Apreciado cliente,

En este momento se encuentra soportado únicamente el protocolo TLS 1.2. Por lo tanto, en caso de presentar ausencia permanente de respuesta de Nuestros sistemas, la prueba que puede realizar para verificar el uso del protocolo TLS 1.2 en sus sistemas es activar en el firewall de ustedes un proceso de captura del tráfico (*debug)* desde la IP de su servidor de aplicaciones hacia la IP de PSE y lanzar una transacción y cuando obtengan la respuesta de nuestro servidor verificar en que versión de TLS se realizó la negociación; En caso de que no se realice en TLS 1.2 y en sus servidores y balanceadores lo tienen habilitado.

Es imprescindible actualizar sus sistemas para continuar con el servicio.

Los siguientes son los pasos que se han realizado los clientes para determinar los puntos de verificación de la actualización son los siguientes, los remitimos como recomendación con base en la experiencia y no constituyen lineamientos ni mandatos:

Se recomienda contar con un equipo conformado por Seguridad Informática, Servidores, Comunicaciones y aplicación de su empresa para realizar las validaciones correspondientes.

1. Verificar en la totalidad de nodos de la aplicación que se encuentre configurado el sistema de manera que se obligue a establecer comunicación por el protocolo más fuerte primero.
    1. .net → https://stackoverflow.com/questions/43872575/net-framework-4-6-1-not-defaulting-to-tls-1-2
       Es necesario que en la configuración de los servidores de aplicación se encuentre habilitado el protocolo TLS 1.2 con las suites de cifrado listadas.
       La verificación de la configuración la pueden realizar con ayuda de una herramienta, en el mercado existen herramientas de acceso libre para Windows como https://www.nartac.com/Products/IISCrypto/ con la cual pueden verificar la configuración del servidor.

2. Java → https://stackoverflow.com/questions/9749339/does-tomcat-support-tls-v1-2 https://stackoverflow.com/questions/9619030/resolving-javax-net-ssl-sslhandshakeexception-sun-security-validator-validatore https://stackoverflow.com/questions/6659360/how-to-solve-javax-net-ssl-sslhandshakeexception-error

   Bajo TLS 1.2, Java **verifica los Endpoints y sus Certificados**, Descargamos el certificado del dominio pse.com.co y lo añadimos al "C:\Program Files\Java\jre1.8.0_65\lib\security\cacerts" utilizando el comando: keytool -import -trustcacerts -alias samplePPE2 -file pse.com.co.cer -noprompt -keystore %JKSkeystore% -storepass %JKSkeystorepassword%

   También es probable que requiera instalar de nuevo el certificado en el java.

2. Ejecutar captura de tráfico desde el nodo de aplicación en el cual se está realizando la prueba y determinar la suite con la cual se está estableciendo la comunicación.
3. Ejecutar escucha del tráfico e identificar la totalidad de nodos/componentes por los cuales se realiza la comunicación, de modo que se verifique uno a uno.
4. Verificar que la totalidad de nodos de la aplicación, así como dispositivos activos en la red por la cual la comunicación viaja son compatibles con TLS 1.2 y específicamente con las siguientes suites de cifrado.
   - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
   - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
   - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA**256**
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

Tenga en cuenta el nombre completo de las suites, ***incluyendo el número al final.***

5. Escuchar el tráfico entrante en el firewall desde la IP de PSE-WS 172.30.19.30 y verificar en qué nodos al interior del banco atienden las peticiones y ver compatibilidad con TLS 1.2
6. *Solo para bancos. → Escuchar el tráfico entrante en el firewall desde la IP de PSE-SONDA 172.30.19.31 y verificar en qué nodos al interior del banco de atienden las peticiones y ver compatibilidad con TLS 1.2*
7. Reiniciar la conexión a nuestro servicio para forzar a los sistemas a determinar una nueva negociación.
8. *Algunos clientes han reinstalado los certificados, cuando la infraestructura está compuesta por un sistema DataPower.*

¿QUÉ ES EL PROTOCOLO TLS?

