digicert®

Guía para evaluar la madurez del ciclo de vida de los certificados

Su camino hacia la reducción de costes y el fin de las interrupciones con una infraestructura de clave pública (PKI) ágil

GUÍA

Introducción

El mundo conectado requiere una gestión de certificados moderna

Los certificados PKI constituyen la base de la confianza digital para el mundo conectado. Las redes modernas operan en infraestructuras cada vez más complejas que se amplían y evolucionan continuamente de acuerdo con las necesidades de las empresas. Estas redes no están aisladas, sino que los sistemas modernos interactúan con muchas otras redes, tanto internas como externas. Ofrecer confianza para este nivel de complejidad requiere una gestión de certificados que sea ampliable y adaptable a partes iguales.

Metodología

¿Qué es la madurez de la gestión del ciclo de vida de los certificados (CLM)?

La madurez de la CLM se refiere a la transición desde las prácticas manuales y reactivas hacia unas operaciones automatizadas y basadas en políticas. A medida que aumenta la madurez, los costes y riesgos se reducen considerablemente. La implementación de herramientas y políticas de gestión más avanzadas y la automatización integrada son elementos importantes en el camino de su empresa hacia la agilidad criptográfica.

La agilidad criptográfica es la capacidad de actualizar o sustituir rápidamente algoritmos, claves y protocolos criptográficos de forma automatizada con una interrupción mínima de las operaciones. Aunque la CLM es un componente principal de la agilidad criptográfica, es importante entender que esta abarca también otros activos criptográficos, como claves de cifrado para bases de datos, discos duros de ordenadores, claves de autenticación multifactor (MFA), etc.

El renacimiento de la PKI

La PKI está volviendo a nacer por obligación. Este renacimiento se debe a una serie de acontecimientos que requieren pasar a la acción para hacer frente a los retos relativos a las amenazas para la seguridad, la normativa, la escalabilidad y la gestión del ciclo de vida. La buena noticia es que esta transformación se traducirá en una nueva generación de PKI que será más segura, resistente y ágil.

Factores que impulsan el renacimiento de la PKI

- **Reducción del período de validez de los certificados**
  Para 2029, las empresas tendrán que utilizar certificados con períodos de validez de 47 días para todos los casos de uso de confianza pública. Con esta decisión del CA/Browser Forum, será prácticamente imposible mantener procesos manuales.

- **Explosión de las identidades de máquinas**
  API, dispositivos IoT, contenedores, entornos multinube y un largo etcétera: las máquinas representan ahora miles de millones de conexiones. Pronto habrá el triple de dispositivos que de seres humanos, y eso sin contar la próxima oleada de agentes de IA que también necesitarán identidades de confianza.

- **Complejidad y alcance de las operaciones**
  En los entornos de nube e híbridos tradicionales, se desdibujan los límites entre las PKI externas, internas y federadas. Estos sistemas exigen grandes volúmenes de distintos tipos de certificados, lo que a su vez requiere una CLM flexible que lo una todo a la perfección.

- **La amenaza cuántica**
  La base misma de la PKI —los algoritmos criptográficos que no pueden adivinarse ni averiguarse mediante ataques de fuerza bruta con la potencia de cálculo actual— está amenazada a día de hoy. Los ordenadores cuánticos pronto podrán romper los algoritmos criptográficos actuales. Existen nuevos algoritmos a prueba de informática cuántica, pero deben someterse a pruebas e implantarse en todas partes antes de 2029, según las previsiones de Gartner y otros expertos del sector.

Escala de la madurez de la CLM

La escala que figura a continuación describe tres niveles de madurez de la CLM: *ad hoc*, en desarrollo y en maduración. Cada nivel ofrece un resumen general del que sería el estado del entorno de gestión de certificados en esa fase. En las secciones siguientes, se aplica esta escala a seis áreas clave de las mejores prácticas en materia de CLM y se describe cada nivel ya de manera específica para cada disciplina.

- *Ad hoc*
  La gestión se lleva a cabo principalmente mediante procesos reactivos y manuales con muy poca visibilidad de todo el entorno de certificados y de los riesgos existentes. Los procesos son difíciles de controlar y la política está poco desarrollada o aislada, lo que dificulta su aplicación. El inventario de certificados suele gestionarse con hojas de cálculo.

- En desarrollo
  La gestión incluye visibilidad centralizada con control parcial de la notificación y mitigación de riesgos. Se está introduciendo una gobernanza basada en políticas, y las renovaciones de certificados están automatizadas para más del 30 % de los sistemas. Además, se ha automatizado la implementación de certificados en un conjunto reducido de sistemas y aplicaciones críticos. Se producen frecuentemente interrupciones provocadas por fallos en los procesos manuales de gestión de certificados.

