digicert®

Certificados TLS de 47 días: preguntas frecuentes

GUÍA

Certificados TLS de 47 días: preguntas frecuentes

P: ¿Cuáles son las nuevas normas sobre la validez de los certificados?

En marzo de 2026, empezarán a entrar en vigor tres cambios importantes que afectan a las nuevas normas del CA/B Forum sobre los certificados TLS:

1. El período de validez máximo de los certificados TLS públicos pasará de 398 días a 47 días.

2. El período máximo durante el cual se podrá reutilizar la información relativa a la validación del dominio y la dirección IP se reducirá de 398 días a 10 días.

3. El periodo máximo durante el cual se podrá reutilizar la información de identidad del sujeto (SII) —esto es, los datos identificativos de la entidad para la cual se emite el certificado— disminuirá de 825 a 398 días.

La automatización de algunos certificados públicos puede requerir herramientas o conocimientos especiales; pero, en la mayoría de los casos, el proceso debería ser relativamente sencillo. Hay una gran cantidad de documentación disponible y el servicio suele ser gratuito (como en el caso de DigiCert).

P: ¿Qué calendario seguirán los cambios?

La validez máxima de los certificados TLS públicos disminuirá progresivamente a lo largo de los próximos años:

- Hasta el 15 de marzo de 2026, la validez máxima de los certificados TLS seguirá siendo de 398 días.
- A partir del 15 de marzo de 2026, la validez máxima de los certificados TLS pasará a ser de 200 días.
- A partir del 15 de marzo de 2027, la validez máxima de los certificados TLS será de 100 días.
- A partir del 15 de marzo de 2029, la validez máxima de los certificados TLS será de 47 días.

También se va a reducir el período máximo durante el cual se puede reutilizar la información relativa a la validación de dominios y direcciones IP:

- Hasta el 15 de marzo de 2026, el período máximo durante el cual se puede reutilizar la información de validación de dominios seguirá siendo de 398 días.
- A partir del 15 de marzo de 2026, el período máximo durante el cual se podrá reutilizar la información de validación de dominios pasará a ser de 200 días.
- A partir del 15 de marzo de 2027, el período máximo durante el cual se podrá reutilizar la información de validación de dominios será de 100 días.
- A partir del 15 de marzo de 2029, el período máximo durante el cual se podrá reutilizar la información de validación de dominios será de 10 días.

P: ¿Qué diferencia hay entre la validez máxima del certificado (hasta 47 días) y el período máximo de reutilización de la validación del dominio (hasta 10 días)?

La validez máxima de un certificado es el número máximo de días durante los cuales se considera válido un certificado. Para emitir un certificado, una autoridad de certificación (CA) debe validar que el solicitante tiene el control del nombre de dominio o la dirección IP identificados en el certificado. Si tiene un certificado y lo renueva una vez al año (según las normas actuales), deberá volver a verificar ese control anualmente junto con su solicitud de renovación.

Pero ¿qué pasa si necesita sustituir el certificado antes de renovarlo (por ejemplo, porque la clave privada se ha visto comprometida)? La CA puede reutilizar la validación que realizó durante el proceso de renovación más reciente, lo que le evita tener que realizar la validación de nuevo. Esto se debe a que aún no se ha agotado el plazo máximo de reutilización de la información de la validación de dominios.

Los Requisitos básicos (también conocidos como las normas del CA/B Forum para la emisión de certificados) siempre han especificado ambos plazos, pero generalmente los han fijado en el mismo número. La finalidad del cambio que se ha introducido en la fase final de las nuevas normas y que hará que la validez máxima de los certificados acabe siendo de 47 días —pero que la validación de dominios solo pueda reutilizarse durante 10 días— es garantizar que la validación se realice con frecuencia, ya que se considera que se queda obsoleta rápidamente. Este cambio también responde a la convicción del CA/B Forum de que la validación de dominios debe automatizarse. Con plazos tan cortos, la verificación manual se vuelve una carga importante; pero, una vez automatizado el proceso, la brevedad de los plazos no supone ningún problema.

Los certificados con OV y EV seguirán el mismo calendario que para la verificación de dominios. Con el tiempo, la validación de dominios para estos certificados deberá realizarse con la misma periodicidad que los certificados con DV, esto es, cada 200, 100 o 10 días. Sin embargo, el resto de la información de esos certificados (como el nombre y la dirección de la empresa) solo habrá que renovarla cada 398 días. La verificación de dominios puede y debe automatizarse, como ocurre con los certificados con DV, pero el resto de la información no puede automatizarse por completo.

