

INFORME · OCTUBRE 2026 · MES DE LA CIBERSEGURIDAD

CERTIFICADOS 2026: VIGENCIAS, AUTOMATIZACIÓN Y LA ERA POST CUÁNTICA

Las nuevas reglas del CA/Browser Forum, el camino a los **47 días**, los protocolos que sostienen la confianza en la web y cómo prepararse para la criptografía resistente a la computación cuántica.

47 días

vigencia máxima de un certificado TLS público desde marzo de 2029

34%

de las organizaciones tiene un inventario completo y al día de sus certificados

2035

año en que NIST propone prohibir RSA y ECC por el riesgo cuántico

CONTENIDO

- 01 Hallazgos clave
- 02 Tipos de certificado
- 03 Vigencias: de 398 a 47 días
- 04 Otras reglas del CA/Browser Forum
- 05 El riesgo de no automatizar
- 06 Automatización: protocolos y prácticas
- 07 DigiCert Trust Lifecycle Manager
- 08 Computación post cuántica
- 09 Protocolos de la confianza en la web
- 10 Plan de acción
- 11 Diagnóstico gratuito y fuentes

INTRODUCCIÓN

Los certificados digitales son la infraestructura invisible de cada conexión segura: sitios web, APIs, correo, VPN, dispositivos y aplicaciones. En 2026 cambian tres cosas a la vez: **las vigencias se acortan** por decisión de la industria, **las reglas de emisión se endurecen** y **la computación cuántica** obliga a planificar el reemplazo de la criptografía actual.

Gestionar certificados a mano ya no es viable. Este informe explica qué cambia, por qué y cómo prepararse.

01 · HALLAZGOS CLAVE

200 días

vigencia máxima de un certificado TLS público desde el 15 de marzo de 2026

~8

renovaciones al año por certificado cuando la vigencia llegue a 47 días

10 días

plazo de reutilización de la validación de dominio desde 2029

34%

de las organizaciones tiene un inventario completo y actualizado de certificados

73%

está muy o extremadamente preocupada por caídas por certificados vencidos

+38%

crecimiento anual de DigiCert Trust Lifecycle Manager, impulsado por la automatización

Fuente: CA/Browser Forum, Ballot SC-081; DigiCert 2026 Global PKI Research; DigiCert, comunicado del 6 de octubre de 2026.

En una frase

La vigencia de los certificados se reduce a una octava parte, la validación se repite con más frecuencia y la criptografía que los firma tendrá que cambiar. **Solo una gestión automatizada y con inventario completo puede absorber ese ritmo sin caídas.**

02 · TIPOS DE CERTIFICADO

Tipo	Qué valida	Uso típico
DV · Validación de dominio	Solo el control del dominio	Sitios informativos, entornos de prueba
OV · Validación de organización	Dominio y existencia legal de la empresa	Sitios corporativos, portales, APIs
EV · Validación extendida	Verificación rigurosa de identidad legal	Banca, comercio electrónico, gobierno
Wildcard	Un dominio y todos sus subdominios de un nivel	*.empresa.com
Multidominio (SAN)	Varios dominios en un certificado	Grupos de marcas, entornos mixtos

Más allá del sitio web

PKI privada

Certificados emitidos por una CA interna para usuarios, dispositivos, VPN, Wi-Fi y servicios internos. No dependen de las reglas del CA/Browser Forum, pero sí de una buena gestión.

S/MIME, firma de código y firma de documentos

Firman y cifran correos, garantizan la integridad del software y dan validez legal a documentos.

Certificados de marca (VMC / CMC)

Muestran el logo verificado de la empresa junto al remitente en la bandeja de entrada, con BIML.

El candado no es identidad: un certificado DV se obtiene gratis en minutos y los sitios de phishing lo usan. OV y EV verifican quién está detrás del dominio.

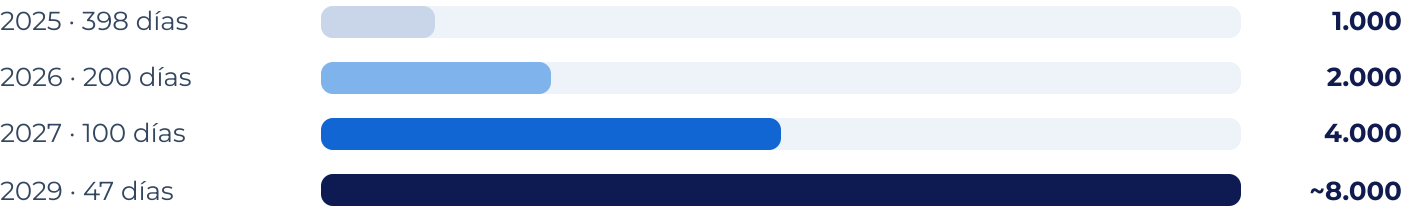
03 · VIGENCIAS: DE 398 A 47 DÍAS

El 11 de abril de 2025 terminó la votación del **Ballot SC-081** en el CA/Browser Forum, propuesto por Apple. Google, que antes promovía 90 días, votó a favor casi de inmediato. Reduce de forma escalonada la vigencia de los certificados TLS públicos y el tiempo que una CA puede reutilizar una validación:

