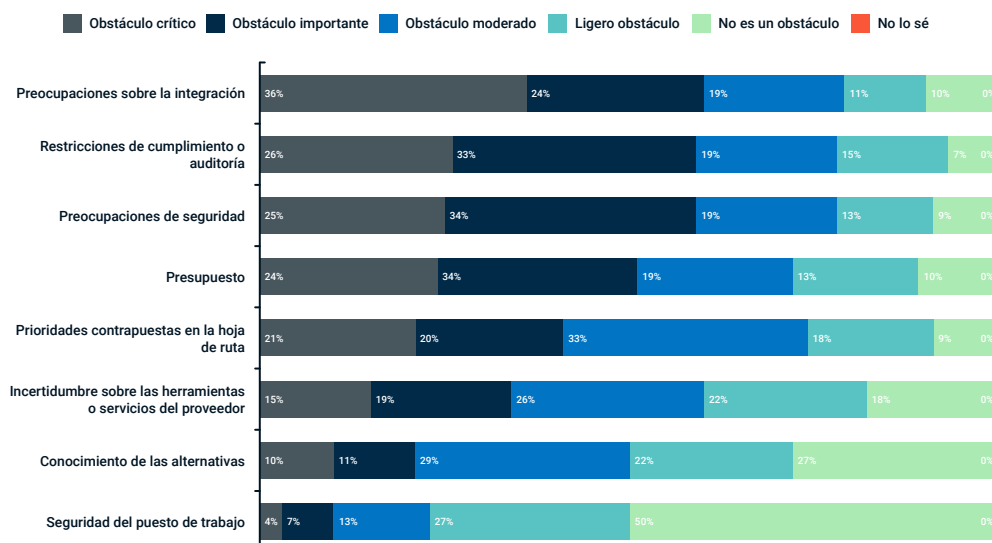
La infraestructura de clave pública (PKI) fragmentada y la gestión fragmentada de la PKI dificultan cada vez más el control de la proliferación de certificados.

La complejidad es un desafío tanto estructural como técnico.

La complejidad es la razón de los persistentes problemas de visibilidad. La infraestructura de clave pública (PKI) se ha vuelto estructuralmente compleja, no solo técnicamente compleja. El problema no radica simplemente en que una integración sea difícil o que un flujo de trabajo sea engorroso. El problema radica en que la confianza digital se ha expandido a través de infraestructuras de clave pública (PKI) públicas y privadas, servicios en la nube, autoridades de certificación heredadas, identidades de máquinas, firma de código, dispositivos conectados y plataformas especializadas más rápido de lo que la mayoría de las organizaciones han podido integrarla y gestionarla.

Los encuestados manifiestan su preocupación por una variedad de cuestiones que abarcan todo tipo de complejidad. Las preocupaciones relacionadas con la integración figuran entre los principales obstáculos para el progreso operativo, pero los profesionales también mencionaron problemas relacionados con la seguridad y el cumplimiento normativo, además del presupuesto, la planificación y otros. Aquí vemos que las organizaciones no se enfrentan a un único obstáculo. La implementación y el funcionamiento de una infraestructura de clave pública (PKI) mejorada se ven dificultados por una compleja red de dependencias: arquitectónicas, procedimentales y organizativas.

¿En qué medida los siguientes factores representan un obstáculo para la adopción de la gestión automatizada de certificados por parte de su organización?



¿Qué desafíos ha experimentado o prevé experimentar al implementar la modernización de la infraestructura de clave pública (PKI)?

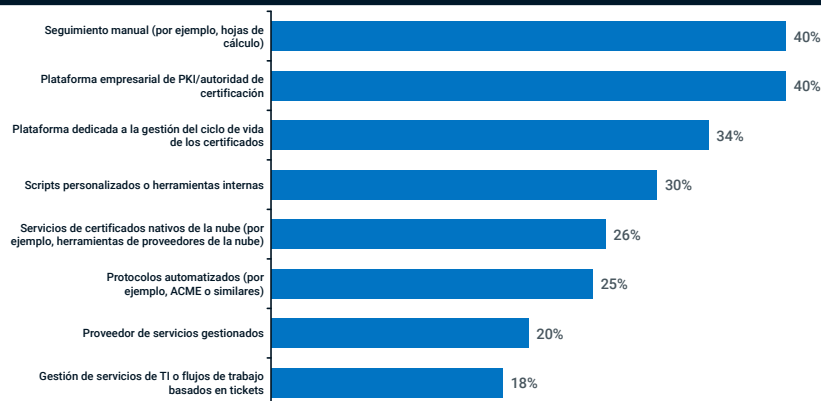


Los múltiples procesos de gestión de certificados no satisfacen las necesidades de la empresa

