ESTANDAR DE CONFIGURACION TLS

Versión 1.0

Arquitectura y Estándares TI

25/02/2020

Tabla de contenido

1. Objetivos

El documento tiene como objetivo estandarizar la configuración TLS en los servidores de Desarrollo y certificación, para las aplicaciones creadas dentro del Banco de Crédito de Bolivia SA.

2. Consideraciones para la configuración.

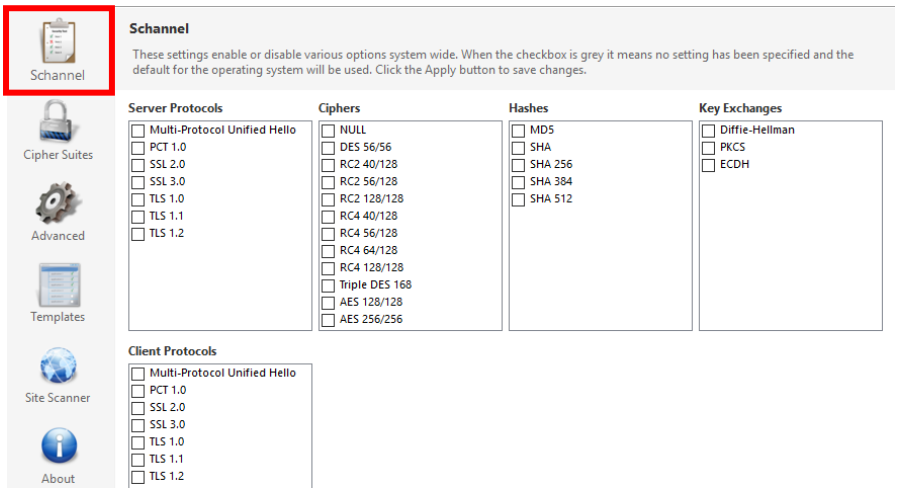
Para la configuración de TLS utilizaremos "IIS Crypto" es una herramienta gratuita que brinda a los administradores la capacidad de habilitar o deshabilitar protocolos, cifrados, hashes y algoritmos de intercambio de claves en Windows Server 2008, 2012, 2016 y 2019.

NOTA: **La configuración en ambientes de desarrollo puede ser realizada por el equipo de desarrollo.**

La configuración en ambientes de certificación y producción debe ser realizada por el equipo de servidores.

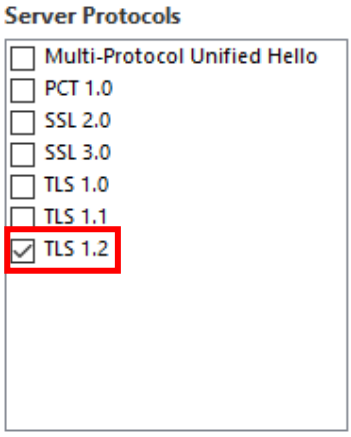
3. Configuración Schannel

Inicialmente ingresaremos a la opción Schannel.



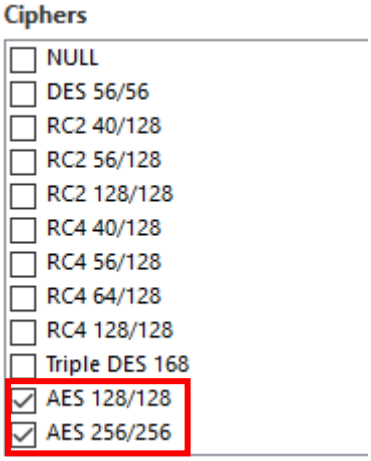
3.1. Configuración Server Protocols

Para la configuración de Server Protocols es requerido que habilite la opción TLS 1.2, como muestra a imagen.



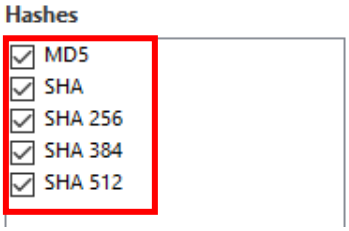
3.2. Configuración de Ciphers

Para la configuración de Ciphers habilite las siguientes opciones “AES 128/128” y “ASES 256/256” como muestra la imagen.



3.3. Configuración Hashes

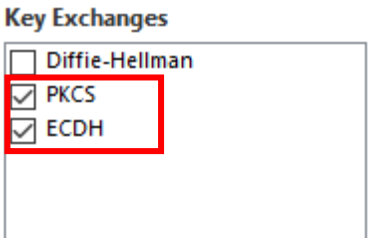
Por defecto deben estar seleccionados todas las casillas de la opción “Hashes”



NOTA: Las nuevas aplicaciones/desarrollos NO deben utilizar los algoritmos “MD5” y “SHA”.

