12 de diciembre de 2025

Boletín 004: “*Actualización de Seguridad de Proveedores de Timbrado* “

Notificación Urgente: Refuerzo de Seguridad en Conexiones para Timbrado.

Asunto: Acción Requerida: Actualización de Protocolos TLS para la Continuidad del Servicio de Timbrado (Efectivo 6 de enero de 2026).

Estimado Cliente,

En nuestro compromiso constante con la seguridad y la protección de su información, y atendiendo a los nuevos estándares de la industria, le informamos sobre un cambio fundamental en los protocolos de conexión segura, utilizados por uno de nuestros proveedores de servicios de Timbrado Electrónico.

⚠ Próximo Cambio de Protocolos SSL/TLS por Proveedor Externo

Nuestro socio tecnológico encargado de la emisión y validación de sus comprobantes fiscales (Timbrado) migrará sus sistemas para utilizar **exclusivamente versiones seguras y modernas del protocolo TLS (Transport Layer Security)**.

- **Entidad Responsable del Cambio:** Proveedor(es) de Servicios de Timbrado.
- **Protocolos Requeridos:** Únicamente **TLS 1.2 y versiones superiores.**
- **Fecha de Implementación:** El cambio por parte del proveedor entrará en vigor a partir del **martes 6 de enero de 2026.**

A partir de esta fecha, cualquier intento de conexión a los servicios de timbrado utilizando protocolos obsoletos (como SSL 3.0, TLS 1.0 o TLS 1.1) será **rechazado automáticamente** por el proveedor, lo que podría interrumpir la emisión de sus documentos fiscales.

🛠 Acciones Críticas que como cliente debe realizar a brevedad

Para garantizar la **continuidad ininterrumpida** de su operación de timbrado, es imprescindible que su equipo técnico tome las siguientes medidas inmediatamente:

1. **Revisión de Sistemas:** Identifique todas las aplicaciones, conectores, librerías o servidores que utilizan la API de nuestro proveedor para la comunicación de timbrado.

   Por porte de Servicrece ya se realizaron los ajustes necesarios dentro del Sistema Administrativo Fxpert, se entregarán en una próxima actualización mayor del sistema. Contacte a nuestros ejecutivos para agendar la actualización y conocer la aplicabilidad de costos.

2. **Desactivación:** Desactive todas aquellas versiones anteriores a la versión 1.2. Para mayor información haga clic en el siguiente enlace:

   https://learn.microsoft.com/es-es/windows-server/identity/ad-fs/operations/manage-ssl-protocols-in-ad-fs

3. **Actualización de Configuraciones:** Asegúrese de que todos estos componentes estén configurados para **negociar y utilizar obligatoriamente TLS 1.2 o TLS 1.3.**

   - ***Sistemas Operativos:*** Verifique con su personal de soporte interno que sus servidores y equipos de cómputo estén actualizados y soporten TLS 1.2 o superior.

   - ***Microsoft SQL Server:*** Confirme con su personal de soporte interno que la versión de Microsoft SQL server cuente con actualizaciones y sea compatible con protocolos TLS 1.2 y superiores.

4. **Pruebas:** Realice pruebas de conexión de ser posible en un entorno controlado para verificar la compatibilidad y buen funcionamiento de todos los aplicativos antes de la fecha límite.

   Importante**:** Si sus sistemas no se actualizan antes del **6 de enero de 2026**, **el servicio de timbrado dejará de funcionar** para su empresa.

Sistema SysExpert - Fxpert : *¡Tus Aliados en el Cumplimiento!*

Un cordial saludo,

A t e n t a m e n t e
Departamento SCE (Sistemas de Comercio Exterior)

Preguntas Frecuentes (FAQ)

Pregunta	Respuesta
¿Qué es SSL/TLS?	Son protocolos criptográficos que establecen un canal seguro para la comunicación en internet. TLS (Transport Layer Security) es la versión moderna y segura que reemplazó a SSL (Secure Sockets Layer).
¿Por qué se vuelven obsoletas las versiones de TLS 1.0 y 1.1?	Estas versiones presentan vulnerabilidades de seguridad conocidas que ya no cumplen con los estándares mínimos de protección de datos de la industria. Migrar a TLS 1.2 o 1.3 elimina estos riesgos.
¿Qué pasa si no actualizamos?	A partir del 6 de enero de 2026, si su sistema intenta conectarse usando una versión obsoleta (como TLS 1.0 o 1.1), la conexión será bloqueada por nuestro proveedor. Esto resultará en la **imposibilidad de realizar el timbrado** de sus facturas y documentos fiscales.
¿Cómo sé qué versión estamos usando?	Debe consultar a su equipo de TI o al encargado de la infraestructura. La verificación incluye revisar la configuración del sistema operativo del servidor, el software del conector de timbrado y las librerías de conexión HTTP/S que esté utilizando.

Ligas de Interés

https://learn.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp-

https://www.internetsociety.org/deploy360/tls/basics/

https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/connect/tls-1-2-support-microsoft-sql-server