Eliminación de TLS1.0 (comercios)

El 14 de octubre de 2014, el equipo de seguridad de Google identificó una vulnerabilidad en el protocolo de seguridad SSLv3, empleado en la protección de las conexiones por Internet, conocida como "Poodle".
Esta vulnerabilidad permitiría a un atacante que realizara un ataque "Man-in-the-middle" obtener cookies HTTP, con las que podría robar información o tomar control de las cuentas de los usuarios.

Posteriormente, en diciembre 2014, se descubrió que un ataque tipo "Poodle" se podía ejecutar directamente sobre ciertas implementaciones del protocolo TLSv1.0.

https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls

Para garantizar la seguridad de las comunicaciones con los comercios, **Redsys** ya deshabilitó en el pasado el protocolo SSLv3 y **procederá a deshabilitar, en producción, el uso del protocolo TLSv1.0 el 3 de octubre de 2017 (SIS y TPVPC).**

En entornos no productivos (pruebas, integración, certificación), Redsys deshabilitará de inmediato tanto el protocolo TLSv1.0 como el protocolo TLSv1.1, de modo que se garantice que los nuevos comercios que se pongan en producción soporten el protocolo TLSv1.2.

¿Cómo verificar que mi navegador soporta TLSv1.2?

Si te conectas a los servicios de Redsys con navegador, debes verificar que soporta el protocolo TLSv1.2. En el siguiente enlace puedes comprobarlo.

https://www.ssllabs.com/ssltest/viewMyClient.html

Navegador Internet Explorer: Versión igual o superior a la 9.0 (Ver abajo soporte TLSv1.2 en función del Sistema Operativo Windows).

Navegador Firefox: Versión igual o superior a la 27

Navegador Chrome: Versión igual o superior a la 30

Navegador Safari: Versión igual o superior a la 7

Navegador Opera: Versión igual o superior a la 17

¿Cómo verificar que mi versión de Windows soporta TLSv1.2?

Windows XP, Vista, Server 2008, Server 2003: No son compatibles con TLS1.1 y 1.2.

Windows 7, 8, Server 2008 R2, y Server 2012: Se requieren ajustes en la configuración[1].

Windows 8.1, 10, Server 2012 R2, Server 2016: Habilitados TLS1.1 y 1.2 por defecto.

[1] https://support.microsoft.com/es-es/help/3140245/update-to-enable-tls-1.1-and-tls-1.2-as-a-default-secure-protocols-in-winhttp-in-windows

¿Cómo verificar que los desarrollos propietarios soportan TLS v1.2?

Si te conectas a Redsys mediante webservice, debes adaptar tu aplicación para permitir sólo la negociación TLSv1.2 (recomendado) y/o TLSv1.1 en las comunicaciones seguras y deshabilitar el protocolo TLSv1.0.

A continuación, se recogen los enlaces a la configuración del protocolo TLS para los lenguajes más habituales.

- **Java 6** (soporta TLSv1.2 a partir de JDK 6u121, pero no está habilitado por defecto):
  http://docs.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html

- **Java 7** (soporta TLSv1.2 pero no está habilitado por defecto):
  http://docs.oracle.com/javase/7/docs/technotes/guides/security/jsse/JSSERefGuide.html

- **Java 8** (habilita por defecto TLSv1.2):
  http://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html

- **.NET/C#** (.NET 4.5 puede configurarse para usar TLSv1.2; .NET 4.6 habilita por defecto TLSv1.2).
  http://msdn.microsoft.com/en-us/library/system.net.securityprotocoltype%28v=vs.110%29.aspx

- **PHP**: http://curl.haxx.se/libcurl/c/CURLOPT_SSLVERSION.html

Si el cifrado de la comunicación se realiza mediante librerías de terceros, será necesario actualizarlas para garantizar el uso de TLSv1.2 (recomendado) y/o TLSv1.1 y no del protocolo TLSv1.0.

Si dispones de la herramienta "openssl", puedes verificar si en tu cliente webservice soportas TLSv1.2 y/o TLSv1.1 mediante los siguientes comandos:

openssl s_client -connect <*dominio*>:<puerto> -tls1_2
openssl s_client -connect <*dominio*>:<puerto> -tls1_1

También puedes verificar si has deshabilitado TLSv1.0 ejecutando:

openssl s_client -connect <*dominio*>:<puerto> -tls1

Si la conexión se establece, el protocolo está soportado. Si obtienes un mensaje del tipo "handshake failure", el protocolo está deshabilitado.

Los comercios que lo consideren necesario podrán realizar validaciones contra los entornos de pruebas (sólo TLSv1.2).

Aclaración sobre el servicio TPVPC

Seguir las indicaciones para navegador Internet Explorer, para configurar (o verificar la configuración) del protocolo TLSv1.2/v1.1 en las siguientes modalidades de TPVPC:

- TPV-PC Web
- TPV-PC ActiveX
- Implantado (Windows)
- Implantado Web

Para el resto de modalidades de TPVPC (WebService, Implantado Java e Implantado Linux[2]), seguir las indicaciones para desarrollos propietarios.

Aclaración sobre el servicio mPOS

- **Android 5.0**: Habilitados TLSv1.1 y 1.2 por defecto.
- **Android 4.0 o inferior**: Redsýs actualizará en el Market de Android las aplicaciones propias del M-POS. El resto de aplicaciones implementadas por terceros deberán actualizar la librería que se proporcionará desde el servicio.
- **IOS**: Habilitados TLSv1.1 y 1.2 por defecto.

[2] Requiere versión actualizada de la librería de Redsys.