P: En las fechas en que entren en vigor los cambios, ¿los navegadores dejarán de aceptar certificados con períodos de validez superiores a 200, 100 o 47 días?

No exactamente. La restricción se aplica a los tipos de certificados que pueden emitir las CA, no a los que pueden aceptar los navegadores. El navegador comprueba si la fecha actual está dentro del período de validez del certificado.

Cuando los cambios en las normas entren en vigor, las CA ya no podrán emitir certificados TLS con una validez superior a 200, 100 o 47 días. Sin embargo, si un certificado con una validez de 398 días se emite antes de que entre en vigor el cambio normativo, este seguirá siendo válido hasta que caduque. Lo mismo ocurre con los certificados con una validez de 200 días cuando la norma cambie a 100 días y con los certificados con una validez de 100 días cuando la norma cambie a 47 días.

P: ¿Qué es el CA/B Forum?

El CA/Browser Forum (CA/B Forum o CABF, para abreviar) es un organismo de normalización del sector formado por autoridades de certificación como DigiCert (conocidas en las normas como «emisores de certificados») y aplicaciones (normalmente navegadores web, conocidos en las normas como «consumidores de certificados») que utilizan certificados para autenticar un recurso. También son miembros del CA/B Forum otras partes interesadas, pero la votación se limita a los emisores de certificados cualificados y a los consumidores.

Los primeros requisitos básicos (BR) para certificados TLS entraron en vigor en 2012. Existen otros grupos de trabajo que se dedican a la elaboración de normas para los certificados públicos de firma de código y S/MIME.

P: ¿Qué opciones tengo?

Solo hay un modo de proceder razonable: automatizar la gestión del ciclo de vida de los certificados (CLM). Tanto el CA/B Forum como el sector en general (DigiCert incluido) llevan muchos años advirtiendo a los clientes de que la validez de los certificados acabaría acortándose y que la gestión manual de los certificados dejaría de ser una solución viable.

La gran mayoría de los casos de uso de los certificados con validación de dominio (DV) pueden automatizarse con bastante facilidad utilizando los protocolos ACME (Automated Certificate Management Environment) y ARI (ACME Renewal Information). Esta función se incluye sin coste adicional en DigiCert CertCentral. Para casos más complicados, DigiCert Trust Lifecycle Manager (TLM) admite automatización gestionada para una amplia variedad de configuraciones empresariales.

En otros casos, una opción alternativa es utilizar una PKI interna, también conocida como PKI privada. Muchos certificados de confianza pública se utilizan para proteger recursos que no necesitan acceso público y a los que, según las mejores prácticas, no debería accederse desde Internet. A veces, los administradores utilizan certificados públicos para estos recursos porque es lo más fácil, pero lo correcto es utilizar una PKI interna.

Las PKI internas emiten certificados que solo son «válidos» o de confianza dentro de su empresa para la comunicación entre recursos privados. Esto significa que puede establecer sus propias reglas sobre el período de validez de los certificados y otros muchos parámetros.

Es posible ejecutar todo el software de una PKI interna sin ayuda, pero es una tarea compleja y propensa a errores. DigiCert ofrece varias soluciones diferentes de PKI interna para casos de uso empresariales, de nube y de fabricación.

P: ¿Afectan estos cambios normativos a las PKI internas (privadas)?

No. Los requisitos básicos solo son vinculantes para las autoridades de certificación públicas.

Una PKI interna se ejecuta dentro de su red o sus nubes. Incluye autoridades de certificación, pero es su empresa la que establece las políticas que deberán aplicar las autoridades de certificación internas, lo que incluye las fechas de caducidad de los certificados. Puede ser más conveniente elegir fechas de caducidad cortas incluso para la PKI interna, pero no es obligatorio.

Es posible ejecutar todo el software de una PKI interna sin ayuda, pero es una tarea compleja y propensa a errores. DigiCert ofrece varias soluciones diferentes de PKI interna para casos de uso empresariales, de nube y de fabricación.

P: ¿Tendré que pagar más por sustituir los certificados más a menudo?

No. Al menos, no con DigiCert CertCentral. Los certificados se pagan como suscripción anual. Mientras dure la suscripción, no habrá ningún coste por renovar o sustituir los certificados tantas veces como sea necesario. Además, las suscripciones incluyen la automatización ACME/ARI sin coste adicional. Anticiparnos a este tipo de acontecimientos es una de las razones por las que hemos optado por un modelo de suscripción.

Hemos comprobado que, una vez que los clientes automatizan la renovación de certificados, adoptan voluntariamente ciclos de sustitución más rápidos porque es sencillo y no hay razón para no hacerlo. Puede, por ejemplo, pasar directamente a realizar la renovación cada 30 días y despreocuparse cuando llegue la fecha límite de 2029.