- En maduración
  La gestión incluye visibilidad centralizada con control casi total de la notificación y mitigación de riesgos. La gobernanza basada en políticas es la norma, y no la excepción. La renovación de certificados está automatizada en más del 50 % de los sistemas, y la implementación está automatizada en los sistemas más críticos. El trabajo actual se centra en la incorporación e integración de los sistemas de nivel 2 y 3 como parte de una estrategia de agilidad criptográfica más amplia.

Aplicación del modelo en su empresa

Su empresa tiene sus propias necesidades particulares, por lo que, para poder utilizar herramientas y procesos diseñados para la agilidad criptográfica en su entorno de certificados, es necesario que entienda en qué punto del modelo de madurez se encuentra. Esta guía le ayudará a evaluar seis áreas clave de la gestión del ciclo de vida de los certificados para determinar la situación de su empresa a medida que avanza hacia la agilidad criptográfica.

Evaluación

Evalúe la madurez de la CLM de su empresa

Las mejores prácticas que exponemos a continuación describen un estado ideal para las soluciones, los flujos de trabajo y la gobernanza que rodean a la PKI diseñada para la agilidad criptográfica. Utilice estas descripciones para evaluar el estado actual de su empresa y trazar el camino hacia un mayor nivel de madurez.

Categoría n.º 1

Detección e inventario

La capacidad de saber dónde están todos sus certificados, cómo están configurados, cuándo caducan, quién es su propietario y cuál es su relevancia para la empresa. La elaboración de este inventario requiere datos procedentes de múltiples fuentes para obtener una visión completa de las PKI externas, internas e integradas.

- *Ad hoc*: seguimiento manual, normalmente mediante hojas de cálculo. Visibilidad fragmentaria y limitada, con poca información sobre el entorno completo de los certificados y los riesgos asociados.

- En desarrollo: detección programada con automatización limitada. Los propietarios están identificados y se han establecido notificaciones básicas sobre las renovaciones y las fechas de caducidad de los certificados, lo que mejora la visibilidad y la asignación de responsabilidades.

- En maduración: detección continua y en tiempo real en fuentes de PKI internas, externas y de terceros. La propiedad está centralizada y documentada, lo que facilita las alertas proactivas, los flujos de trabajo de aprobación y la gobernanza a gran escala. El sistema también proporciona análisis que contribuyen al seguimiento y la previsión de costes.

Razón fundamental

La detección fomenta la elaboración de inventarios, lo que facilita la creación de políticas y, en última instancia, la automatización. Cuando se cuenta con funciones de detección e inventario, se sabe dónde están todos los certificados, cómo están configurados, cuándo caducan, quién es su propietario y cuál es su relevancia para la empresa, incluso si los certificados proceden de la informática en la sombra.

Categoría n.º 2

Política y gobernanza

La implementación y aplicación de políticas bien definidas que hacen posible la emisión, renovación y revocación basadas en normas. Estas políticas impiden usos indebidos, minimizan el riesgo de que se produzcan interrupciones relacionadas con los certificados y accesos no autorizados y garantizan que la empresa cumpla siempre las normas y reglamentos.

- *Ad hoc*: si hay supervisión, la gobernanza es ocasional y, normalmente, reactiva. No existe una manera eficaz de aplicar o auditar la política en todo el entorno, lo que hace que resulte casi imposible garantizar la coherencia y la asignación de responsabilidades.
- **En desarrollo:** aunque existe una comunicación coherente y cierto nivel de gobernanza, la aplicación de las políticas todavía es manual en gran medida. Sigue siendo difícil aplicar las políticas de manera coherente en todas las unidades de negocio o regiones.
- **En maduración:** la gobernanza se integra en los procesos de CLM mediante la automatización basada en políticas. Las normas se aplican de forma dinámica, lo que garantiza la coherencia en la emisión, renovación y revocación. Los equipos pueden informar rápidamente del estado de los activos de PKI.

Razón fundamental

Una política y una gobernanza sólidas reducen el error humano, aceleran la corrección e imponen la asignación de responsabilidades en todos los equipos y entornos, por lo que la gestión de certificados pasa de ser una carga reactiva a un activo proactivo y estratégico.

Categoría n.º 3

Automatización de CLM integrada

La capacidad de automatizar la renovación y la implementación de certificados con las autoridades de certificación correspondientes, así como la implementación de certificados en sus servidores, aplicaciones, dispositivos, etc., específicos, de forma repetible y con una intervención humana mínima. Depende de que exista un inventario avanzado y centralizado que incluya los propietarios y políticas definidos, así como los diferentes métodos y protocolos de integración, en función de los requisitos de cada sistema.

