

Guadalajara, Jalisco, a 19 de octubre de 2026

Guía de cambio de certificado SSL

services.sw.com.mx · Clientes SAP y otros sistemas

Lo esencial

Lo que no cambia: El dominio **services.sw.com.mx** y los endpoints; se actualiza únicamente el certificado que protege la conexión.

Ventana de cambio: Jueves 22 de octubre de 2026, de 22:00 a 23:00 h (hora de Ciudad de México).

Qué hacer: Confirmar que su almacén de confianza (STRUST en SAP; en otros sistemas, el de su firewall, proxy, servidor o aplicación) confía en **DigiCert Global Root G2** e importar la raíz y el intermedio si hace falta. En ABAP, SAP confía únicamente en lo importado en su PSE, no en el almacén del sistema operativo.

1. Qué cambia

Cambia el certificado y la entidad que lo emite:

	Antes	Ahora
Autoridad certificadora	Sectigo	DigiCert
Cadena de confianza	Raíz: Sectigo Public Server Authentication Root R46 (firma cruzada USERTrust RSA) Intermedio: Sectigo Public Server Authentication CA EV R36	Raíz: DigiCert Global Root G2 Intermedio: DigiCert Global G2 TLS RSA SHA256 2020 CA1
Razón social	LUNA SOFT S.A. DE C.V.	SW Sapien, S.A. de C.V.
Validación y llave	EV · RSA	OV · RSA 2048, SHA-256
Vigencia	Hasta el 6-nov-2026	16-oct-2026 a 16-abr-2027 (182 días)
Renovación	Manual	Automática antes del vencimiento (Azure Key Vault con DigiCert)

Por qué: El CA/Browser Forum reduce la vigencia máxima de los certificados públicos (398 días hasta marzo de 2026; 200 días actualmente; 100 días desde marzo de 2027; 47 días desde marzo de 2029). Por esto SW Sapien renueva el certificado de forma automática con Azure Key Vault y DigiCert.

Qué significa para usted: El certificado del servicio se renovará con mayor frecuencia, por eso la confianza se configura en la **raíz** de DigiCert, que no cambia con las renovaciones (vigente hasta enero de 2038), y no en el certificado individual.

Certificados de la cadena DigiCert

Certificado	Función	Dónde se configura
DigiCert Global Root G2	Ancla de confianza de la cadena; se mantiene entre renovaciones.	Almacén de confianza de su sistema
DigiCert Global G2 TLS RSA SHA256 2020 CA1 (intermedio)	Enlaza el certificado del servicio con la raíz; el servidor lo entrega en cada conexión. Algunas plataformas lo piden también de forma local.	Almacén de confianza de su sistema
services.sw.com.mx	Certificado del servicio; se renueva solo y el servidor lo presenta en cada conexión.	No requiere configuración en su sistema

Con la raíz y el intermedio configurados, las renovaciones del certificado del servicio no deberían requerir cambios en su sistema.

2. Antes de actualizar

Aplica si su sistema tiene cargado el certificado de **services.sw.com.mx** o los de Sectigo, ancla la huella del certificado, inspecciona tráfico SSL o usa un almacén de confianza propio (SAP, Java, .NET, Python, Node). Si usa el almacén estándar de un sistema operativo actualizado, probablemente no requiere cambios; solo confirme que confía en DigiCert Global Root G2.

- **Identifique dónde está cargado** el certificado actual y respalde la configuración: en SAP ABAP, el PSE en SM59 (Logon & Security, Certificado SSL: ANONYM, DFAULT u otro); en PI/PO y BTP, el almacén correspondiente (secciones 3.2 y 3.3); en firewalls, proxies, servidores y aplicaciones, su almacén de CA de confianza.
- **Responsable y ventana propia:** administrador Basis o de redes y seguridad. Si su versión de SAP requiere reiniciar el ICM, o el cambio en su equipo puede interrumpir tráfico (por ejemplo, al recargar la inspección SSL), planéelo en su ventana de mantenimiento.
- **Reglas y salida a DigiCert:** use reglas por nombre de dominio (FQDN) en lugar de huella o certificado. Si su firewall restringe tráfico saliente, permita **ocsp.digicert.com**,

crl3.digicert.com, crl4.digicert.com y cacerts.digicert.com (HTTP, puerto 80; tomados del propio certificado).

- **Archivos:** use el paquete adjunto o el sitio oficial de DigiCert. Con varios servidores de aplicación SAP, confirme que el PSE quede disponible en cada uno.
- **Certificados actuales:** consérvelos durante el cambio y retire después solo los que ningún otro servicio utilice. Si su organización requiere certificados EV o valida el campo Organización (antes LUNA SOFT), avise a soporte@sw.com.mx con anticipación.