Muchas empresas no operan con un modelo unificado de gestión de certificados. Están utilizando varios métodos simultáneamente, y el seguimiento manual suele coexistir con soluciones PKI/autoridad de certificación privada empresariales, plataformas de gestión del ciclo de vida de los certificados, scripts personalizados y software de gestión de flujos de trabajo de TI (ITSM).

De media, las empresas utilizan entre dos y tres métodos diferentes al mismo tiempo. Esto significa que muchas organizaciones se encuentran en una fase de transición, pasando de la ausencia total de automatización a la automatización parcial y, finalmente, a la automatización completa. En la práctica, la automatización parcial significa renovar automáticamente los certificados, pero no instalarlos. Si bien esto supone una mejora con respecto a los procesos totalmente manuales, sin una automatización integral, el riesgo de interrupción del servicio sigue siendo alto.

¿Qué métodos/plataformas utiliza actualmente su organización para la gestión de certificados?



Los métodos manuales no pueden solucionar el problema de la proliferación, especialmente las hojas de cálculo.

Las hojas de cálculo han servido de base para la gestión del inventario y el estado de la infraestructura de clave pública (PKI) durante décadas. Son prácticas, familiares y, a menudo, la forma más rápida de mantener a un equipo en movimiento. El problema es que se les está pidiendo que realicen un trabajo para el que nunca fueron diseñados. A medida que aumenta el volumen de certificados y se reducen los plazos de renovación, las hojas de cálculo dejan de ser una herramienta de gestión y comienzan a convertirse en un multiplicador de riesgos.

Antes de que existieran herramientas automatizadas fiables, las hojas de cálculo eran imprescindibles. Sin embargo, hoy en día, las plataformas maduras de gestión del ciclo de vida de los certificados, los estándares de interoperabilidad, los controles de políticas y la instalación automatizada pueden reducir una cantidad significativa de la carga asociada con las hojas de cálculo y otros procesos manuales. La clave está en la secuenciación: racionalizar, integrar y automatizar primero los casos de uso de certificados de mayor valor, en lugar de intentar integrar todo el ecosistema PKI empresarial bajo una única plataforma de automatización de una sola vez.

Conclusión clave

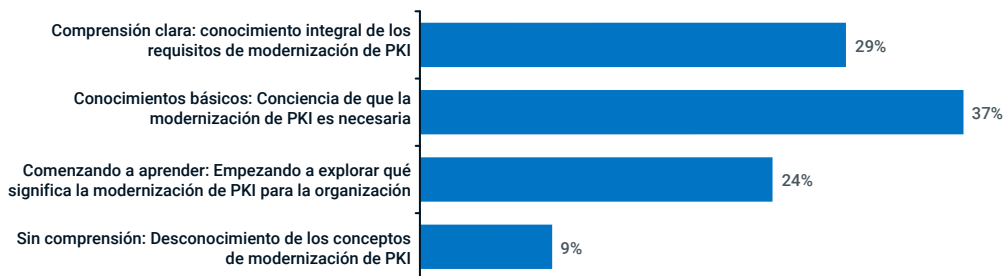
La complejidad supone un reto, pero es manejable. Esto demuestra que la infraestructura de clave pública (PKI) necesita un modelo operativo unificado, con una consolidación por fases, integraciones fiables y automatización aplicada primero donde el riesgo es mayor.

La madurez implica la puesta en práctica de las mejores prácticas de PKI.

