SEGURIDADAMÉRICA.com
Fortaleciendo Internet

GlobalSign by GMO

LIVE WEBINAR

# CERTIFICADOS SSL/TLS: CAMBIOS INMINENTES Y AUTOMATIZACIÓN ESTRATÉGICA

## Preparando tu organización para 2026

**DIEGO LÓPEZ**
Jefe de Soporte TI

**SPEAKERS**

**FRANCISCO SANTIBÁÑEZ**
Gerente Comercial

# Introducción

La gestión de certificados SSL/TLS ha cambiado drásticamente en los últimos años. Hoy, las organizaciones enfrentan ciclos de vida más cortos, una mayor carga operativa y la necesidad de prevenir caídas críticas por expiraciones no detectadas.

**Queremos que al terminar este webinar puedas:**

- Entender el porqué de los cambios en la vigencia de certificados.
- Conocer los riesgos reales de una mala gestión.
- Evaluar herramientas y prácticas para automatizar procesos.

# Evolución de la vigencia de los certificados

**Desde 1995**
la duración de los certificados SSL/TLS ha disminuido progresivamente:

1995 → 5 años
↓
3 años → 2 años → 13 meses → propuesta de 47 días → 200 días (2026)

Este cambio refleja una tendencia clara: menor tolerancia al riesgo, necesidad de adaptarse rápidamente a nuevos estándares y más control sobre los certificados emitidos.

*Con cada reducción se vuelve más difícil mantener control sin herramientas automatizadas.*

# Organismos que definen las reglas

Detrás de estos cambios están el CA/B Forum (Certificate Authority/Browser Forum) y los principales navegadores web.

Estas entidades establecen los requisitos técnicos y las buenas prácticas que todas las Autoridades Certificadoras deben seguir. Cuando ellos cambian una regla, el ecosistema digital completo debe adaptarse.

# ¿Por qué se reduce la vigencia?

## Motivos de seguridad y eficiencia

- 🔐 Menor exposición ante compromisos: si un atacante roba un certificado, tendrá menos tiempo para aprovecharlo.
- 🔄 Actualización constante de estándares: las CA pueden emitir certificados con configuraciones más seguras.
- ⚙️ Mayor control criptográfico: menos tiempo = más vigilancia sobre el ecosistema digital.

# ¿Dejarías tu cerradura sin cambiar durante 5 años?

Una cerradura antigua es una analogía perfecta. Aunque pueda seguir funcionando, su seguridad se degrada con el tiempo. ¿Te sentirías seguro con la misma llave por 5 años?

Del mismo modo, los certificados digitales necesitan actualizarse con frecuencia para mantener tu infraestructura protegida.

La tecnología cambia, las amenazas también.

# Qué pasará desde 2026


La reducción implicará duplicar (o más) los procesos de renovación.
Para muchas empresas, esto será insostenible sin automatización

| Ahora 2025 | 15 de marzo 2026 | 15 de marzo 2027 | 15 de marzo 2029 |
|---|---|---|---|
| Vigencia del certificado 398 Días | Vigencia del certificado 200 Días | Vigencia del certificado 100 Días | Vigencia del certificado 47 Días |
| Validez del dominio/IP 398 Días | Validez del dominio/IP 200 Días | Vigencia del dominio/IP 100 Días | Vigencia del dominio/IP 10 Días |
| Validación de Organización 825 Días | Validación de Organización 398 Días | | |

