Buenos Aires Ciudad

PROCURACION GENERAL

MANUAL DE PROCEDIMIENTO

Política de Seguridad de Redes de Información

1. Introducción

La presente política establece los criterios de seguridad necesarios para la gestión de redes que garanticen la confidencialidad, integridad y disponibilidad de la información en los usos requeridos por los agentes de la Procuración General.

2. Objetivo

Asegurar una adecuada protección de la información procesada en la red de datos de la Procuración General.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones de la Procuración General.

4.1 Contenido

4.1 Análisis de riesgo

La procuración General cuenta con una cantidad de equipos informáticos que resultan indispensables para la estabilidad del negocio, por lo tanto, es necesario establecer pautas a corto y largo plazo que garanticen tanto la continuidad como la rápida resolución de los problemas que puedan darse en cada uno de los componentes críticos, de esta manera se garantizara el orden y un mantenimiento eficaz.

4.2 Elementos a proteger

- Stack de Router
- Switch
- Enlace a la Red MAN
- Conectividad entre router y switch de los pisos (enlaces de fibra óptica)
- Conectividad de Switch de piso con puesto de trabajo (cableado horizontal)
- Racks protegidos por cerradura
- Condiciones Ambientales en Sala de Servidores
- Acciones ante cortes de luz en la Sala de Servidores.

Dentro de este conjunto de periféricos podemos encontrar múltiples complicaciones, estas pueden variar desde problemas de Hardware, Software, error en las configuraciones, etc.

Ante cada una de estas posibles causas existen algunos pasos que se deberán seguir para identificar rápidamente el conflicto y pasar a la resolución más adecuada para el mismo.

4.2.1 Stack de Routers:

El Stack de Routers, es el equipo con mayor importancia dentro de la estructura, en él se definen los parámetros de la red que luego replicaran en los diferentes Switch`s del edificio, por lo tanto, debe destacarse que de generarse una falla en este equipo la parálisis es completa en la totalidad del edificio.

El mismo se encuentra en la sala de servidores ubicada en el 1º piso del edificio, en un ambiente climatizado y con acceso limitado al personal autorizado mediante acceso con huellas digitales habilitadas para la apertura de las puertas.

Se cuenta con 2 equipos interconectados entre si formando un STACK, lo cual garantiza una continuidad de negocio ante la falla de algún equipo, administra y duplica el ancho de banda, permitiendo transacciones más rápidas y seguras a través de la red por la configuración de LACP.

Fallas posibles

01-Falta de suministro eléctrico (ver gráfico eléctrico)

02- Rotura general de router por falla que necesite su reposición

03- Rotura parcial de router por falla de configuración o puertos SFP

- **02 - <u>Rotura general de 1 router por falla que necesite su reposición:</u>**

El router interconecta el 100% de los Switch alojados en cada uno de los pisos de la Procuración General y a su vez nos brinda la conectividad con ASI y la salida hacia todos los servicios externos. La misma se realiza a través de sus puertos de fibra óptica (SFP), en el caso de una falla general automáticamente el Router dañado queda fuera de servicio y el Stack conformado seguirá brindando servicios, limitando su velocidad de transferencias hasta evaluar los daños y su posible reposición. -

- Si el equipo falla por un problema eléctrico propio o porque agoto su vida útil y no tiene reparación, el mismo debe ser reemplazado por un equipo de similares características.

- En caso de no tener un router de Backup se deberá comprar inmediatamente uno para su puesta en funcionamiento.

- Si contamos con un router como Backup o si ya adquirimos el mismo se procederá a la configuración* idéntica del router a reemplazar para garantizar la continuidad del negocio.

- El tiempo estimado de resolución dependerá de la disponibilidad de dinero en la Procuración General, de las limitaciones en el mercado para reponer el equipo dañado y la demora en entrega del proveedor al que se le adquiera dicho producto.

- Si ya contamos con el equipo (existente en procuración, se realizó la compra y respectiva entrega o fue provisto por ASI) se procederá a cargar la configuración actual y puesta en marcha.

*Dicho archivo de configuración es “procuracion.cfg” el cual se encuentra resguardado dentro de los procedimientos de Backup habituales. En caso de no poder ser importado el archivo mencionado, se deberá proceder a la configuración manual respetando los parámetros originales.

