1. INTRODUCCIÓN

El manual que se presenta a continuación cuenta con la información necesaria para que una Entidad pueda obtener una configuración que le permita percibir un mejor desempeño del aplicativo SIIF Nación.

2. CONFIGURACIÓN PARA SIIF NACIÓN

La infraestructura informática cuenta con componentes que se encargan de la administración y seguridad de la información que viaja a través de las redes de comunicaciones. Cada componente realiza una tarea específica, donde requiere del análisis de la información, identificar que es perjudicial y que no lo es, para el desempeño del aplicativo. Sin embargo, este tipo de procesos de verificación de la información adicionan tiempos (Delays) que genera percepción de lentitud al usuario final. Por este motivo cada componente de seguridad como Firewall, Filtros de contenido Web, Servidores Proxy, Antivirus y aplicaciones propias del usuario, se recomienda la aplicación de excepciones y políticas que permiten el evitar este tipo de análisis y verificación, generando un mejor desempeño de los aplicativos. A continuación, se presenta las configuraciones recomendadas para implementar en cada componente de la infraestructura informática de la Entidad.

3. CONFIGURACIONES EN EL COMPUTADOR PERSONAL DEL USUARIO

Computador PC

- Leer el documento “SIIF - Instructivo Configuración Clientes” publicado en la Página de SIIF Nación en la pestaña “Aspectos Técnicos”, “Conectividad”

- Excepciones Proxy web:
  - https://portal2.siifnacion.gov.co
  - https://portal3.siifnacion.gov.co

- Antivirus actualizado no mayor a 15 días.
- Permiso de acceso para los protocolos TCP443
- Drivers de Token actualizado

Nota: Los requerimientos mínimos permiten trabajar con el aplicativo SIIF Nación, sin embargo, la experiencia con las Entidades ha demostrado que la configuración de Computador presentada permite una mejor experiencia de usuario.

4. NAVEGADOR

El sistema SIIF Nación es un aplicativo WEB y depende completamente de la calidad y desempeño del navegador por eso es importante contar con un navegador actualizado.

Ingresar la excepción del portal seguro (https://portal2.siifnacion.gov.co, https://portal3.siifnacion.gov.co en el navegador que utilice, el cual depende la topología implementada en la Entidad, es decir, si la Entidad utiliza Internet como canal principal para acceder al aplicativo SIIF Nación no es recomendable aplicar la excepción, de hacerlo el administrado de firewall perimetral deberá crear reglas de acceso para cada usuario o segmento, porque el usuario seria quien hace la petición y no el servidor proxy. Si la Entidad utiliza un canal diferente para conectarse al aplicativo SIIF Nación, si se recomienda la aplicación de la excepción.

Excepciones Proxy web: *.siifnacion.gov.co

5. CONFIGURACIONES EN SERVIDORES PROXY Y/O ISA

Como se explicó en las excepciones Proxy Web en el Navegador , ingresar la excepción del portal seguro (https://portal2.siifnacion.gov.co, y https://portal3.siifnacion.gov.co), depende la topología implementada en la Entidad, es decir, si la Entidad utiliza internet como canal principal para acceder al aplicativo SIIF Nación no es recomendable aplicar la excepción, de hacerlo el administrado de firewall perimetral deberá crear reglas de acceso para las direcciones de SIIF Nacion, porque el usuario seria quien hace la petición y no el servidor proxy. Si la Entidad utiliza un canal diferente para conectarse al aplicativo SIIF Nación, si se recomienda la aplicación de la excepción.

Recomendación: Aplicar las excepciones en su Servidor Proxy o ISA.
https://portal2.siifnacion.gov.co y https://portal3.siifnacion.gov.co (aplica para 2 canales de comunicación).

6. CONFIGURACIONES EN CONSOLAS DE ANTIVIRUS O FILTROS DE CONTENIDO

En la actualidad, los productos de antivirus empresariales proveen un servicio de análisis de contenido y la identificación de formas web defectuosas, es decir, si un usuario accede a una página web, esta es monitoreada con el fin de comprobar que el servicio web no se encuentre infectado de virus a través de una imagen, texto o cualquier programa engañoso para acceder al computador personal valiéndose de la ingenuidad del usuario y generar daños en la Entidad. Por eso cada antivirus implementa agentes centinelas alojados en el computador del usuario que analizan cada página web desconocida que el usuario accede. El análisis requiere completar en su totalidad la página web verificando el contenido (firma digital) y después presentárselo al usuario, durante este proceso pueden transcurrir entre 10 a 50 segundos, dependiendo del tamaño de la página Web, generando en el usuario una percepción de lentitud del aplicativo SIIF Nación. Por este motivo se recomienda en las consolas de los antivirus aplicar excepciones que permitan obviar esta verificación porque el aplicativo es completamente seguro.

Recomendación: Aplicar las excepciones en su Consola de Antivirus o Filtros de Contenidos https://portal2.siifnacion.gov.co y https://portal3.siifnacion.gov.co

7. CONFIGURACIONES EN FIREWALL PERIMETRAL

En los equipos de seguridad perimetral solo deben configurar los permisos para el acceso al aplicativo. Las recomendaciones de topología ideal se encuentran en el numeral 8. “Gráfico de Topología Ideal” de este documento.