Secure Socket Layer (SSL) y Transport Layer Security (TLS) son protocolos criptográficos que garantizan el intercambio de datos a través de una red; por ejemplo, un cliente que se conecta a un servidor web. Al comienzo de una conexión TLS o SSL se realiza un **"handshake"** , durante este handshake **"apretón de manos"**, el cliente y el servidor determinarán qué algoritmos de cifrado mutuo y hash son compatibles. Aquí también es donde un servidor proporcionará su certificado digital a un cliente de conexión.

TLS es la siguiente generación del Certificado SSL. Nos referimos al TLS como la evolución del SSL dado que está basado en este último certificado y funciona de manera muy similar, básicamente: encripta la información compartida.

A lo largo de los años, las vulnerabilidades han sido y continúan siendo descubiertas en los protocolos SSL y TLS en desuso. Por esta razón, se debe desactivar SSLv2, SSLv3, TLS 1 .O y TLS 1 .1 en la configuración de su servidor, dejando habilitados únicamente los protocolos TLS 1.2 y 1.3.

¿CUÁLES SON LOS NAVEGADORES SOPORTADOS?

· Internet 11
· Edge:16
· Firefox: 58
· Chrome: 49

¿CÓMO ES EL PROCEDIMIENTO DE ACTUALIZACIÓN?

Para configurar **Internet Explorer versión 8** y posteriores, siga estos pasos:

1. En Internet Explorer, pulse Herramientas> Opciones de Internet.
2. En el cuadro de diálogo Opciones de Internet, pulse en la pestaña Avanzado.
3. Vaya a la sección Seguridad, seleccione la casilla de verificación Utilizar TLS 1 .2 y pulse aceptar.

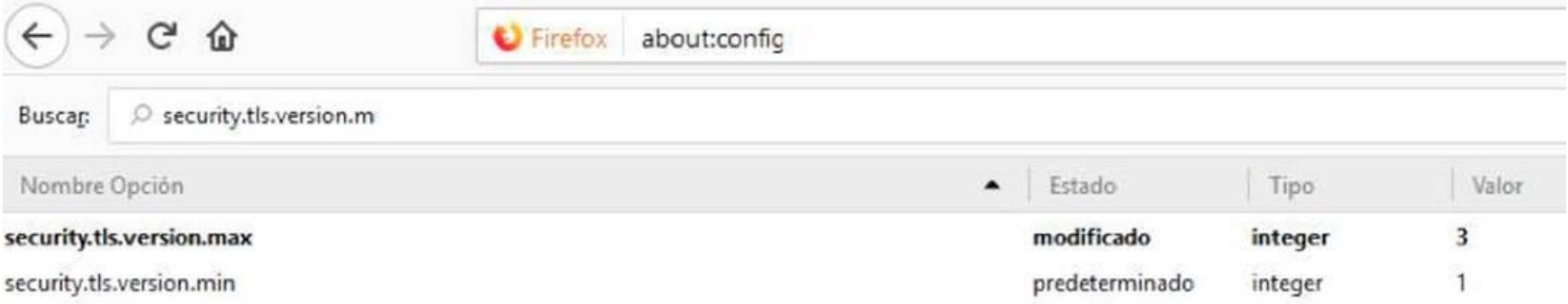
Para configurar **Firefox versión 24** y posterior, siga estos pasos:

1. Abra un navegador Firefox y escriba **about:config** en la barra de direcciones.

2. Cuando se le solicite, pulse ¡Tendré cuidado, lo prometo! y acepte el aviso

3. Busque **security.tls.version.max.**

4. Efectúe una doble pulsación en **security.tls.version.max** y cambie el valor por 3 configurar el navegador para dar soporte a TLS1 .2.