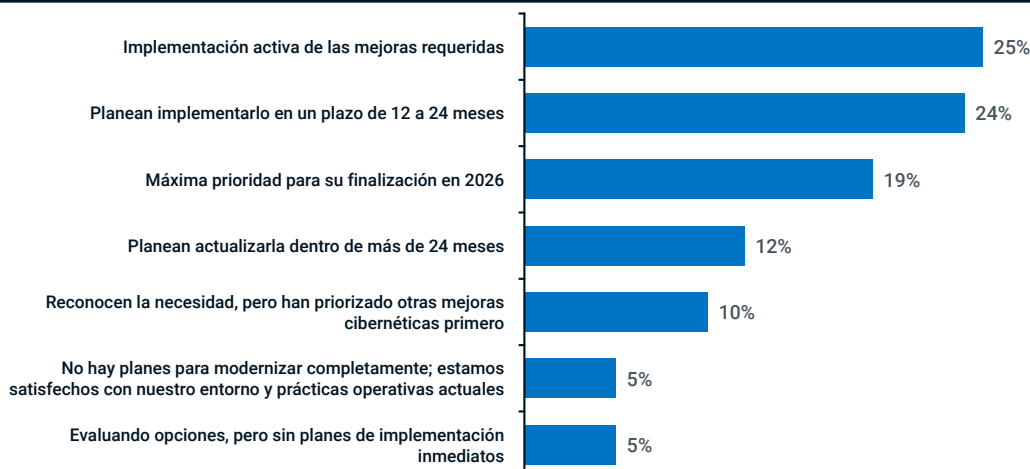
La madurez es el punto en el que la infraestructura de clave pública (PKI) deja de ser un conjunto de buenas intenciones y comienza a convertirse en un modelo operativo que permite a la empresa escalar y acelerar de forma segura. Se trata de construir la visibilidad, la propiedad, la gobernanza y los procesos repetibles necesarios para operar la infraestructura de clave pública (PKI) como un sistema inteligente. Según ese criterio, los esfuerzos de modernización están en una fase inicial, pero no son incipientes. Sin embargo, existe un claro desfase: la concienciación, la urgencia y la ejecución no avanzan al mismo ritmo.

Esa discrepancia queda clara en la encuesta. Casi tres de cada diez encuestados afirman que su organización comprende claramente la modernización de la infraestructura de clave pública (PKI), y uno de cada cuatro dice que ya está implementando las mejoras necesarias. Al mismo tiempo, aproximadamente el 80 % está actuando o planeando actuar en los próximos uno a tres años. Existe una intención generalizada, aunque la ejecución siga siendo irregular.

Ante la creciente necesidad de reducir la vida útil de los certificados y la inminente repercusión de la criptografía poscuántica (PQC), las organizaciones necesitan actualizar sus infraestructuras de clave pública (PKI). ¿Cómo describe su organización la comprensión de la modernización de la infraestructura de clave pública (PKI)?



¿Cuáles son los planes de su organización para modernizar completamente la infraestructura PKI?



También hay indicios de que la comunicación está mejorando dentro de las organizaciones. Poco más de la mitad de los encuestados describen su comprensión empresarial de la identidad digital y la integridad criptográfica como exhaustiva o buena, mientras que otro 35 % afirma que la empresa comprende la criptografía, pero aún tiende a considerarla principalmente como un asunto de TI. En otras palabras, la infraestructura de clave pública (PKI) está adquiriendo mayor relevancia para la alta dirección, pero muchas organizaciones aún están en el proceso de traducir esa concienciación en disciplina de procesos y gobernanza.

En su opinión, ¿cuál es la percepción general dentro del sector empresarial sobre la importancia de una infraestructura de clave pública (PKI) eficaz y moderna?