- **03 -<u>Rotura parcial de router por falla de configuración o puertos SFP:</u>**

Una rotura parcial puede significar que uno o más puertos SFP no brinden conectividad a uno o más Switch de piso. Limitando el acceso a los servicios en los sectores afectados por esta falla.

- En caso de detectarse un problema de conectividad nula a través del software de monitoreo se deberá constatar el origen del mismo, para esto en primer lugar se procederá al reemplazo del módulo SFP instalado para detectar si la falla se corresponde al módulo SFP o al puerto del Router.

- Si dicho módulo SFP resultara que se quemó o dejo de funcionar, se realizara el cambio del mismo para la reestablecer la conectividad de los servicios en los sectores afectados.

- Si la falla se desprende del mal funcionamiento del puerto del router, dicho módulo SFP se conectará en uno de los puertos disponibles contemplados para este tipo de fallas restableciendo así el servicio.

4.2.2 Switch`s:

Este equipo es el nodo que conecta mediante un tendido horizontal UTP los equipos de trabajo a la red LAN de la Procuración General, en él replican todas las configuraciones establecidas en el Router, como ser Vlan`s y reserva de IP`s por Mac Address y se conecta al router mediante fibra óptica.

Un mal funcionamiento de este equipo produce el corte parcial o total del piso donde se encuentre, por lo tanto, se debe tener especial atención a los siguientes posibles inconvenientes.

Fallas posibles

01 - Falta de suministro eléctrico (ver procedimiento aparte)

02 - Rotura general de Switch de piso por falla que necesite su reposición

03 - Rotura parcial de Switch de piso por falla de puerto SFP o RJ45

04 – Falla parcial de Switch por error en la configuración

02 -<u>Rotura general de Switch de piso por falla que necesite su reposición:</u>

Cada Switch interconecta aproximadamente el 50% del parque informáticos del piso donde está alojado, cada piso cuenta, en promedio, con 2 Switch’s de 48 puertos cada uno conectados entre sí.

Si un equipo falla por un problema eléctrico propio o porque agoto su vida útil y no tiene reparación, el mismo debe ser reemplazado por un equipo similar según características detalladas (***a**).

En caso de no tener un Switch de Backup se deberá comprar inmediatamente uno para su puesta en funcionamiento.

El tiempo estimado de resolución dependerá de la disponibilidad de dinero en la Procuración General, de las limitaciones en el mercado para reponer el equipo dañado y la demora de entrega del proveedor al que se le adquiera dicho producto.

Si contamos con un Switch como Backup (existente en procuración o se realizó la compra y respectiva entrega) se procederá a la configuración idéntica del equipo dañado para garantizar la continuidad del negocio (***b**).

***a** - **<u>Características de Switch</u>**: Layer 2, administrable, 48 puertos más 2 puertos SFP Con sus correspondientes módulos y compatible con Vlan`s como características indispensables.

***b** - **<u>Configuración del Switch:</u>** Para la correcta configuración del mismo se lo accederá por consola, se le fijará la dirección IP correspondiente y mediante la documentación existente de cada Switch se procederá a la configuración general del mismo. A continuación, se establecerán las Vlan que contenía el equipo dañado respetando el relevamiento* de red actual para garantizar que todo funcione correctamente.

Ejemplo de relevamiento de Vlan´s en Switch:

Nº BOCA	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	49	51
SWITCH:																										
BOCA PATC:	PROXY*	D1-02	D1-03*	D1-04	D1-05	D1-06*	T1-41	D1-07	T1-07	D1-10	D1-11*	D1-12*	D1-13	T1-32	PC-DC1	T1-37	D1-26	D1-18	D1-19	D1-20	D1-21	D1-22*	D1-63	T1-28		LINK*
VLAN ID:	604	628	628	628	628	628	628	628	628	628	628	612	628	628	604	628	628	628	628	628	628	628	604	628	1	1
OFICINA:	12	12	12	13	12	12	13	13	13	14	14	14	15	14	14	17	17	13	17	17	17	18	14	18		
PISO:	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º	1º
* PROXY REVERSO			D1-03*: SW NOGANET (3 Pc's)					D1-11*: SW TP-LINK (3 Pc's)					D1-22*: SW ENCORE (4 Pc's)						*LINK DEL SW 3COM 4210 POR F.O. (PORT 52)							
			D1-06*: SW ENCORE (5 Pc's)					D1-12*: ENCORE (5 Pc's)																		

02 -<u>Rotura parcial de Switch de piso por falla puerto SFP o RJ45</u>

Una rotura parcial puede significar que uno o más puertos no brinden conectividad o que todo el Switch no nos permita acceder a los servicios, información y aplicaciones.