P: ¿Afectarán las nuevas normas a los certificados raíz e intermedios?

No. Solo afectan a los certificados leaf emitidos por una CA intermedia.

No existen normas del CA/B Forum ni de otros organismos de normalización que restrinjan la validez de los certificados raíz e intermedios, pero sí hay una serie de mejores prácticas ampliamente aceptadas, y los proveedores de software que utilizan certificados establecen sus propias normas para sus programas de raíces de confianza, que pueden variar enormemente.

La política del almacén de raíces de Mozilla dice (en la sección 7.4) que Mozilla dejará de confiar en los certificados raíz 15 años después de la generación de la clave.

Las normas sobre la validez de los certificados recogidas en la política del programa de raíces de Chrome, versión 1.6 (del 15 de febrero de 2025), son más complicadas. No existe un límite de validez máximo, pero «[c]ualquier certificado de CA raíz cuyo material de clave correspondiente se haya generado hace más de 15 años se eliminará de la Chrome Root Store con regularidad». Las raíces que contengan claves creadas antes del 16 de abril de 2014 se eliminarán según un calendario anual fijado y definido en la política del programa de raíces.

El programa de certificados raíz de confianza de Microsoft dice que «[l]as CA raíz recién acuñadas deben ser válidas durante un mínimo de ocho años y un máximo de 25, a partir de la fecha de presentación». Las diferencias entre las reglas de la política de Microsoft y de otras políticas se deben a la gran variedad de aplicaciones que Microsoft admite en su PKI, que es mucho más amplia que la de cualquier otro navegador.

Una buena práctica de sentido común es que un certificado de CA raíz no debe caducar antes que los certificados de CA intermedias que estén encadenados a él.

La mala gestión de los ciclos de vida de los certificados de CA raíz e intermedia puede tener graves consecuencias, como ocurrió recientemente cuando caducó un certificado de CA intermedia de Google que, por lo visto, se había olvidado, lo que dejó sin servicio a muchos dispositivos Google Chromecast.

P: ¿Cómo puedo automatizar la gestión del ciclo de vida de mis certificados?

Para casos habituales y sencillos, como servidores web y certificados TLS públicos, la automatización es gratuita para los clientes de CertCentral mediante los protocolos ACME (Automated Certificate Management Environment) y ARI (ACME Renewal Information), ampliamente admitidos en el sector.

Evidentemente, no todos los certificados son TLS públicos, y no todas las tecnologías admiten ACME. Para esos casos, DigiCert Trust Lifecycle Manager ofrece funciones de automatización e integraciones avanzadas.

La automatización con ACME implica algo más que marcar una casilla. Hay cambios que deberá realizar en el dispositivo o aplicación (normalmente, un servidor web) que solicita el certificado; pero, para la mayoría de los administradores, el proceso no es complicado y está bien documentado.

P: ¿Qué son ACME y ARI?

ACME son las iniciales de «Automated Certificate Management Environment» (o entorno de gestión automatizada de certificados). ARI es la sigla de «ACME Renewal Information» (o información de renovación de ACME).

ACME es un protocolo admitido por todas las grandes autoridades de certificación, mediante el cual un software cliente de certificados (normalmente, un servidor web) solicita un certificado a la CA y lo instala en el cliente. (En este caso, el servidor web es el cliente).

El software cliente también debe ser compatible con ACME. Existe una compatibilidad generalizada, pero no universal. Por lo general, el programa cliente de ACME se ejecuta en el sistema cliente según un calendario mediante la herramienta Cron de Linux o las tareas programadas de Windows, pero existen otras soluciones que integran el calendario en productos más amplios.

ARI es un protocolo relacionado por el que el servidor puede sugerir un calendario para que el cliente sepa que debe renovar el certificado antes de que caduque. Si se configura bien, el protocolo ARI puede indicar al cliente que debe renovar el certificado si este ha sido revocado, evitando así posibles interrupciones.

P: ¿Cómo afectará esto a mis certificados con validación de empresa (OV) y con validación extendida (EV)?

Según las nuevas normas para certificados TLS, a partir del 15 de marzo de 2026, las validaciones de la información de identidad del sujeto (SII) solo podrán reutilizarse durante 398 días, en comparación con el plazo actual de 825 días.

Por lo tanto, la principal consecuencia para sus certificados con OV y EV será que tendrá que volver a verificar la SII (la información del certificado que identifica a su empresa) anualmente en lugar de cada dos años.

Según los requisitos básicos de TLS, esto requiere una llamada telefónica anual con un representante de DigiCert y, por lo tanto, no puede automatizarse por completo.