Desde	Vigencia máxima	Reutilización de validación de dominio	Renovaciones al año
Hasta 14 mar 2026	398 días	398 días	~1
15 mar 2026	200 días	200 días	~2
15 mar 2027	100 días	100 días	~4
15 mar 2029	47 días	10 días	~8

Fuente: CA/Browser Forum, Ballot SC-081 (Baseline Requirements). Desde el 15 de marzo de 2026, la información de identidad de la organización en certificados OV y EV (razón social y otros datos) solo puede reutilizarse por 398 días, frente a los 825 anteriores. No afecta a los DV.

El impacto en números



Renovaciones al año para una organización con 1.000 certificados. Cada renovación implica generar la clave, solicitar, validar, instalar y verificar.

Por qué se acortan

- **Menos tiempo de exposición** si una clave se compromete o un certificado se emite por error.
- **La revocación no funciona bien a escala:** los navegadores no siempre la consultan, así que una vigencia corta es la forma más confiable de retirar un certificado.
- **Agilidad criptográfica:** renovar con frecuencia prepara la infraestructura para cambiar de algoritmo, incluida la transición post cuántica.

Tres preguntas frecuentes

¿Por qué justo 47 días?

Es una cascada: **200** = 6 meses de 31 días + medio mes + 1 día de margen; **100** = 3 meses de 31 días + un cuarto de mes + 1 día; **47** = 1 mes de 31 días + medio mes + 1 día.

¿Se puede seguir validando a mano?

Técnicamente sí, pero con la reutilización de validación en **solo 10 días** desde 2029, hacerlo manualmente es una receta para errores y caídas. Desde 2023 existen además certificados de corta duración, de hasta 7 días, que no requieren CRL ni OCSP.

¿Renovar más seguido cuesta más?

No. El costo se basa en una suscripción anual, no en la cantidad de reemplazos. DigiCert soporta ACME para certificados DV, OV y EV, incluido ACME Renewal Information (ARI).

04 · OTRAS REGLAS DEL CA/BROWSER FORUM

Además de las vigencias, las reglas de emisión se han endurecido en los últimos dos años:

Validación desde múltiples perspectivas (MPIC)

Las CA deben comprobar el control del dominio desde varias ubicaciones de red, para frenar ataques de secuestro de rutas BGP o DNS durante la validación. Obligatorio desde 2025.

Registros CAA · RFC 8659

El dueño del dominio declara en el DNS qué CA puede emitir certificados para él. Las CA están obligadas a consultarlo.

Certificate Transparency · RFC 6962

Todo certificado público se registra en bitácoras públicas y auditables. Permite detectar emisiones no autorizadas a nombre de su dominio.

Revocación: CRL obligatoria, OCSP opcional

Desde 2024 las CA pueden dejar de operar OCSP y basarse en listas de revocación (CRL). Varias ya apagaron sus servicios OCSP.

Jerarquías dedicadas a TLS

Los programas raíz de los navegadores exigen que los certificados públicos de servidor no se usen para autenticación de cliente; ese uso se retira de las jerarquías TLS públicas durante 2026.

Fuera del CA/Browser Forum, los **programas raíz** de Google, Apple, Mozilla y Microsoft pueden retirar la confianza a una CA que no cumpla. Elegir una CA sólida y con historial es parte de la gestión del riesgo.

05 · EL RIESGO DE NO AUTOMATIZAR

34%

tiene un inventario completo
y al día de sus certificados

73%

teme caídas por certificados
vencidos

100.000+

certificados gestionan
algunas grandes empresas
con TLM

Fuente: DigiCert 2026 Global PKI Research; DigiCert, comunicado del 6 de octubre de 2026.

Un certificado vencido detiene un sitio, una API de pagos, una VPN o la conexión entre microservicios. Los errores más comunes:

- **Certificados desconocidos:** emitidos por equipos o proveedores fuera del control central.
- **Renovaciones en planilla:** recordatorios por correo que nadie recibe cuando alguien deja la empresa.
- **Renovar sin instalar:** el certificado nuevo existe, pero el servidor sigue usando el antiguo.
- **Dependencias ocultas:** balanceadores, appliances y almacenes de confianza que nadie revisa.

“Una sola renovación olvidada puede provocar una caída costosa, y las vigencias más cortas dejan menos margen de error al gestionar miles de certificados.”