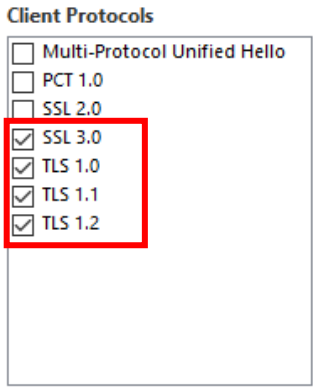
3.4. Configuración Key Exchanges

Para la configuración de Key Exchanges debe estar seleccionado la casilla de “PKCS” y “ECDH” como muestra la imagen.

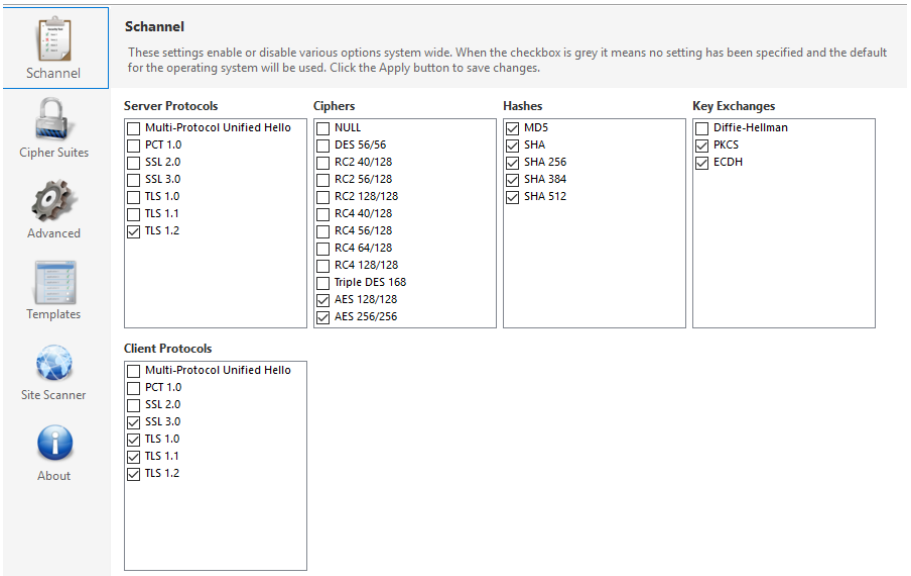


3.5. Configuración Client Protocols

Para la configuración de Client Protocols debe seleccionar las casillas “SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2” como muestra la imagen.

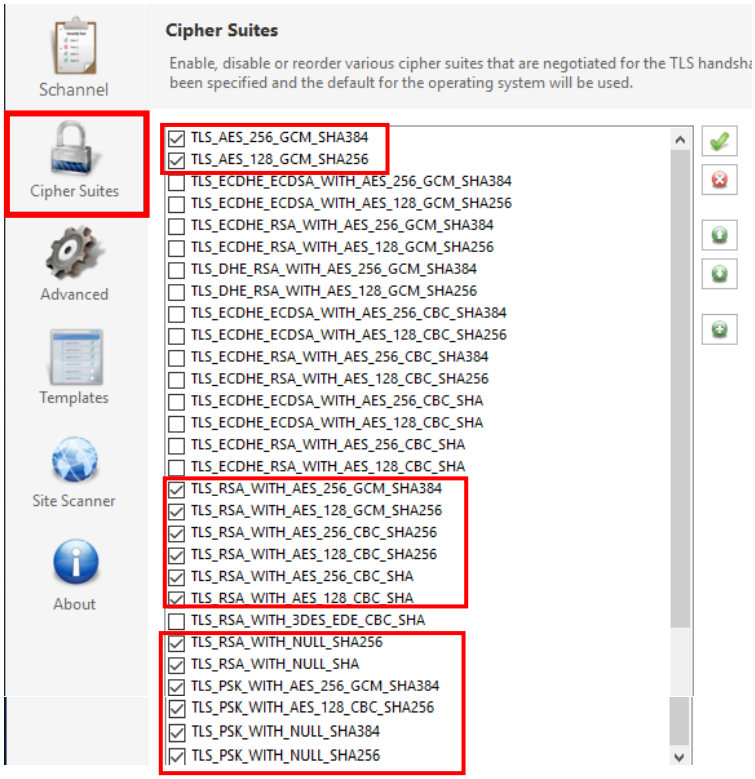


Al finalizar la configuración Schannel debería quedar la siguiente manera.



4. Configuración Cipher Suites

Para la configuración de la opción Cipher Suites seleccione las siguientes casillas:



NOTA: Para los Cipher Suites las siguientes casillas

- **DHE**
- **ECOHE**
- **3DES**

Deben estar deshabilitados, de otro modo el servidor esta vulnerable.