Nota: Aunque se suele hablar del protocolo ACME (Automated Certificate Management Environment) indistintamente para referirse a la automatización de la CLM, ACME representa solo una pequeña parte de la automatización de la CLM.

- *Ad hoc*: ni la gestión ni la renovación están automatizadas. Los administradores renuevan e instalan los certificados manualmente cuando así se lo indican las alertas en sus calendarios u otro tipo de recordatorios. A medida que aumentan los volúmenes de certificados y disminuyen sus períodos de validez, aumentan la carga de trabajo y el número de interrupciones.
- **En desarrollo:** se configuran máquinas individuales para comprobar el estado de los certificados y renovarlos e instalarlos automáticamente, tareas que se ejecutan regularmente siguiendo un calendario establecido. La automatización está distribuida y no hay manera de supervisar el estado, responder a los errores ni aplicar las políticas de forma centralizada.
- **En maduración:** automatización centralizada de las renovaciones, las sustituciones y la instalación de los certificados, basada en un inventario y una propiedad centrales que estipulan unas políticas globales. Esta automatización contribuye a facilitar la adopción prevista de los cambios en materia de criptografía, incluida la criptografía poscuántica.

Razón fundamental

Dado que el protocolo ACME debe configurarse en cada endpoint, no se puede ampliar fácilmente en entornos complejos. Incluso cuando la propiedad de los certificados está distribuida entre distintos equipos o sistemas, es esencial adoptar un enfoque centralizado para la gestión. Esto garantiza la visibilidad, la coherencia y el control, algo que el protocolo ACME no puede ofrecer por sí solo. Para gestionar de forma centralizada todas las tareas en todo su ecosistema, necesita también otros protocolos e integraciones.

Categoría n.º 4

Preparación para auditorías

La capacidad de, por un lado, llevar un seguimiento y registro proactivos de todos los certificados mediante la automatización —con los análisis e informes necesarios para producir rápidamente pruebas de cumplimiento— y, por el otro, unificar los datos de los certificados y los registros de cambios relacionados en todos los sistemas de la empresa, incluido Active Directory, y las plataformas de gestión de activos como SAP EAM y las herramientas de ITSM.

- *Ad hoc*: prácticamente no hay pruebas de cumplimiento ni se tiene la capacidad de presentarlas a tiempo. Sin supervisión de los activos, riesgos y necesidades existentes, la empresa no puede responder a los requisitos de auditoría ni evitar interrupciones.
- **En desarrollo:** existen inventarios y pruebas del cumplimiento de las políticas, pero no están centralizados. No existe un seguimiento coherente de las políticas y procedimientos para todos los certificados y aplicaciones. La visibilidad y las auditorías son viables, pero requieren una gran cantidad de recursos.
- **En maduración:** seguimiento exhaustivo de todos los certificados, políticas y procedimientos en la mayoría de las aplicaciones de su empresa. Esto permite responder rápidamente a las auditorías para presentar pruebas del cumplimiento de las políticas.

Razón fundamental

Para evitar problemas de cumplimiento, debe saber dónde están sus certificados y poder gestionarlos activamente. La clave para ello es la auditoría completa de todas las CA y todos los sistemas, con la capacidad de realizar informes que cumplan las normas del sector.

Categoría n.º 5

PKI pública, interna y federada

Visibilidad y control convergentes de todas las PKI, tanto públicas como internas y federadas, independientemente del caso de uso. La capacidad de utilizar el tipo de modelo de confianza de certificados adecuado para el caso de uso en cuestión.

- *Ad hoc*: es probable que existan PKI internas dentro de la empresa, pero no se tiene la capacidad de encontrar y gestionar de forma centralizada esos certificados de CA privados.
- **En desarrollo:** la empresa ha identificado sus PKI aisladas y ha abordado los problemas críticos relativos a la seguridad o al cumplimiento. Sin embargo, estas PKI siguen estando aisladas y se gestionan por separado.
- **En maduración:** la empresa puede ver y gestionar todas las PKI públicas, internas y federadas a través de un sistema consolidado. Las PKI internas pueden gestionarse mediante una solución centralizada, en lugar de con las herramientas de las aplicaciones. Una solución de CLM eficaz puede sustituir sin problemas a Microsoft CA en la gestión de certificados de Active Directory y gestionar certificados de cualquier CA pública, lo que facilita el traslado de certificados de una a otra.