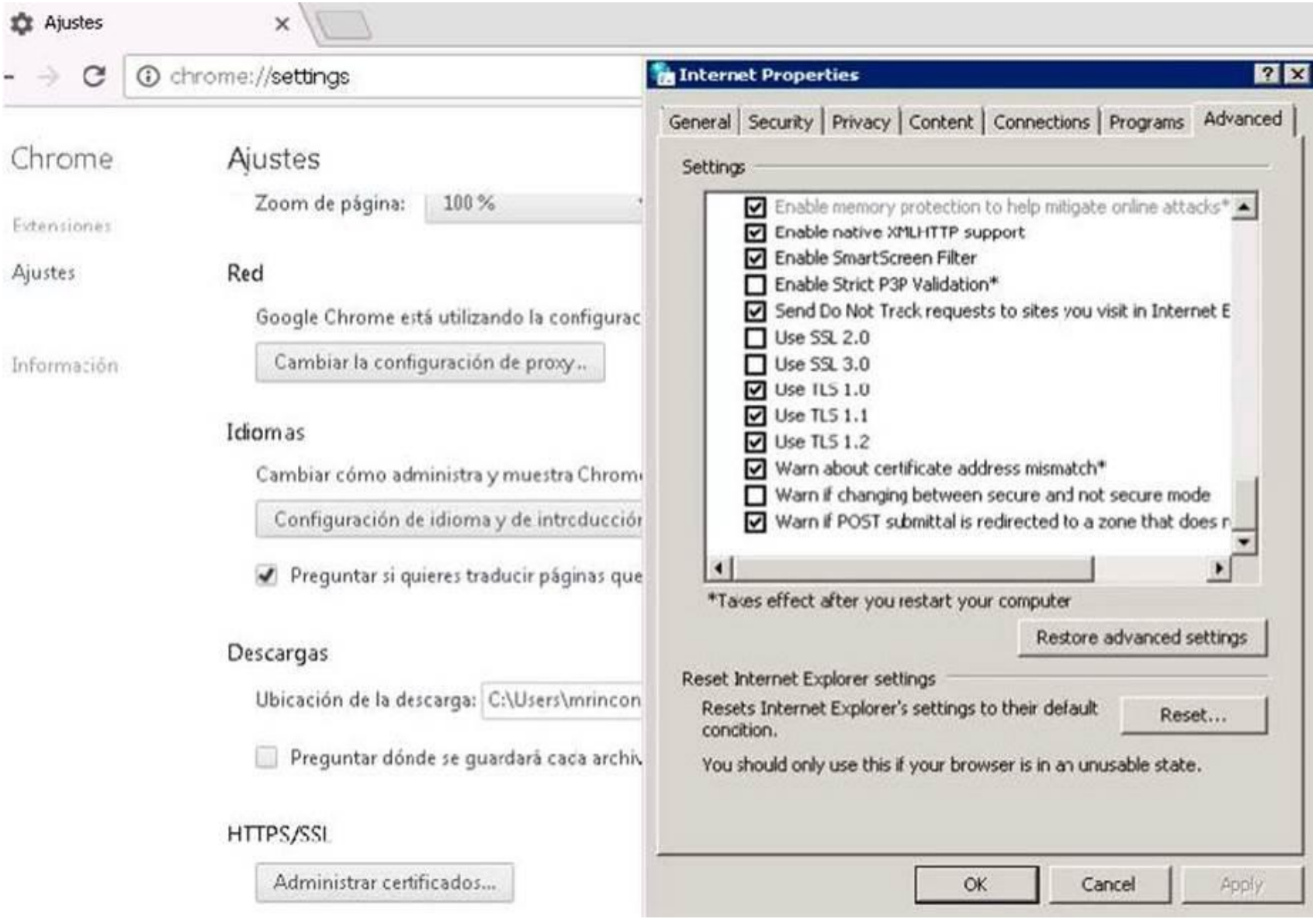
El valor 1 da soporte a: TLS1 .O.
El valor 2 da soporte a: TLS1 .O y TLS1 .1.
El valor 3 da soporte a: TLS1 .O, TLS1 .1 y TLS1 .2

PARA UN MAYOR ENTENDIMIENTO DE LOS VALORES QUE PODEMOS AGREGAR:

http://kb.mozillazine.org/Security.tls.version

PARA CONFIGURAR GOOGLE CHROME, SIGA ESTOS PASOS:

1. Abra un navegador Google Chrome
2. Presione Alt + F y seleccione configuración.
3. Selecciona Mostrar **configuración avanzada …**
4. Seleccione Red y haga click Sobre **Cambiar la configuración de proxy …**
5. Pulse en la pestaña Avanzado
6. Busque la sección **Security**, Seleccione la casilla de verificación Usar TLS 1.2.