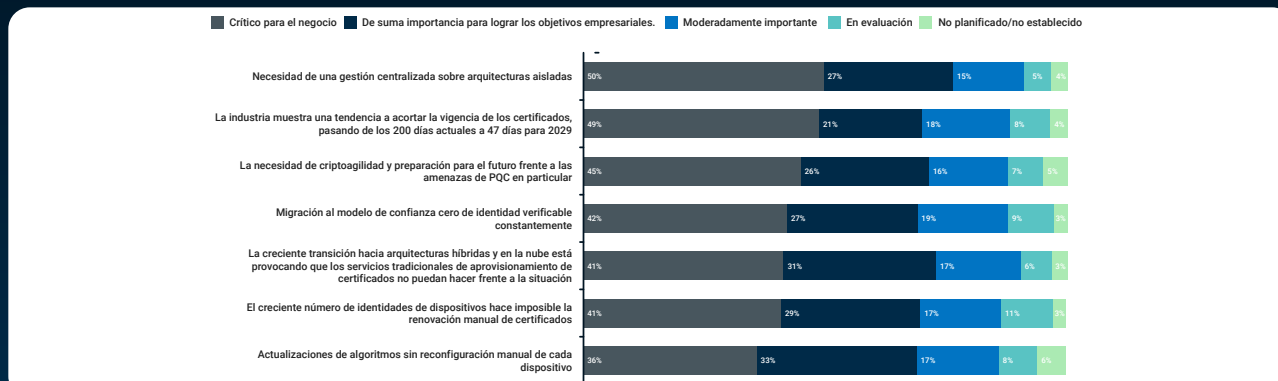


Las organizaciones maduras priorizan la centralización.

Los entornos aislados dificultan el mantenimiento de una visibilidad completa, la prevención de los riesgos asociados a la proliferación de certificados y la gestión de todos los certificados. Observamos que las organizaciones consolidadas optan por la gestión centralizada de la infraestructura de clave pública (PKI), y el 76 % la identifica como crítica para el negocio o de suma importancia.

Junto con la gestión unificada, las preocupaciones en torno a la reducción de la vida útil de los certificados y la preparación para las amenazas poscuánticas describen un modelo operativo maduro en términos sencillos: centralizar la infraestructura PKI crítica, automatizar lo que se repite y diseñar pensando en el cambio, en lugar de tratar la PKI como algo estático.

¿Qué importancia tienen los siguientes factores que impulsan o impulsarían la necesidad de su organización de modernizar o actualizar su entorno PKI?



Mejores resultados para las organizaciones modernizadas.

Los resultados de la encuesta indican mejoras notables en áreas problemáticas tras la implementación de la infraestructura de clave pública (PKI) modernizada. Entre los encuestados que ya han modernizado su infraestructura, el 64 % informa de una gestión automatizada del ciclo de vida, el 60 % menciona una reducción de las interrupciones, el 44 % señala un mejor soporte para el cumplimiento normativo y el 43 % afirma haber obtenido mayor visibilidad y control. Cuando se realiza correctamente, la modernización reduce las interrupciones del servicio, disminuye los gastos administrativos y agiliza el cumplimiento de las normativas.

La madurez de la infraestructura de clave pública (PKI) no se define por la cantidad de autoridades de certificación que posee una organización ni por la cantidad de herramientas que ha adquirido. Se define por la capacidad de la organización para responder de manera fiable a una serie de preguntas operativas prácticas: ¿qué tenemos, quién es el propietario, cuándo se renovará, qué servicio depende de ello, qué política se aplica y podemos realizar cambios sin interrupciones?

Conclusión clave

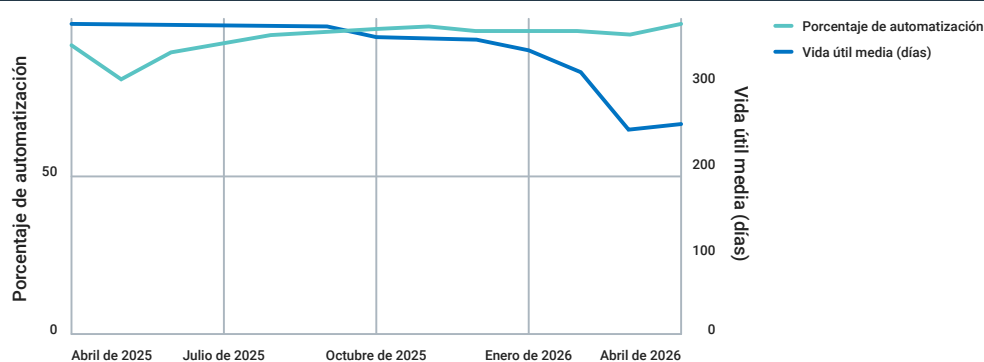
Las organizaciones son conscientes del problema y están empezando a comprender lo que deben hacer. Quienes están más avanzados en el proceso de implementación están viendo los beneficios.