# Riesgos Reales

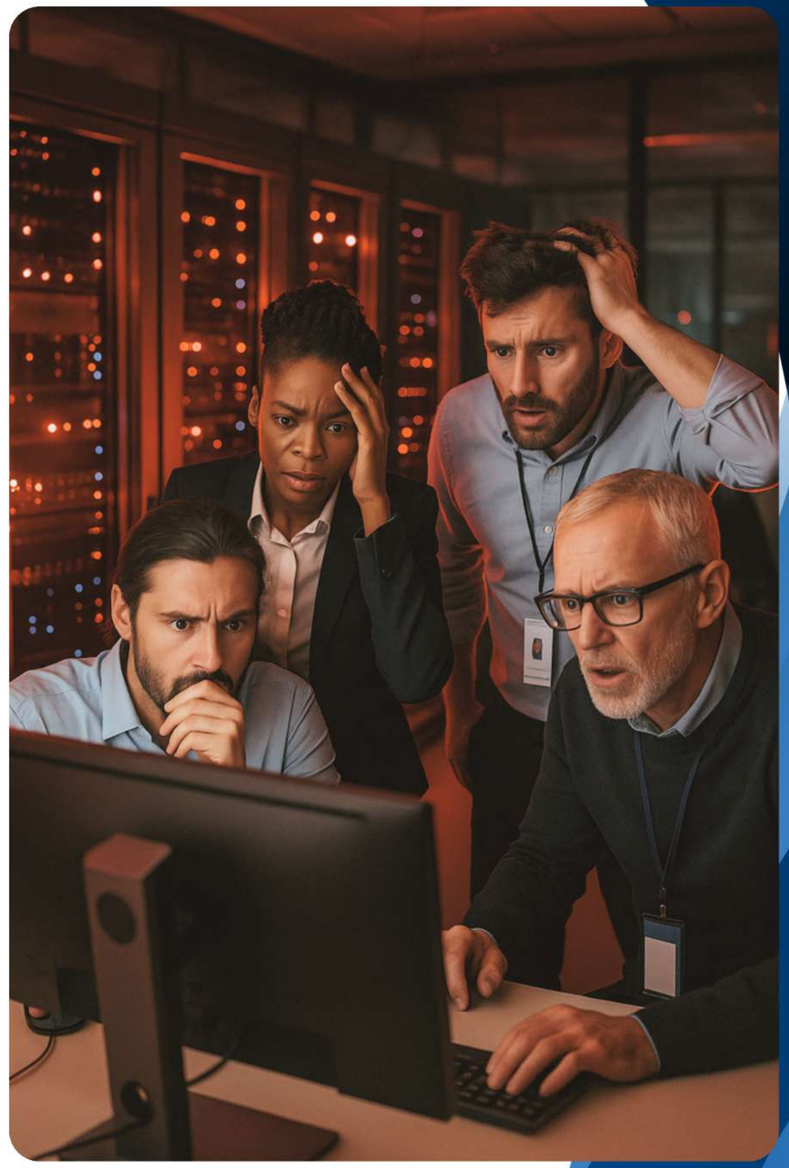
## Casos concretos de empresas afectadas

- **LinkedIn** y **Spotify** experimentaron caídas globales por certificados vencidos

- **Red social internacional (2021)** también sufrió fallas críticas por el mismo motivo.

Esto demuestra que incluso grandes empresas pueden fallar si no tienen un proceso automatizado.
Impactos:

- Interrupción de servicios
- Pérdida de usuarios
- Daño reputacional y económico



# ¿Qué podemos hacer?

## Automatizar es obligatorio, no opcional

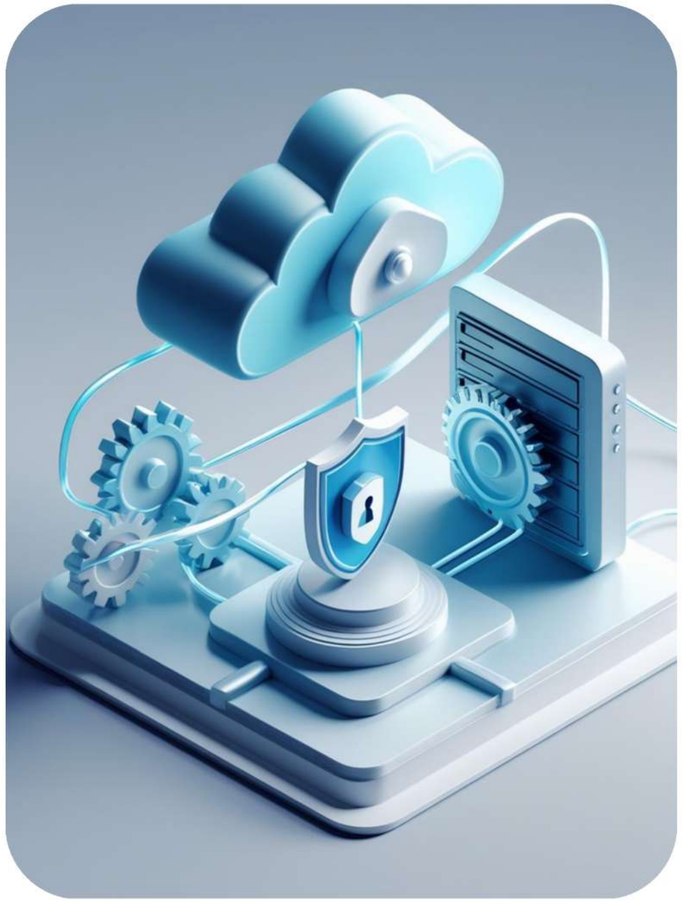
La automatización ya no es una opción, es una necesidad. La gestión manual de certificados no permite crecer ni adaptarse a las demandas actuales. Con ciclos de vida cada vez más cortos, la única forma eficiente de administrar múltiples certificados es automatizando todo el proceso: desde la emisión hasta la renovación y revocación.