Ajustes
chrome://settings
Chrome
Extensiones
Ajustes
Información
Ajustes
Zoom de página:
100 %
Red
Google Chrome está utilizando la configurac
Cambiar la configuración de proxy...
Idiomas
Cambiar cómo administra y muestra Chrom
Configuración de idioma y de introducción
Preguntar si quieres traducir páginas que
Descargas
Ubicación de la descarga:
C:\Users\mrincon
Preguntar dónde se guardará caca archiv
HTTPS/SSL
Administrar certificados...
Internet Properties
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Enable memory protection to help mitigate online attacks*
Enable native XMLHTTP support
Enable SmartScreen Filter
Enable Strict P3P Validation*
Send Do Not Track requests to sites you visit in Internet E
Use SSL 2.0
Use SSL 3.0
Use TLS 1.0
Use TLS 1.1
Use TLS 1.2
Warn about certificate address mismatch*
Warn if changing between secure and not secure mode
Warn if POST submittal is redirected to a zone that does n
*Takes effect after you restart your computer
Restore advanced settings
Reset Internet Explorer settings
Resets Internet Explorer's settings to their default condition.
Reset...
You should only use this if your browser is in an unusable state.
OK
Cancel
Apply

INFORMACIÓN GENERAL:

https://knowledge.digicert.com/generalinformation/INFO3299.html

Sistema operativo Soportados

Windows Server 2008 R2

1. Para habilitar el protocolo TLS 1.2 Inicie el editor de registro haciendo clic en Inicio y Ejecutar. Escriba **"regedit"** y presione la tecla enter.

2. Haga una copia de seguridad del registro primero haciendo clic en Archivo y luego en Exportar.

3. Busque la siguiente clave de registro:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

4. Haga clic con el botón derecho en la carpeta Protocolos y seleccione Nuevo "Key", esto creará una nueva carpeta.

5. Cambie el nombre de esta carpeta a TLS 1 .2.

6. Haga clic derecho en la clave TLS 1 .2 y agregue dos nuevas claves debajo de ella.

7. Cambie el nombre de las dos nuevas claves como:

- **A.** Cliente
- **B.** Servidor

8. Haga clic con el botón derecho en la clave del Cliente y seleccione Nuevo y luego Valor DWORD (32 bits) en la lista desplegable.

9. Cambie el nombre de DWORD a **DisabledByDefault.**

10. Haga clic con el botón derecho en el nombre **DisabledByDefault** y seleccione Modificar … en el menú desplegable.

11. Asegúrese de que el campo de datos de valor esté establecido en O y la Base sea **hexadecimal.** Haga clic en Aceptar.