Mandato de 47 días y automatización



Los datos de gestión de certificados de los clientes de DigiCert ONE muestran que comenzaron a acortar la vigencia de los certificados TLS públicos tras la aprobación por parte del CA/B Forum de una reducción gradual a períodos de validez de certificados de 47 días. Esta reducción gradual no implica necesariamente un aumento en el número de certificados que una organización debe gestionar. Sí aumenta la cantidad de veces que los equipos de seguridad tienen que realizar tareas relacionadas con el ciclo de vida de los certificados.

Porcentaje de automatización frente a la vida útil media de los certificados públicos



IA y computación cuántica

La IA y la computación cuántica suponen tanto una aceleración como un cambio de paradigma.

Estas tecnologías emergentes representan el mayor desafío —y quizás la única transformación verdaderamente fundamental— para la infraestructura de clave pública (PKI) en décadas.

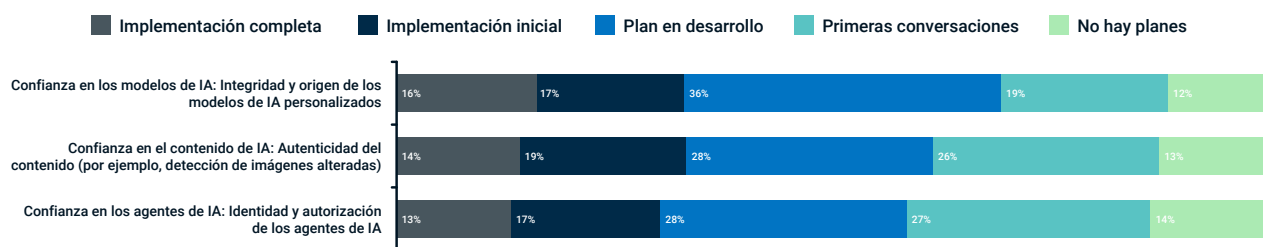
La confianza en los contenidos, modelos y agentes de IA requiere consideraciones especiales sobre la infraestructura de clave pública (PKI).

La IA eleva el listón de la confianza digital al obligar a las organizaciones a responder preguntas más complejas sobre identidad, procedencia y autorización a la velocidad de las máquinas. A medida que las empresas introducen agentes autónomos, implementan modelos y generan contenido, necesitan métodos más sólidos para demostrar qué es auténtico, qué es fiable y qué tiene permiso para actuar. Estos son problemas habituales que se pueden resolver con PKI, pero la IA los hace más visibles.

La encuesta muestra que los líderes ya reconocen la estrecha relación entre el desafío de la IA y la infraestructura de clave pública (PKI). Aproximadamente tres cuartas partes de los encuestados afirman que la PKI desempeñará un papel importante en el uso de la IA.

Lo que aún falta es preparación. Los encuestados sugieren que, si bien las organizaciones reconocen cada vez más la relevancia de la infraestructura de clave pública (PKI) para la seguridad y la gobernanza relacionadas con la IA, la mayoría aún se encuentra en las primeras etapas de planificación e implementación. La tendencia predominante no es la adopción generalizada de procesos consolidados, sino una combinación de exploración inicial, desarrollo de planes y proyectos piloto.

¿Qué describe mejor su nivel actual de planificación en torno a estos aspectos específicos de la confianza en la IA?

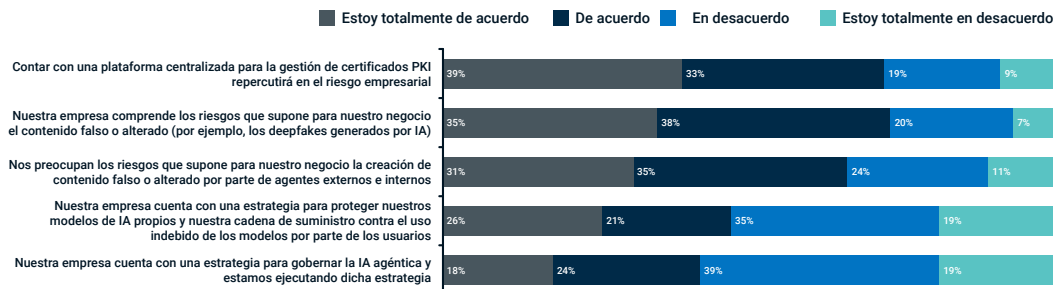


Cómo pasar de la concienciación sobre los riesgos a una estrategia operativa de confianza en la IA.

