digicert + Omdia

Los puntos ciegos en los certificados son interrupciones en potencia

Solo el 34% de las empresas cuenta con un inventario completo de certificados, según el Informe global de investigación sobre PKI 2026 de DigiCert.

Las organizaciones no están tan preparadas como creen. Los nuevos hallazgos de Omdia y DigiCert revelan por qué.

Las organizaciones operan entornos PKI que no pueden controlar por completo, **pero siguen siendo responsables de las interrupciones, las brechas de seguridad y los incumplimientos normativos.**

La infraestructura de clave pública (PKI) ya no es un sistema aislado. Es un ecosistema completo que se ha fragmentado con tanta rapidez que las organizaciones no pueden seguirle el ritmo.

La modernización de la infraestructura de clave pública (PKI) no puede esperar. La inteligencia artificial y la computación cuántica están acelerando la necesidad de pasar de la concienciación a la acción.

No puede gestionar lo que no puede ver.

El riesgo de la infraestructura de clave pública (PKI) comienza con la falta de visibilidad. Muchas empresas operan en entornos de certificados de los que no tienen una visibilidad completa , lo que genera una exposición sistémica.

Casi dos de cada tres empresas no disponen de un inventario completo y actualizado de sus certificados digitales.

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

34%
Inventario completo y actualizado de todos los certificados digitales.

50%
Inventario parcial. Puede haber certificados que no estén identificados.

16%
No estoy seguro de cuántos certificados tenemos ni dónde se utilizan.

El riesgo de PKI se comprende. Pero no se controla.

Existe una clara brecha entre la concienciación y la ejecución. Las organizaciones reconocen el riesgo, pero sus modelos operativos aún no se han adaptado.

Empresas muy o extremadamente preocupadas por:

73%
Riesgo de interrupciones o fallos del servicio debido a certificados caducados.

74%
Proliferación de certificados a medida que aumenta el número de sistemas o identidades.

La infraestructura de clave pública (PKI) ha evolucionado. Su gestión no.

El seguimiento manual y las hojas de cálculo siguen siendo el método de gestión de certificados más utilizado.

La complejidad es el enemigo de la infraestructura de clave pública (PKI) moderna.

La infraestructura de clave pública (PKI) se ha vuelto estructuralmente compleja, no solo técnicamente compleja. La integración y las fricciones organizativas son ahora los principales obstáculos para avanzar.

Retos actuales en la gestión y verificación de certificados:

- Falta de visibilidad
- Soluciones aisladas

Desafíos previstos en la implementación de la modernización de la infraestructura de clave pública (PKI):

- Complejidad del sistema
- Coordinación entre equipos

La proliferación de identidades representa tanto un desafío como una oportunidad para la infraestructura de clave pública (PKI).

La transición a gran escala hacia las identidades no humanas (NHI, por sus siglas en inglés) está desbordando los enfoques tradicionales de PKI, especialmente en el ámbito de la IA agéntica. Las organizaciones tienen dificultades para lograr una cobertura suficiente.

Cobertura actual de PKI:

Mayor cobertura
Identidades de máquinas (**64%**)

Menor cobertura
IA agéntica (**19%**)

Todo el mundo utiliza la PKI. Nadie se responsabiliza de ella.

La responsabilidad fragmentada está ralentizando el progreso. La modernización de la infraestructura de clave pública (PKI) no es solo un desafío técnico, sino también una cuestión de gobernanza y rendición de cuentas.

¿Qué grado de participación tiene cada parte interesada en la toma de decisiones sobre la infraestructura de clave pública (PKI) en su organización?



Los CISO son, con diferencia, **los principales responsables de la toma de decisiones sobre PKI (40%).**

Aunque los CIO, los CTO y los equipos de seguridad participan en el proceso, una mayor implicación del resto del equipo directivo (CxO) puede aportar un apoyo adicional valioso.

Solo en el 9% de los casos el consejo de administración toma la decisión final sobre la infraestructura de clave pública (PKI).

El futuro de la confianza ya está aquí. Las organizaciones no están preparadas.

La próxima oleada de demanda, impulsada por la IA, la amenaza cuántica y el modelo de confianza cero, avanza más rápido que la capacidad de preparación de las organizaciones.

Conocimiento actual sobre la modernización de la infraestructura de clave pública (PKI):

70%
Bajo
Agrupa «conocimientos básicos», «empezando a aprender» y «sin comprensión».

Planes para modernizar completamente la infraestructura de clave pública (PKI):

68%
En los próximos 24 meses

Las organizaciones no pueden abordar esta transformación por sí solas. Los conocimientos especializados y el apoyo de proveedores y socios de confianza digital les ayudarán a llevarla a cabo.

Las organizaciones que han modernizado su infraestructura de clave pública (PKI) informan de una reducción de las interrupciones **superior al 60%.**

Descargue el informe completo



digicert
digicert.com/es | Digicert | Digicert

Omdia
omdia.com | Omdia | OmdiaHQ

Copyright © 2026 DigiCert | Todos los derechos reservados.