En caso de detectarse una falla en uno o más puertos RJ45 se procederá a realizar las tareas de testing correspondientes, verificando la conectividad del mismo, que su patchcord este bien conectado y en condiciones óptimas de funcionamiento. Si todo se encuentra dentro de los parámetros establecidos continuaremos reconectando dicha boca de red en otro puerto

del Switch para verificar finalmente si el puerto que falla dejo de funcionar definitivamente.

Si todo el Switch no nos está permitiendo acceder a los servicios se revisará la conexión a través de los puertos de fibra óptica (SFP) el correcto funcionamiento y configuración.

En caso de estar fallando el módulo SFP se realizará el cambio del mismo y se volverá a conectar todos los servicios de red.

04 – Falla parcial de Switch por error en la configuración:

Una falla en la configuración del Switch provoca que uno o más puertos del mismo dejen de funcionar o nos brinden servicios limitados o no nos permita acceder a ciertos aplicaciones o periféricos como ser impresoras de red.

- En caso de tratarse de uno o más puertos RJ45 se procederá a realizar la revisión pertinente acerca de si mantienen su configuración original y en la Vlan correspondiente según relevamiento de redes existente, accediéndolo de forma Web o por medio de la consola. En caso de detectar alguna anomalía se procederá a su corrección.

4.2.3 Enlace a la Red MAN

El enlace con la Red MAN significa el medio de conexión que tiene la Procuración General con la red del área metropolitana, osea el acceso a toda aplicación externa a la Procuración General (Correo electrónico oficial, Acceso a Internet, Intranet, Escritorio Único, etc.)

Esta conectividad y su respectiva seguridad y monitores es compartido con ASI (Agencia de Sistemas de Información)

Fallas posibles:

01 – Error en el ruteo saliente de la procuración hacia la MAN

02 – Imposibilidad de acceso a servicios externo

01 – Error en el ruteo saliente de la procuración hacia la MAN

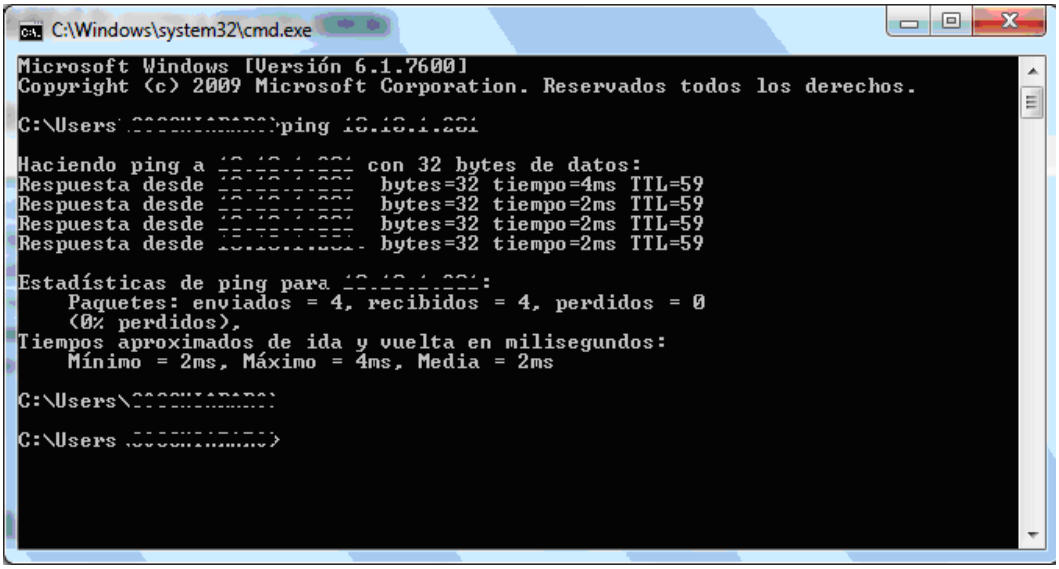
Para que el ingreso a las aplicaciones externas, como ser el escritorio único (paquete de aplicaciones como Gedo, Comunicaciones Oficiales, etc.) funcione correctamente una de las cosas importantes a tener en cuenta son las rutas que nos apuntan directamente a los servidores donde se encuentran alojados dichas aplicaciones, estas rutas están especificadas en los equipos que nos interconectan con la red MAN (Equipos externos controlados por la ASI).