Es en la gobernanza donde esa brecha de preparación se hace más evidente. La mayoría de los encuestados no está de acuerdo en que su empresa tenga una estrategia establecida para gobernar e implementar la IA agéntica. Más de la mitad tampoco considera que su empresa cuente con una estrategia para proteger los modelos de IA propios y garantizar la seguridad de la cadena de suministro de los modelos externos que puedan utilizar. Al mismo tiempo, el 73 % afirma que su empresa comprende los riesgos del contenido falso o alterado, el 66 % dice que sigue preocupado a pesar de las medidas que están tomando, y el 72 % afirma que la visibilidad centralizada para la gestión de certificados PKI será fundamental en la era de la IA.

Por eso, la IA debe considerarse un factor determinante para la modernización de la infraestructura de clave pública (PKI), en lugar de un programa de confianza independiente. Las organizaciones que hoy no pueden visualizar ni controlar el uso de certificados tendrán dificultades para confiar en los agentes, modelos y contenidos de IA en el futuro.

¿En qué medida está de acuerdo con las siguientes afirmaciones?



Conclusión clave

La confianza en la IA no es una disciplina independiente de la modernización de la infraestructura de clave pública (PKI). Es una de las razones más evidentes por las que las organizaciones necesitan una gobernanza más sólida ahora.

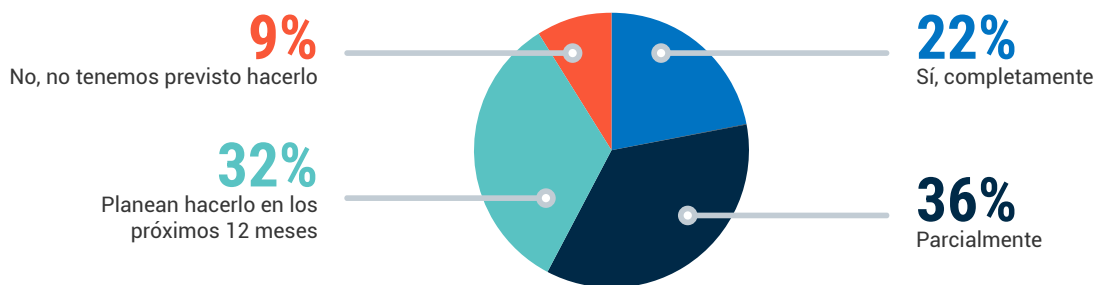
La era cuántica se acerca rápidamente. Planificar lleva tiempo.

Si bien la IA representa el desafío inmediato en materia de confianza, la computación cuántica no se queda atrás. La transición a la criptografía poscuántica no será una actualización rutinaria ni una actividad puntual. Será necesario que las organizaciones comprendan dónde reside la criptografía, qué sistemas dependen de ella, cómo están conectadas esas dependencias y cómo realizar la transición con la menor interrupción posible.

Los resultados de la encuesta muestran tanto nivel de concienciación como trabajo pendiente. Solo el 22 % de los encuestados afirma haber evaluado exhaustivamente las bibliotecas y los sistemas criptográficos en busca de vulnerabilidades en el contexto de futuros ataques cuánticos. Otro 36 % afirma haberlas evaluado parcialmente, y el 32 % dice que planea hacerlo en los próximos 12 meses. Aún es poco común alcanzar un nivel de preparación óptimo, pero la mayoría de las organizaciones están avanzando en la dirección correcta.

Esto coincide con la forma en que los encuestados describen los factores que impulsan la modernización. Más del 71 % afirma que la necesidad de agilidad criptográfica y de estar preparados para afrontar las amenazas cuánticas en el futuro es fundamental o de suma importancia para el negocio. Los líderes comprenden la importancia estratégica de la preparación cuántica, incluso si el trabajo subyacente de descubrimiento y migración aún se encuentra en una etapa temprana.