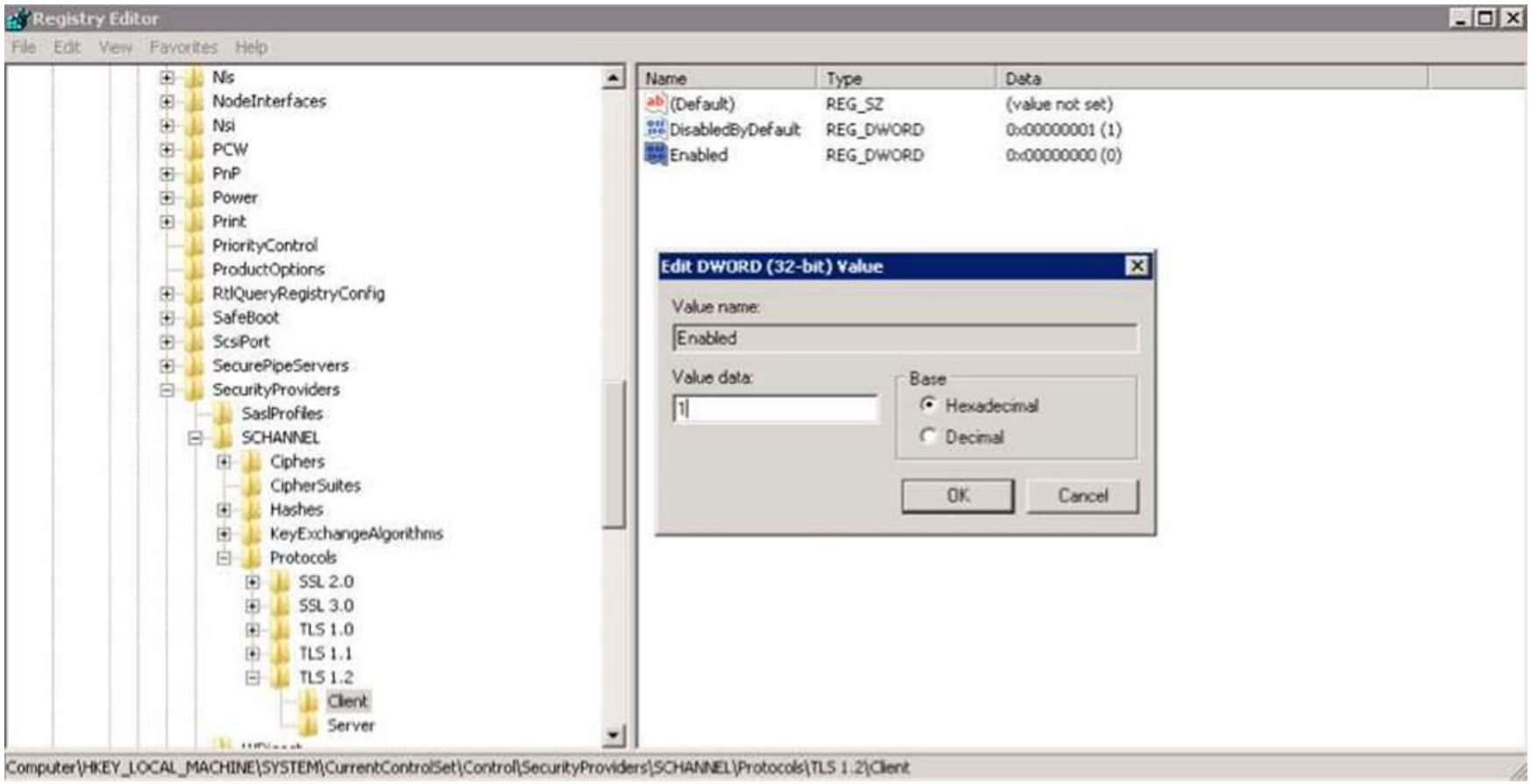
12. Cree otro DWORD para la clave del Cliente como lo hizo en el paso 8.

13. Cambie el nombre de este segundo DWORD a **Enabled.**

14. Haga clic con el botón derecho en el nombre Habilitado y seleccione Modificar … en el menú desplegable.

15. Asegúrese de que el campo de datos de valor esté establecido en 1 y la Base sea **hexadecimal.** Haga clic en Aceptar.

16. Repita los pasos 8 a 15 para la clave de Servidor (creando dos DWORD, **DisabledByDefault y Enabled,** y sus valores debajo de la tecla Servidor).



¿CUÁLES SON LOS PROTOCOLOS DE CIFRADO SOPORTADOS?

· TLS_ECDHE_ECDSA_WITH_AES_ 128_GCM_SHA256
· TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
· TLS_ECDHE_ECDSA_WITH_AES_ 128_CBC_SHA256
· TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
· TLS_ECDHE_RSA_WITH_AES_ 128_GCM_SHA256
· TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

· TLS_ECDHE_RSA_WITH_AES_ 128_CBC_SHA256
· TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
· TLS_DHE_RSA_WITH_AES_ 128_GCM_SHA256
· TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
· TLS_DHE_RSA_WITH_AES_ 128_CBC_SHA256
· TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

GUÍA DE VALIDACIÓN PARA LINUX RED HAT:

https ://access.redhat.comidocumentation/en-us/red_hat_enteprise_I in ux/7/htm 1/security_guide/sec-hardening_tls_configuration

OTRAS HERRAMIENTAS:

https://support.globalsign.com/customer/portal/articles/2356063

AVISOS LEGALES

· Este manual es una guía informativa que pretende orientar a los clientes de ACH Colombia que hacen uso de los productos y/o servicios prestados por la compañía.
· Antes de realizar cualquier cambio se debe evaluar con el área encargada todo el contenido y recomendaciones para desarrollar las actividades de acuerdo con sus necesidades.