Si nos encontramos con alguna imposibilidad para el ingreso a dichas aplicaciones (no así para navegar por Internet) es necesario revisar que nuestro enlace este correctamente apuntado, para esto se debe realizar una traza completa que nos ayude a verificar los saltos correctos hacia los servidores, para esto debemos ingresar en una ventana de DOS y realizar un tracert como se muestra en la siguiente imagen.

En este caso vemos como la traza se realizó correctamente, pero si nos encontramos que en el punto 7 estamos llegando a otra dirección (o la traza termina incompleta) estamos ante un problema en la configuración de los equipos de la ASI el cual se debe informar para la resolución del mismo ya que no disponemos de acceso a dichas configuraciones.

02 – <u>Imposibilidad de acceso a servicios externos</u>

Al detectarse este tipo de falla ya sea por software de monitoreo o reclamo de otra repartición, éste departamento realizara las tareas de revisión necesaria para detectar el motivo de la falla. Al tener un control en conjunto con ASI nuestra tarea se verá limitada pudiendo verificar el estado de suministro eléctrico correspondiente al rack de **“ASI”**, si todo está en condiciones normales, se realizará la verificación mediante un **“ping”**desde una ventana de **“DOS”** hacia el **“DEFAULT”** que dispone **ASI** para realizar dicha comprobación (10.xx.xx.xx) como se muestra a continuación.



Si el informe es como el de la imagen anterior (respuesta desde 10.xx.xx.xx: bytes =32 tiempo=ms TTL=xx) eso significa que el enlace con la red MAN funciona correctamente y el problema solamente lo tiene el servicio al cual estamos queriendo acceder (Correo, Internet, Escritorio Único, etc.).

En caso de que la respuesta del informe varíe a la imagen y sea: **“Tiempo de espera agotado para esta solicitud” o “destino de host inaccesible”** ahí si estamos teniendo problemas con el enlace hacia la red MAN ***(previa revisión de Router y su funcionamiento incluido en esta guía)***

A esta altura del problema, nosotros como departamento informático de la Procuración General, ya no contamos con el poder de realizar otro tipo de pruebas o monitoreo, por lo tanto, debemos reportar dicha falla a la Gerencia Operativa de Redes de la Dirección General de Infraestructura correspondiente a la Agencia de Sistemas de Información, sito en Av. Independencia Nº 635 Piso 4º, teléfono 4323-9300 Int. 1437.

4.2.4 Conectividad entre Router y Switch de los pisos:

La interconexión entre los Routers (STACK) desde la sala de Servidores hacia los diferentes Switch´s (STACK) instalados en cada piso de la Procuración General es realizada mediante un cableado de fibra óptica, compuesto por 2 (dos) pares de cables de iguales características para cada uno de los pisos, lo que nos brinda redundancia hacia el STACK, en caso de detectarse una falla en la conexión **primaria**, garantizando así la continuidad de las labores diarias.

El tendido de la misma esta realizado por la montante del edificio

Fallas posibles:

01 - Daño en la patchera de fibra óptica

02 - Corte parcial del tendido de fibra óptica

03 - Corte total del tendido de fibra óptica

01 - Daño en la patchera de fibra óptica:

El daño de uno o más puertos en la patchera de fibra óptica puede producirse por un error humano o de manipulación al realizar algún tipo de trabajo o mantenimiento sobre la misma. Esto producirá que el/los puertos involucrados no permitan la comunicación entre el router y el/los pisos afectados.

- En caso de producirse dicho daño se deberá identificar el/los puertos dañados para reparar dicha conexión y reestablecer el servicio.

02 - <u>Corte parcial del tendido de fibra óptica:</u>

El corte Parcial de la fibra óptica puede producirse por un error humano o de manipulación al realizar algún tipo de trabajo o mantenimiento en el sitio por donde está realizado el tendido. Al detectarse este tipo de falla sobre la fibra óptica Master, se mantendrá la conexión Slave para poder continuar con las tareas del personal de la Procuración General.

Una vez detectada la falla se deberá contemplar la realización de un tendido nuevo de fibra óptica para reemplazar la dañada desde el router del 1º piso al sector afectado.