¿Su organización ha evaluado las vulnerabilidades de las bibliotecas y los sistemas criptográficos en el contexto de futuros ataques de computación cuántica?



Lo importante es que la preparación cuántica depende de los mismos fundamentos operativos que se analizan a lo largo de este informe. Una organización no puede ser ágil en materia criptográfica si desconoce dónde se implementan los certificados, las claves, los algoritmos y las bibliotecas criptográficas. No se puede planificar un cambio coordinado si la propiedad está fragmentada o si los procesos del ciclo de vida siguen siendo manuales. Por lo tanto, la preparación para la computación cuántica comienza mucho antes de que una organización implemente un nuevo algoritmo.

Conclusión clave

La preparación cuántica no es un esfuerzo aparte. La automatización del inventario y del ciclo de vida de los certificados, necesaria para otras iniciativas, contribuye a lograr la agilidad necesaria para migrar a la criptografía poscuántica.

Modernización de la PKI

La modernización de PKI resuelve los problemas de visibilidad, complejidad, madurez, IA y computación cuántica.

El mensaje central de esta investigación no es que las organizaciones estén fallando en la gestión de la infraestructura de clave pública (PKI), sino que esta ha superado las capacidades de los enfoques que muchas organizaciones aún utilizan para gestionarla. El problema es más fácil de solucionar de lo que parece a primera vista. Los líderes reconocen la necesidad de modernizarse, están destinando presupuestos para ello y la mayoría de las organizaciones ya están planeando hacerlo. El objetivo es transformar ese impulso en un control operativo repetible.

Para los responsables de TI y seguridad, esto significa tratar la modernización de la infraestructura de clave pública (PKI) como una capacidad fundamental. La infraestructura de clave pública (PKI) afecta al tiempo de actividad, la eficiencia operativa, la gobernanza de la IA y la agilidad criptográfica. Las organizaciones que se modernicen eficazmente no solo reducirán las interrupciones relacionadas con los certificados o mejorarán la eficiencia operativa, sino que implementarán un sistema de confianza inteligente y escalable para la próxima ola de identidad de máquinas, adopción de IA y seguridad poscuántica.

La modernización de la infraestructura de clave pública (PKI) puede sonar a algo muy amplio porque, en efecto, lo es. Pero no es un concepto impreciso. Empezar por donde el valor operativo sea inmediato y el caso de negocio sea fácil de explicar.

Realice el descubrimiento y el inventario

Resuelva los riesgos derivados de la falta de visibilidad

Cree un inventario fiable de certificados y activos criptográficos relacionados en entornos públicos y privados. A continuación, añada contexto, como la propiedad y el impacto en el negocio, que convierte el descubrimiento inicial en información útil para la toma de decisiones. Esta es la base de todo lo que sigue. El proceso de descubrimiento permite a los equipos pasar del “creemos” al “sabemos”.

Automatice los certificados críticos

Resuelva las deficiencias y las lagunas para gestionar la complejidad y aumentar la madurez

Los certificados TLS/SSL públicos son el caso de uso de modernización más universal, ya que todas las organizaciones con acceso a Internet se ven afectadas por la reducción de la duración de los certificados. El ritmo solo va en una dirección. Por lo tanto, automatizar la emisión e instalación de TLS públicos es una de las maneras más rápidas de reducir el riesgo de interrupciones al tiempo que se desarrolla una capacidad de ciclo de vida repetible. También ayuda a los equipos a crear patrones operativos que necesitarán para extender la automatización a la infraestructura de clave pública (PKI) interna, la firma de código, la identidad de los dispositivos y otros dominios de confianza.

Estandarice la infraestructura de clave pública (PKI) interna

Reduzca la fragmentación y prepárese para futuros cambios criptográficos.

La infraestructura de clave pública interna (PKI) suele ser donde la complejidad se acumula más rápidamente y donde las prácticas obsoletas persisten durante más tiempo. A medida que aumenta el volumen de certificados y evolucionan los requisitos criptográficos, las prácticas inconsistentes incrementan el riesgo operativo y dificultan la coordinación del cambio.