Si su política solo permite importar el certificado del servidor

Es posible, pero ese certificado cambia con cada renovación. Por eso recomendamos, de ser posible, solicitar una excepción para confiar en la raíz y el intermedio, que no cambian. Si no es posible, escriba a soporte@sw.com.mx para validar esta situación en particular.

3. Procedimiento

Siga la sección que corresponde a su sistema: 3.1 a 3.3 para SAP y 3.4 a 3.6 para el resto.

3.1 SAP ABAP (ECC y S/4HANA): STRUST y SM59

Archivos del paquete: [DigiCertGlobalRootG2.cer](#) y [DigiCertGlobalG2TLSRSA2562020CA1.cer](#).

1. Transacción **STRUST**, modo edición, y abra el PSE SSL Client del destino (ver sección 2).
2. En Certificado, **Importar certificado**, seleccione [DigiCertGlobalRootG2.cer](#) y pulse **Añadir a lista de certificados**.
3. Repita con el intermedio [DigiCertGlobalG2TLSRSA2562020CA1.cer](#) y **guarde**.
4. Solo si su versión lo requiere, reinicie el ICM en su ventana de mantenimiento: **SMICM**, Administración, ICM, Salida soft.
5. Después de la ventana de cambio, pruebe en **SM59**: destino HTTP hacia services.sw.com.mx (puerto 443, SSL activo con ese PSE), **Test de conexión**. Resultado esperado: respuesta HTTP del servicio, sin mensaje SSL.

3.2 SAP PI/PO (NetWeaver Administrator)

1. NWA, Configuration, Security, **Certificates and Keys**, Key Storage, vista **TrustedCAs**.
2. **Import Entry**, tipo X.509 Certificate: raíz y luego intermedio.
3. Después de la ventana, pruebe un envío desde el canal de comunicación que apunta a services.sw.com.mx.

3.3 SAP BTP Integration Suite (Cloud Integration)

1. Monitor, Manage Security, **Manage Keystore**: revise si **DigiCert Global Root G2** ya aparece; si está y la huella coincide, no hace falta importarla de nuevo.
2. Si no está, **Add**, Certificate, y suba la raíz (de preferencia también el intermedio).
3. Después de la ventana, ejecute un **Connectivity Test (TLS)** hacia services.sw.com.mx, puerto 443, con la validación del certificado del servidor activada.

3.4 Firewalls, proxies, WAF y balanceadores (con o sin inspección SSL)

Archivo: [DigiCertGlobalRootG2.cer](#) (Base64). Los menús varían por fabricante; el flujo general es:

1. Ingrese a la consola con permisos para administrar certificados y abra el almacén de **CA de confianza** (CA certificates, Trusted CA, Trusted root o similar).
2. Importe la raíz como **CA de confianza** (por ejemplo, con el nombre [DigiCert Global Root G2](#)) y, si el equipo lo permite, el intermedio.
3. Si usa perfiles de inspección SSL, confirme que la CA esté **incluida en la lista de CA de confianza del perfil**; en algunos equipos no basta con importarla.
4. Si había reglas por huella del certificado de [services.sw.com.mx](#), cámbielas por reglas por nombre de dominio.
5. Aplique los cambios, recargue la política si el fabricante lo indica y verifique (sección 4).

3.5 Windows, IIS y .NET

Archivos: los dos [.cer](#). Desde una consola de administrador (almacén del equipo local):

```
certutil -addstore -f Root "DigiCertGlobalRootG2.cer"  
certutil -addstore -f CA "DigiCertGlobalG2TLRSASHA2562020CA1.cer"
```

También puede importarlos desde [certlm.msc](#) (Equipo local): la raíz en **Entidades de certificación raíz de confianza** y el intermedio en **Intermedias**. Windows actual normalmente ya incluye la raíz.

3.6 Linux, Java y aplicaciones

Archivo: **DigiCertGlobalRootG2.cer** (PEM).

```
# Debian / Ubuntu (extensión .crt)
sudo cp DigiCertGlobalRootG2.cer /usr/local/share/ca-certificates/DigiCertGlobalRootG2.crt
sudo update-ca-certificates

# RHEL / CentOS / Rocky / Fedora
sudo cp DigiCertGlobalRootG2.cer /etc/pki/ca-trust/source/anchors/
sudo update-ca-trust extract

# Java (solo si usa truststore propio; reinicie la aplicación)
keytool -importcert -trustcacerts -alias digicert-global-root-g2 -file
DigiCertGlobalRootG2.cer -keystore <ruta-truststore>
```

Las versiones recientes de Java y la mayoría de las aplicaciones ya confían en esta raíz. Si su aplicación usa un archivo de CA propio, agréguela ahí; en Node.js, por ejemplo, con **NODE_EXTRA_CA_CERTS** apuntando a **DigiCertGlobalRootG2.cer** (PEM; reinicie el proceso).