Razón fundamental

En el mundo real, el número de certificados en PKI privadas o internas eclipsa al de las públicas, pero probablemente la diferencia debería ser mayor. A veces, los administradores de sistemas utilizan certificados públicos, sobre todo gratuitos, cuando la aplicación estaría mejor protegida con una PKI interna o federada, pero esto introduce riesgos. Asegúrese de elegir la PKI adecuada para cada caso de uso y de tener la capacidad de supervisar y controlar cada certificado, independientemente del tipo que sean.

Categoría n.º 6

Escalabilidad y posibilidad de ampliación

Las soluciones y los procesos diseñados para la agilidad criptográfica facilitan el crecimiento y el cambio en toda la empresa y a lo largo del tiempo, y están preparados para las integraciones de criptografía poscuántica.

- *Ad hoc*: la gestión de certificados está fragmentada y no es escalable, por lo que requiere intervención manual en cada paso. El resultado es un sistema frágil y reactivo que no puede evolucionar fácilmente.
- **En desarrollo:** la emisión de certificados está parcialmente estandarizada, con una mezcla de CA privadas antiguas, servicios en la nube y CA públicas. Sin embargo, la gestión sigue estando fragmentada, al igual que el desarrollo y el mantenimiento de las integraciones.
- **En maduración:** el control central permite que la PKI empresarial funcione en las instalaciones locales y en una o varias nubes. Una PKI de este nivel se adapta al aumento del número de usuarios y máquinas y se integra con numerosas tecnologías a medida que evoluciona la infraestructura de la empresa.

Razón fundamental

Las integraciones frágiles suelen fallar, requieren correcciones frecuentes y no se adaptan bien a los nuevos requisitos y flujos de trabajo. Los procesos de CLM de un nivel de madurez alto permiten a su organización responder dinámicamente a las necesidades empresariales y de seguridad, ya que admiten el aprovisionamiento automatizado, la aplicación flexible de políticas e integraciones perfectas en entornos locales, en la nube e híbridos.

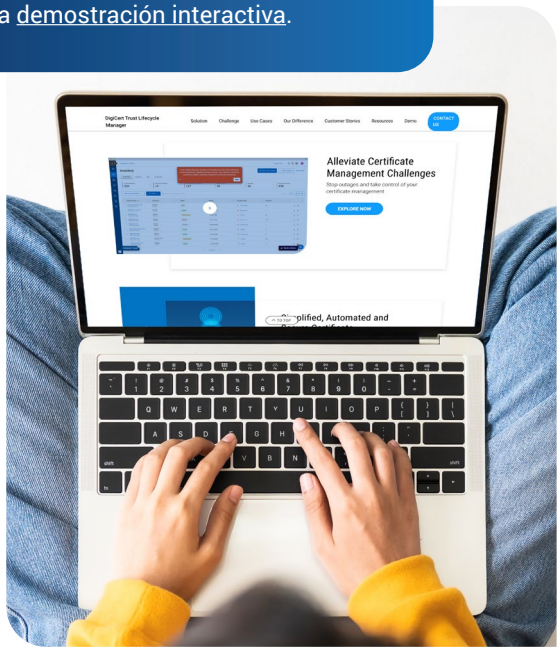
Qué hacer con esta guía

Siguientes pasos

Ahora que se ha hecho una idea del nivel de madurez actual de su empresa, ¿qué es lo siguiente que debe hacer? Es importante tener en cuenta que la automatización en sí no es el objetivo último, y tampoco se trata de alcanzar un estado final de madurez. Al centrarse en soluciones, procesos y políticas diseñados para la agilidad criptográfica, su empresa podrá seguir adaptándose conforme crezcan sus sistemas, evolucionen las normas y surjan nuevas amenazas.

Con la solución adecuada de gestión del ciclo de vida de los certificados, puede preparar su infraestructura para el futuro, garantizar el cumplimiento y mantener la confianza en un ecosistema digital que cambia rápidamente.

Vea cómo DigiCert lo hace posible. Haga un recorrido del producto con esta demostración interactiva.



Acerca de DigiCert

DigiCert nació con un claro objetivo: encontrar una forma mejor de proteger Internet. Por eso, particulares y empresas de todo el mundo confían en nuestras soluciones de PQC, TLS, PKI e IoT en todas partes, millones de veces al día. Por eso, nuestros clientes otorgan a nuestros servicios y nuestra asistencia técnica el mayor número de valoraciones de cinco estrellas del sector. Y por eso seguiremos liderando el camino hacia un futuro preparado para la informática cuántica con ayuda de lo que llamamos Digital Trust para el mundo real.