Las organizaciones deben establecer una gobernanza centralizada definiendo políticas para los entornos PKI internos. Las políticas pueden especificar factores como las autoridades de certificación aprobadas, la criticidad para el negocio y la asignación de responsabilidades, los estándares criptográficos y de configuración de certificados, y las necesidades de cumplimiento. Las políticas coherentes mejoran la visibilidad, reducen la fricción operativa, simplifican los esfuerzos de cumplimiento y crean una base más sólida para futuras iniciativas como la gobernanza de la IA y la criptografía poscuántica.

Las políticas permiten a las organizaciones consolidar autoridades de certificación innecesarias o superpuestas, retirar plataformas heredadas y unificar los entornos PKI internos aislados bajo un modelo de gobernanza más coherente. Primero, hay que corregirlas infracciones de políticas de mayor impacto. El objetivo no es reconstruir todo a la vez, sino reducir sistemáticamente el riesgo en los usos actuales y emergentes de la infraestructura de clave pública (PKI).

Metodología

Este informe se basa en una investigación primaria realizada de forma independiente por Omdia en abril de 2026. La encuesta abarcó la evolución de la infraestructura de clave pública (PKI), los factores que impulsan la modernización, los desafíos operativos y las consideraciones futuras.

La investigación incluyó a 423 altos responsables de la toma de decisiones, entre ellos CISO, CIO y altos cargos de TI/seguridad, responsables de la ciberseguridad, la infraestructura de clave pública (PKI) y la infraestructura digital. Los encuestados representaban las funciones de Producto e investigación y desarrollo, TI y operaciones técnicas, Ciberseguridad y gobernanza, riesgo y cumplimiento.

Los encuestados procedían de organizaciones de Norteamérica, EMEA y Asia Pacífico, y abarcaban 11 sectores industriales.



Todas las organizaciones participantes contaban con al menos 1.000 empleados

39%

tenía entre 1.000 y 4.999 empleados

24%

tenía entre 5.000 y 9.999 empleados

37%

tenía 10.000 o más empleados

Las preguntas de la encuesta se diseñaron para medir las realidades operativas y las prioridades estratégicas relacionadas con la modernización de la infraestructura de clave pública (PKI), la confianza digital y la preparación criptográfica. Los análisis y las conclusiones se basan en los datos recopilados, la metodología de investigación de Omdia y un conjunto de datos propio. Algunas preguntas permitían varias respuestas; por lo tanto, el total puede superar el 100 %.

El análisis complementario utilizó datos sobre las operaciones de infraestructura de clave pública (PKI) gestionada por DigiCert y sobre la autoridad de certificación pública desde enero de 2025 hasta marzo de 2026. Los datos incluyeron estadísticas resumidas de una selección de 757 clientes empresariales. Los datos sobre las operaciones de la autoridad de certificación pública procedían de los registros de transparencia de certificados.

Autores y colaboradores

Consultoría Omdia

Omdia es una empresa líder en el mercado de datos, investigación y consultoría, centrada en ayudar a los proveedores de servicios digitales, las empresas tecnológicas y los responsables de la toma de decisiones empresariales a prosperar en la economía digital conectada. A través de una red global de analistas, ofrecemos análisis expertos y perspectivas estratégicas en los sectores de TI, telecomunicaciones y medios de comunicación. La combinación única de datos fidedignos, análisis de mercado y experiencia en sectores verticales de la industria que ofrece Omdia está diseñada para facilitar la toma de decisiones. Omdia forma parte de Informa TechTarget; el grupo Informa cotiza en la Bolsa de Valores de Londres.

Comience ahora su proceso
de modernización de PKI



Acerca de DigiCert

DigiCert es líder mundial en confianza inteligente. Protegemos el mundo digital garantizando la seguridad, la privacidad y la autenticidad de cada interacción. Nuestra plataforma DigiCert ONE, impulsada por IA, unifica la gestión del ciclo de vida de la infraestructura de clave pública (PKI), el DNS y los certificados para proteger la infraestructura, el software, los dispositivos, los mensajes y el contenido, los agentes y los modelos de IA. Descubra por qué más de 125 000 organizaciones, entre ellas, el 90 % de las empresas de Fortune 500, eligen DigiCert para detener las amenazas actuales y prepararse para un futuro seguro frente a la computación cuántica en www.digicert.com/es