Recomendación: Aplicar políticas de Acceso en el Firewall Perimetral

Nombre Dominio: portal2.siifnacion.gov.co
Direcciones IPs Destino: 186.147.64.27, 190.60.101.218, 23.100.19.33

Nombre Dominio: portal3.siifnacion.gov.co
Dirección Destino: 186.147.64.16, 190.60.101.216

Puerto de Servicio: TCP 443 (https)

8. GRÁFICO DE TOPOLOGÍA IDEAL

En este punto se presenta unas recomendaciones para implementar una topología ideal, que le va permitir a una Entidad mejorar el comportamiento de su infraestructura informática.

- **Nivel Seguridad Perimetral**

La prioridad del nivel de seguridad perimetral, es garantizar que el tráfico que proviene de las redes públicas (Internet) y algunas privadas como enlaces dedicados, WAN de regionales, entre otras, el cual busca acceder a los servicios que la Entidad administra, se realice de manera confiable y se eviten ataques de denegación de servicios y/o propagación de virus; además de aislar la red interna LAN de la Entidad. Por este motivo se sugiere que realice la reubicación de los servidores de acceso público como lo son portales, correo electrónico y redes externes, hasta el nivel perimetral a través de las interfaces DMZ, como se observa en la Figura No.1. Si solo se cuenta con una interface DMZ se debe verificar si la interface del firewall permite aplicar subinterfaces lógicas a través de una interface física, cada subinterfaz corresponde a un segmento de red físico y a un segmento lógico VLAN.

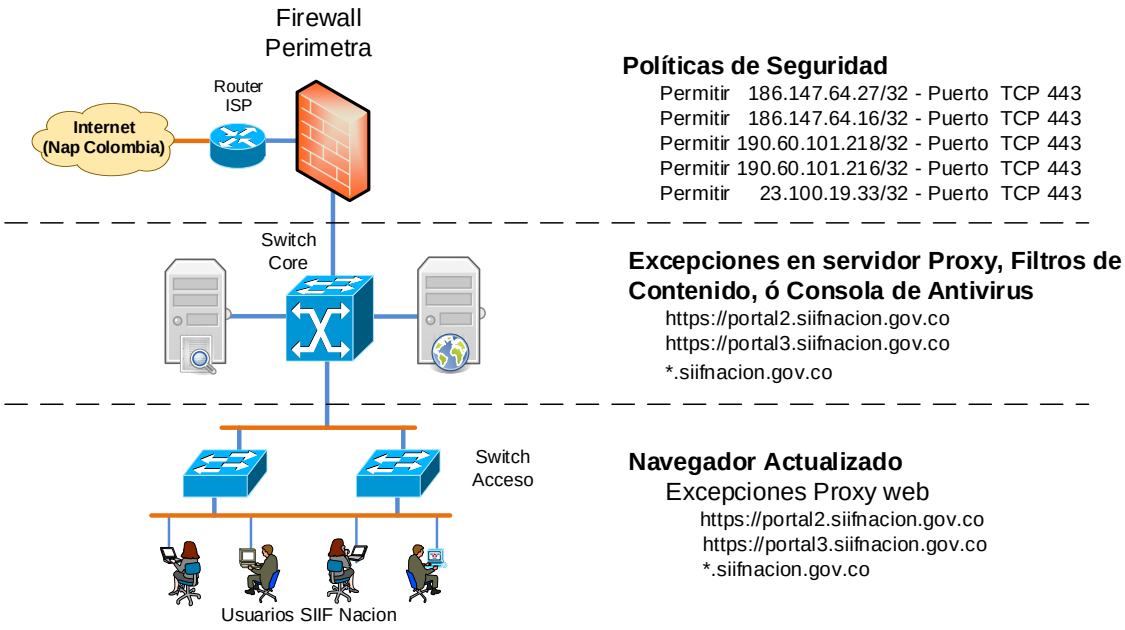

Figura No.1

- **Nivel Central de Comunicaciones**

A nivel CORE es importante aprovechar las bondades de enrutamiento, segmentación y control de acceso que tienen los equipos de comunicaciones de capa 3 para mejorar el desempeño de la infraestructura informática, por este motivo se recomienda todo el tráfico de la red interna LAN tenga puerta de enlace al Switch Core, para que determine su destino.

El servidor TMG (ISA) también debe tener como puerta de enlace al Switch Core, esto evitara que el tráfico de servicio http y https que son administrados por el TMG efectúen un salto hacia el nivel perimetral evitando la administración del Core, aunque la actual topología, a primera vista resulta fácil de implementar, a futuro impide el escalamiento de la plataforma informática.

- **Nivel de acceso de Comunicaciones**

Las redes actuales deben orientarse a servicios, para lograr un mejor desempeño de las mismas, por este motivo se sugiere rediseñar la segmentación física actual para buscar un grupo de segmentos orientados a servicios. Entre más pequeños sean los grupos mejorara el desempeño de la red y a su vez el control de tráfico, se agregan listas de control de acceso a nivel de CORE, para el tráfico entre usuarios.

9. CONFIGURACION DEL CORREO

El SIIF Nación envía los mensajes a través de un servicio SMTP que tiene como nombre de envío de correos: correo@siifnacion.gov.co, el cual las entidades deben configurarlo en la lista blanca de los servidores de la entidad.

Adicionalmente, las entidades deben configurar el servicio ANTISPAM para que no tengan restricción y/o evaluación que impida que el correo llegue a su destino.