Tenga en cuenta que los certificados con OV y EV también protegen nombres de dominio, por lo que su validez cambiará según el mismo calendario que seguirán los certificados con DV: a 200 días en 2026, a 100 días en 2027 y a 47 días en 2029. Automatizar la gestión de estos certificados es igual de importante que automatizar la gestión de los certificados con DV.

Este modelo de fijar un periodo de tiempo poco habitual con un margen de maniobra extra ha sido durante mucho tiempo el procedimiento operativo estándar del CA/B Forum

P: ¿Por qué 47 días?

47 días puede parecer un número arbitrario, pero en realidad es el resultado de una operación matemática sencilla:

- 200 días = 6 meses máximos (184 días) + 1/2 mes de 30 días (15 días) + 1 día de margen
- 100 días = 3 meses máximos (92 días) + ~1/4 de mes de 30 días (7 días) + 1 día de margen
- 47 días = 1 mes máximo (31 días) + 1/2 mes de 30 días (15 días) + 1 día de margen

Este modelo de fijar un periodo de tiempo poco habitual con un margen de maniobra extra ha sido durante mucho tiempo el procedimiento operativo estándar del CA/B Forum. Al límite actual de 398 días se llegó así: 1 año máximo (366 días) + 1 mes máximo (31 días) + 1 día de margen.

P: ¿Estos cambios están relacionados de algún modo con las amenazas a la criptografía derivadas de la informática cuántica?

No directamente, pero sí esperamos que tengan el efecto de mejorar la preparación frente a la criptografía poscuántica (PQC), ya que obligan a las empresas a adoptar soluciones de gestión automatizada de certificados.

En los próximos años, la transición a la PQC implicará realizar numerosos cambios en los sistemas criptográficos de la infraestructura (autoridades de certificación, por ejemplo), en los sitios de los clientes (servidores web y otras aplicaciones que utilizan certificados digitales) y en el propio software (navegadores web, dispositivos de red, etc.). Para no quedarse atrás, las empresas deberán ser capaces de hacer cambios en su software con rapidez y sin que sus operaciones se vean afectadas. La gestión automatizada del ciclo de vida de los certificados facilita una parte importante de este proceso.

Los certificados son solo una parte (aunque importante) de la PQC. Muchos otros productos de software y hardware que utiliza, de muchos proveedores diferentes, también tendrán que actualizarse para ser compatibles con la PQC. Cabe mencionar que 2029 —el año en que entrarán en vigor todos estos cambios— es también el año en que, según Gartner, las organizaciones deben estar preparadas para la informática cuántica.

P: ¿Cómo se verán afectados los clientes que no son navegadores (como los dispositivos de red)?

El mercado de los certificados TLS públicos admite mayoritariamente certificados para navegadores instalados en algún tipo de servidor web, pero existen otros. Las pasarelas VPN y algunos dispositivos IoT son buenos ejemplos de ello.

Estos dispositivos también tendrán que aumentar la frecuencia de la CLM. Muchos de ellos admiten directamente ACME o algún otro protocolo de automatización, por lo que cambiar los parámetros no debería ser una tarea demasiado pesada. En otros casos, podrían ser compatibles con un mecanismo de automatización alternativo o con ninguno, en cuyo caso el usuario tiene que hacer algo de programación para automatizar.

Seguir el nuevo calendario en estos dispositivos será un problema común. Es importante crear un inventario completo de sus activos afectados, un proceso con el que puede ayudarle DigiCert.

¿Puedo renovar mis certificados antes de la fecha límite de 2026 para que sigan teniendo una validez de 398 días?

Sí. No va contra las normas renovar los certificados antes del 15 de marzo de 2026 para conseguir otros 398 días de validez, pero es una prórroga única: la siguiente vez que renueve sus certificados, la duración máxima se habrá reducido a 100 días. Asegúrese de automatizar el proceso con CertCentral o Trust Lifecycle Manager con antelación para prepararse.

Si necesita generar una clave nueva para su certificado a partir del 15 de marzo de 2026, DigiCert (y cualquier otra CA pública) deberá respetar las normas vigentes en ese momento, por lo que obtendrá, en el mejor de los casos, un certificado con una validez de 200 días.

El mejor momento para automatizar la gestión de certificados es tan pronto como pueda. Así, se asegurará de que su empresa está preparada para hacerlo sin arriesgarse a sufrir interrupciones, ya sea por culpa de certificados caducados o por cualquier otra causa.

Obtenga más información sobre cómo DigiCert puede ayudarle a automatizar la gestión de certificados para prepararse para la reducción de los períodos de validez de los certificados.