Deepika Chauhan, Chief Product Officer, DigiCert · octubre 2026

06 · AUTOMATIZACIÓN: PROTOCOLOS Y PRÁCTICAS

Automatizar es encadenar cinco pasos sin intervención: **descubrir, emitir, instalar, renovar y revocar**. Los estándares que lo hacen posible:

Protocolo	RFC	Para qué sirve
ACME	RFC 8555	Emisión y renovación automática de certificados TLS
ACME ARI	RFC 9773	La CA indica cuándo conviene renovar, incluso antes de tiempo
EST	RFC 7030	Inscripción segura de dispositivos y servicios
SCEP	RFC 8894	Inscripción de dispositivos móviles y de red (MDM)
CMP	RFC 9480	Gestión de certificados en entornos industriales y telecom

Novedades que eliminan trabajo manual

Validación continua de dominio

Con DNS gestionado, el dominio queda validado de forma permanente y listo para emitir y renovar sin pasos manuales: clave cuando la reutilización baje a 10 días.

Gestión de almacenes de confianza

Distribución automática de certificados raíz e intermedios en toda la empresa: evita caídas y prepara el cambio de algoritmos.

Atestación de dispositivos Apple

Verifica la identidad del hardware antes de emitir el certificado, con inscripción automática en equipos gestionados.

Fuente: DigiCert, comunicado del 6 de octubre de 2026.

07 · DIGICERT TRUST LIFECYCLE MANAGER

DigiCert Trust Lifecycle Manager (TLM) descubre, emite, instala y renueva certificados públicos y privados desde una sola consola, con cualquier CA y en entornos híbridos y multinube.

+38%

crecimiento anual de ingresos recurrentes de TLM

Líder

IDC MarketScape: Certificate Lifecycle Management 2026

90%

de las Fortune 500 confía en DigiCert

Fuente: DigiCert, comunicado del 6 de octubre de 2026.

Descubrimiento e inventario

Encuentra certificados y activos criptográficos en servidores, nube, balanceadores y dispositivos, sin abrir puertos de entrada.

Políticas y gobierno

Reglas por algoritmo, longitud de clave, CA y vigencia; alertas y reportes de cumplimiento.

Automatización de extremo a extremo

Renovación e instalación automática con agentes, sensores e integraciones con F5, Fortinet, NetScaler, Imperva, HashiCorp, HPE, BeyondTrust, AWS, Azure y Kubernetes.

Lo usan, entre otras, American Red Cross, Agilent, Circle K, Hitachi, MGM Resorts, Nokia y Schweizerische Mobiliar.

“A medida que se acortan las vigencias, la gestión manual se vuelve cada vez más difícil a escala empresarial. Trust Lifecycle Manager nos da la visibilidad y automatización que necesitamos para reducir el riesgo operacional.”

Kenneth Nydegger, Product Owner, Schweizerische Mobiliar

08 · COMPUTACIÓN POST CUÁNTICA

Un computador cuántico suficientemente potente podrá romper RSA y la criptografía de curva elíptica (ECC), que hoy protegen casi todos los certificados. No existe aún, pero el riesgo ya es actual: **“cosechar ahora, descifrar después”**. Un atacante puede guardar hoy tráfico cifrado y descifrarlo cuando la tecnología esté disponible.



Fuente: DigiCert, Post-Quantum Cryptography.

No hay una fecha fija para la llegada de un computador cuántico capaz de romper el cifrado actual, pero **prepararse toma más tiempo del que parece**: inventariar la criptografía de toda la empresa, definir una hoja de ruta por cada caso de uso y ejecutar la migración. Mientras tanto, la innovación cuántica y la adopción de los nuevos algoritmos se aceleran.

Los nuevos estándares de NIST

Estándar	Algoritmo	Uso
FIPS 203	ML-KEM (Kyber)	Intercambio de claves
FIPS 204	ML-DSA (Dilithium)	Firma digital, principal candidato para certificados
FIPS 205	SLH-DSA (SPHINCS+)	Firma digital basada en hash, respaldo conservador
FN-DSA	Falcon	Firma compacta, en proceso de publicación

Fuente: NIST, estándares publicados en agosto de 2024; NIST IR 8547.

Calendario de transición

Hito	Qué ocurre
2024	NIST publica los primeros estándares post cuánticos.
2025–2026	Navegadores y CDN activan por defecto el intercambio de claves híbrido (X25519 + ML-KEM) en TLS 1.3.
2030	NIST propone deprecAR RSA y ECC de 112 bits de seguridad.
2035	NIST propone prohibir RSA y ECC en sistemas federales.