4. Verificación y mensajes frecuentes

Después de la ventana de cambio (22:00 a 23:00 h), valide la conexión. En SAP, con las pruebas indicadas en la sección 3; en otros sistemas, desde su equipo o aplicación:

```
curl -v https://services.sw.com.mx
openssl s_client -connect services.sw.com.mx:443 -servername services.sw.com.mx -
verify_hostname services.sw.com.mx -showcerts
```

Resultado esperado (salida de openssl): emisor **DigiCert Global G2 TLS RSA SHA256 2020 CA1** y **Verify return code: 0 (ok)**; bajo inspección SSL, el emisor visible puede ser el de su equipo. Con un almacén propio use **-CAfile** (openssl, PEM) o **--cacert** (curl).

SAP

Mensaje o situación	Qué indica	Qué hacer
SSSLERR_PEER_CERT_UNTRUSTED	La cadena no pudo validarse; suele ser que la raíz aún no está en el PSE del destino.	Confirme el PSE en SM59 (Logon & Security) e importe ahí la raíz y el intermedio.
Responde un servidor de aplicación y otro no	Conviene confirmar que todos los servidores tengan el PSE actualizado.	Guarde de nuevo en STRUST (o use Distribute) y pruebe desde cada servidor.
La importación no se refleja todavía	El ICM puede conservar la configuración anterior.	Reinicie el ICM solo si su versión lo requiere, en ventana de mantenimiento (SMICM, Salida soft).
Responden solo algunos destinos	Usan otra identidad SSL (ANONYM, DEFAULT u otra).	Importe la raíz en el PSE de cada destino.

Otros sistemas

Mensaje o situación	Qué indica	Qué hacer
unable to get local issuer certificate O certificate verify failed	La raíz (o el intermedio) aún no está en el almacén que usa el cliente.	Cárguela en el almacén correcto y reinicie el servicio o la aplicación.
El firewall indica certificado no confiable al inspeccionar	La CA no está en la lista del perfil de inspección SSL.	Agregue DigiCert Global Root G2 a la lista de CA de confianza del perfil.
La conexión funcionaba y cambia tras una renovación	Había una regla por huella o la hoja como confianza.	Cambie la regla a FQDN y cargue la raíz.
Mensaje de revocación (OCSP/CRL) o cadena incompleta	El firewall restringe la salida a DigiCert.	Permita ocsp.digicert.com , cr13.digicert.com , cr14.digicert.com y cacerts.digicert.com .

Si el mensaje continúa después de cargar la raíz y el intermedio, escriba a soporte@sw.com.mx con el texto exacto y la captura del test o el resultado de `openssl s_client`; con gusto lo revisamos.

5. Beneficios del cambio

- **Renovación automática:** Azure Key Vault y DigiCert emiten y renuevan el certificado sin intervención manual.

- **Alineado con la industria:** Cumple el calendario de vigencias del CA/Browser Forum (100 días en 2027, 47 días en 2029).
- **Confianza estable:** Raíz vigente hasta 2038, incluida en Windows, Java, navegadores y Linux actuales.
- **Configuración única:** Se realiza una vez; las renovaciones no deberían requerir cambios mientras la configuración no dependa del certificado individual.
- **Razón social actualizada** a SW Sapien, S.A. de C.V., con validación de organización (OV).

6. Preguntas frecuentes

¿Tendremos que repetirlo? ¿Por qué ahora dice SW Sapien y es OV? No, mientras confíen en DigiCert Global Root G2 (vigente hasta 2038). La razón social validada ante la CA es SW Sapien, S.A. de C.V., con validación de organización (OV); el servicio y el contrato no cambian.

¿Es seguro confiar en la raíz de DigiCert? Es una CA pública auditada, incluida en Windows, Java, navegadores y Linux; su sistema sigue validando que el certificado corresponda a services.sw.com.mx.

¿Y si la raíz no está en el almacén al momento del cambio? Si es la causa, impórtela y vuelva a probar (según la plataforma, puede requerirse recargar la configuración).

Archivos incluidos

El paquete adjunto contiene solo certificados públicos (sin llaves privadas). Son tres archivos, los mismos para cualquier sistema: **DigiCertGlobalRootG2.cer** (raíz) y **DigiCertGlobalG2TLSRSA2562020CA1.cer** (intermedio), en formato Base64, que aceptan STRUST, Linux, Java, Windows, firewalls y la mayoría de los equipos, así como **services.sw.com.mx.cer** (certificado del servicio - hoja) en caso de requerirlo.

Verificación opcional, huella SHA-256 de DigiCert Global Root G2:

CB:3C:CB:B7:60:31:E5:E0:13:8F:8D:D3:9A:23:F9:DE:47:FF:C3:5E:43:C1:14:4C:EA:27:D4:6A:5A:B1:CB:5F

También puede descargar la raíz del sitio oficial: <https://www.digicert.com/kb/digicert-root-certificates.htm>