



1. OBJETIVO

Este documento proporciona a los funcionarios de soporte técnico de las entidades que usan el aplicativo del Sistema de Presupuesto y Giro de Regalías (SPGR), las instrucciones que deben ejecutar al interior de las entidades, una vez sean aplicados los cambios anunciados por el Ministerio de Hacienda, con el objeto de habilitar el acceso al sistema SPGR.

Nota: Los cambios a aplicar se encuentra organizados de la siguiente manera:

Ver Numeral 3 SPGR

Ver Numeral 5 SPGR y Capacitación

2. DEFINICIONES

- **ESTACIÓN USUARIO SPGR**

Es el computador personal del usuario final desde la cual se conectan para acceder al aplicativo SPGR.

- **FIREWALL, PROXY Y TMG SERVER**

Son equipos de seguridad de la entidad que permiten controlar el flujo de datos en doble vía (entrada o salida) de acuerdo a unas políticas de control de acceso que permite o no la utilización de los servicios en redes públicas (internet) o privadas (WAN).

3. POLÍTICAS DE ACCESO SPGR

- En caso que la salida a Internet sea a través de un **Firewall** este debe realizar los siguientes cambios:

Para **portal.sgr.gov.co**

Actualizar la dirección Destino:

181.79.2.28, 181.79.2.16 190.60.101.218, 190.60.101.216, 23.100.19.33

Actualizar Puerto de Servicio: TCP 443 (https),



4. VERIFICACIÓN DE CONECTIVIDAD

Antes de iniciar la conexión de VPNSSL verifique los siguientes puntos:

No	Descripción	OK
Pruebas de Conectividad Básicas		
1	Ping a su propia dirección IP	
3	Ping a la dirección portal.sgr.gov.co	
4	Ping a la dirección IP 181.79.2.28	
Verificación en Firewall (en caso de tenerlo)		
5	Verifique que exista la regla la cual tenga: • SOURCE (Fuente): Grupo de clientes que se conectarán por VPNSSL • DESTINATION (Destino): salida a Internet o Direcciones válidas del Ministerio de Hacienda: 181.79.2.28, 181.79.2.16, 190.60.101.218, 190.60.101.216, 23.100.19.33 • SERVICE(Servicios): servicios creados TCP 443 https. • Registre logs para poder realizar el monitoreo	

5. POLÍTICAS DE ACCESO SPGR, CAPACITACIÓN

NOTA: CAPACITACION: solamente aplica para usuarios del aplicativo SPGR

- En caso que la salida a Internet sea a través de un **Firewall** este debe realizar los siguientes cambios:

Actualizar las direcciones destino:

181.79.2.28, 181.79.2.16 190.60.101.218, 190.60.101.216, 23.100.19.33

Actualizar Puerto de Servicio: TCP 443 (https)

6. VERIFICACIÓN DE CONECTIVIDAD

Antes de iniciar la conexión a la capacitación de SPGR verifique los siguientes puntos: <https://portal3.siifnacion.gov.co/capacitacionsgr>

No	Descripción	OK
Pruebas de Conectividad Básicas		
1	Ping a su propia dirección IP	
3	Ping a la dirección portal3.siifnacion.gov.co	
4	Ping a la dirección IP 181.79.2.16	
Verificación en Firewall (en caso de tenerlo)		
5	Verifique que exista la regla la cual tenga: • SOURCE (Fuente): Grupo de clientes que se conectarán • DESTINATION (Destino): salida a Internet o Direcciones válidas del Ministerio de Hacienda: 181.79.2.16. • SERVICE(Servicios): TCP443 • Registre logs para poder realizar el monitoreo	

7. ELIMINACIÓN DE DIRECCIONES Y RUTAS OBSOLETAS

Eliminar los siguientes objetos con direcciones IP Publicas que pertenecieron a direcciones SPGR anteriores, pero ya no son utilizados:

186.147.64.28	186.147.64.16	186.147.64.27
190.60.77.91	190.60.248.144	190.60.226.197
190.60.77.92	200.30.87.84	200.26.159.157
190.60.77.80	200.26.159.151	200.30.87.91
200.122.236.27	190.144.150.86	190.60.226.217