*“Automatizar ya no es una opción. Es obligatorio.”*

# ACME: Automatic Certificate Management Environment

**¿Qué es ACME?**

Es un protocolo de comunicación para automatizar interacciones entre autoridades certificadoras y los servidores de sus usuarios, permitiendo el despliegue automático a bajo costo. Creado por el Internet Security Research Group para su servicio Let’s Encrypt.



**Definición en sencillas palabras:**

-Es un protocolo, un medio de comunicación entre equipos.
-Utilizado de manera que el servidor alojando un sitio web pueda solicitar un certificado directamente a una CA.
-Creado por los controladores de Let's Encrypt.
-Let's Encrypt es la CA que ofrece DVs de 90 días gratis.
-Beneficio: AUTOMATIZACION.

***Una vez configurado, puedes solicitar un certificado, validar el dominio, instalar el certificado en el servidor y renovarlo automáticamente.***

## ¿Cómo funciona?

-La CA tiene un servidor ACME.
-El webserver del cliente tiene un agente/cliente ACME.
-El cliente/agente ACME genera un par de llaves (CSR + Llave privada que se queda en el server).
-Valida el dominio en la hora (con HTTP o DNS, DNS necesario para WildCard).
-Después de Validar el dominio, envía el CSR a la CA.
-El servidor ACME de la CA regresa el certificado.
-ACME lo instala (bind) y crea una tarea (scheduled task) para renovación automática antes de su expiración.

# Tabla comparativa

| Característica | GlobalSign (ATLAS + GCC) | DigiCert CertCentral | Keyfactor Command | Certinext |
|---|---|---|---|---|
| Automatización completa | ✅ Emisión, renovación, revocación, descubrimiento automático | ⚠️ Limitada en entornos con certificados ligados a apps | ✅ Avanzada pero compleja de implementar | ❌ Requiere configuración manual |
| Facilidad de integración | ✅ API REST, AD, MDM, SaaS listo para usar | ⚠️ Requiere configuración por agente o sensor | ⚠️ Requiere conocimientos PKI avanzados | ❌ Integración básica |
| Escalabilidad y rendimiento | 🔝 99.95% de disponibilidad, alto volumen de certificados | ⚠️ Buen rendimiento pero con limitaciones en descubrimiento | 🔝 Alta escalabilidad, pero con curva de aprendizaje | ⚠️ Escalabilidad media |
| Soporte técnico | ✅ Especializado, con enfoque local y personalizado | ✅ 24/7, pero con menor personalización | ⚠️ Limitado por falta de equipos PKI dedicados | ⚠️ Soporte limitado |
| Costo y retorno de inversión (ROI) | ✅ Modelo accesible, sin necesidad de CA interna | ⚠️ Costos elevados y complejidad en implementación | ⚠️ Alto costo inicial, ROI a largo plazo | ✅ Bajo costo, pero limitado en funciones |
| Visibilidad y control | ✅ Panel centralizado, descubrimiento automático | ⚠️ Descubrimiento limitado si los certificados no están en el almacén | ✅ Dashboard robusto, pero requiere experiencia | ❌ Sin panel de control avanzado |

# Herramientas para una gestión moderna

**GlobalSign** ofrece soluciones robustas para automatizar y centralizar la gestión de certificados:

- **CAM:** Integración con Active Directory.
- **ATLAS:** Plataforma empresarial para emisión masiva.
- **Discovery Tool:** Inventario automático y alertas de expiración.

# Beneficios de la Automatización

## Qué gana tu empresa al automatizar

- Renovación automática, sin intervención manual.
- Visibilidad total sobre todos los certificados.
- Cumplimiento normativo más sencillo.
- Menos errores humanos y mayor continuidad operativa.

*Automatizar transforma un punto débil en una ventaja competitiva.*

# Conclusión y CTA

## Pasos recomendados tras el webinar

1. Audita tu inventario de certificados actuales.
2. Solicita una demo de nuestras soluciones.
3. Implementa automatización antes de que llegue 2026.

📌 *Evita ser el próximo caso de caída global.*

🎯 *Agenda tu asesoría personalizada.*

SEGURIDADAMÉRICA.com
Fortaleciendo Internet

LIVE WEBINAR

Atlas by GlobalSign

# Próxima Fecha Webinar

## 4 DE SEPT. 2025

**DIEGO LÓPEZ**
Jefe de Soporte TI

*SPEAKERS*

**FRANCISCO SANTIBÁÑEZ**
Gerente Comercial

Atlas - Plataforma de identidad digital

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

GlobalSign by GMO

# ¡GRACIAS POR LA ATENCIÓN!

WWW.SEGURIDADAMERICA.COM