Qué hacer hoy

- **Inventario criptográfico:** saber qué algoritmos y claves usa cada sistema.
- **Agilidad criptográfica:** poder cambiar de algoritmo sin rehacer la infraestructura; la automatización es la base.
- **Priorizar datos de larga vida:** lo que debe seguir confidencial por más de 10 años.
- **Probar en laboratorio** certificados híbridos y post cuánticos antes de que sean obligatorios.

Herramientas para empezar

DigiCert ofrece un verificador de preparación cuántica para TLS y, en DigiCert Labs, un entorno de pruebas Quantum Safe y el código para montar un servidor de prueba con certificados ML-DSA. TLM ganó en los Global InfoSec Awards y fue reconocido como Producto de Computación Cuántica del Año 2026 por TMCnet.

09 · PROTOCOLOS DE LA CONFIANZA EN LA WEB

Estándar	RFC	Función
X.509	RFC 5280	Formato de los certificados y listas de revocación
CSR · PKCS#10	RFC 2986	Solicitud de certificado
TLS 1.3	RFC 8446	Versión actual del protocolo seguro: más rápida y sin cifrados débiles
TLS 1.0 y 1.1	RFC 8996	Formalmente obsoletos: deben deshabilitarse
HSTS	RFC 6797	Obliga al navegador a usar siempre HTTPS
OCSP	RFC 6960	Consulta de revocación en línea; en retirada en la web pública
CAA	RFC 8659	Qué CA puede emitir para un dominio
Certificate Transparency	RFC 6962 / 9162	Registro público de certificados emitidos
ACME	RFC 8555	Automatización de emisión y renovación
MTA-STS	RFC 8461	TLS obligatorio para el correo entre servidores

Configuración recomendada

- Solo **TLS 1.2 y 1.3**, con cifrados de secreto perfecto hacia adelante.
- Claves **RSA de 2048 bits** como mínimo, o **ECDSA P-256**.
- **HSTS** activado y registros **CAA** publicados.
- Monitoreo de **Certificate Transparency** para detectar emisiones no autorizadas.

10 · PLAN DE ACCIÓN

Con 200 días ya vigentes y 100 en marzo de 2027, **el momento de automatizar es antes del próximo recorte.**

- 1 Descubrir.** Inventario completo de certificados públicos, privados y activos criptográficos.
- 2 Centralizar.** Una consola, un responsable por certificado y políticas claras.
- 3 Proteger el dominio.** Registros CAA y monitoreo de Certificate Transparency.
- 4 Automatizar.** ACME, agentes e integraciones para renovar e instalar sin intervención.
- 5 Validación continua.** Preparar la validación de dominio para el plazo de 10 días de 2029.
- 6 Endurecer protocolos.** TLS 1.2/1.3, HSTS y fin de TLS 1.0/1.1.
- 7 Agilidad criptográfica.** Inventario de algoritmos y pruebas post cuánticas.
- 8 Medir.** Reportes de vencimientos, cumplimiento y caídas evitadas.

Cómo lo hacemos en Digitalcorp LATAM

Implementamos **DigiCert Trust Lifecycle Manager** y certificados **DigiCert y GeoTrust** (DV, OV, EV, wildcard y multidominio), con PKI privada, firma de código y preparación post cuántica. Diagnóstico, despliegue y soporte local en español.

11 · DIAGNÓSTICO GRATUITO

REVISE SUS CERTIFICADOS EN **TOOLS.DIGITALCORPLATAM.COM**

Herramientas sin costo y sin instalar nada para revisar certificados, configuración TLS y correo.

Verificador SSL · validez, cadena y vencimiento

Cabeceras HTTP · HSTS, CSP y más

MTA-STS · TLS-RPT · cifrado del correo en tránsito

Decodificador CSR · dominio, SAN y algoritmo

Analizador DMARC · SPF, DKIM, DMARC, MTA-STS y BIMi

Formateador BIMi · logo a SVG Tiny PS

tools.digitalcorplatam.com

Fuentes: CA/Browser Forum, Baseline Requirements y Ballot SC-081; DigiCert, “TLS Certificate Lifetimes Will Officially Reduce to 47 Days” (Stephen Davidson, 16 de mayo de 2025) y FAQ “¿Cuánto duran los certificados TLS/SSL?”; DigiCert, “Post-Quantum Cryptography” y DigiCert Labs; DigiCert, comunicado “DigiCert Accelerates Trust Lifecycle Manager Growth” (6 de octubre de 2026) y 2026 Global PKI Research; IDC MarketScape: Worldwide Certificate Lifecycle Management 2026; NIST FIPS 203, 204 y 205, e IR 8547; IETF — RFC 5280, 2986, 8446, 8996, 6797, 6960, 8659, 6962, 9162, 8555, 9773, 7030, 8894, 9480 y 8461. Las fechas de transición post cuántica de NIST son propuestas y pueden ajustarse. Digitalcorp LATAM es partner de DigiCert en Latinoamérica. Este informe es informativo.