03 - <u>Corte total del tendido de fibra óptica:</u>

El corte total del tendido de interconexión por medio de fibra óptica significa una pérdida total de comunicación de los diferentes sectores de la Procuración General.

Las causas pueden deberse a fenómenos naturales o a una imprudencia humana.

Ante este tipo de fallas necesitaremos realizar alguna de las siguientes tareas según la disponibilidad de recursos con la que contemos al momento de la falla.

- **Opción A: Realizar un nuevo tendido de fibra óptica:**

El tiempo de un tendido nuevo de ambas fibras varía según disponibilidad de dinero para la adquisición de materiales, contratación de empresa de forma directa o licitación y disponibilidad de la misma para realizar el trabajo.

- **Opción B: Realizar un tendido provisorio UTP cat.5e:**

El restablecimiento a través de cableado UTP cat. 6e dependerá de la existencia de materiales o dinero para su adquisición como así también de la disponibilidad de la empresa a realizar el trabajo Empresa contratada o ASI)

- **Plan C: Último recurso:**

En caso de no poder solucionarlo por los puntos anteriormente mencionados se procederá a cascadear los Switch sin conectividad desde el piso más cercano a través de cable UTP cat. 6e de forma provisoria hasta tanto pueda darse la solución planteada en Plan A.

4.2.5 Conectividad de Switch de piso con puesto de trabajo (cableado horizontal)

La conectividad entre los equipos informáticos de cada piso (PC, Impresoras de red, Teléfonos IP, etc.) está compuesta por un cableado horizontal UTP cat. 6e debidamente canalizado e identificado en cada una de las oficinas como así también en el rack correspondiente donde la patchera se conecta al Switch de piso.

Fallas posibles:

01 - Daño en la patchera de RJ45

02 - Daño parcial del tendido de UTP cat.6

03 - Daño total del tendido de UTP cat.6

01 - Daño en la patchera de RJ45

Los daños en una patchera no son algo frecuente y generalmente cuando sucede se debe a un problema de manipulación por parte del personal. Dicho daño se desprende de algún trabajo que se pueda estar realizando en el lugar y por medio de manipulación podría desconectarse alguno de los cables existentes, generando la falta de servicio de un equipo informático. En caso de que suceda se proceder a la reconexión de dicho conector reestableciendo el servicio. -

02 - Dañoparcial del tendido de UTP cat.6:

El tendido horizontal de UTP cat.6 se encuentra canalizado e identificado en las oficinas como así también en su correspondiente patchera. Este puede sufrir un deterioro parcial debido a la ubicación física del mismo, ya que pueden producirse roturas por manipulación de muebles, mudanzas y factores de error o impericia humana, en caso de que esto suceda se relevara el daño ocasionado y su posible reparación o reemplazo. Si se produce una rotura de uno o más cables se deberá identificar a los mismos para poder ser reemplazados, mientras se evalúan los tipos y formas de reemplazo, se reacomodará el equipo informático (PC, Impresora o

Teléfono IP) a una nueva boca de red del área garantizando la continuidad de sus tareas, previa reconfiguración de su nuevo puerto de conexión en la Vlan correspondiente en el Switch de piso.

03 - <u>Daño total del tendido de UTP cat.6:</u>

El daño total en el cableado horizontal de un piso es de muy baja probabilidad ya que el mismo se encuentra completo desde el rack correspondiente, pero en su trayecto se va distribuyendo a las diferentes oficinas del piso, por lo tanto, que haya un corte total es improbable.

4.2.6 <u>Racks</u>

Los Racks ubicados tanto en los pisos de la Procuración General como dentro de la sala de Servidores nos sirven para mantener en condiciones de orden y seguridad todo el equipamiento informático (patchera, Switch’s, servidores, etc.). Dichos Racks cuentan con una cerradura en la puerta frontal lo cual nos permite restringir el acceso de toda persona ajena al sector, a los elementos que se encuentran en él, cabe destacar que las llaves de dichas cerraduras deben estar en poder de este departamento correctamente identificadas.

ANEXOS

Configuracion switch Actuales

ALLIED TELESIS AT-8000S Series

Acceso por consola y Web:

- Se accede al Switch mediante la consola, (115200)una vez colocado el usuario y password se procede a designarle una dirección **IP** fija para poder administrarlo y accederlo de forma **WEB**.

- La asignación de **IP** por consola se realiza de la siguiente manera.

User Name: manager

Password:******

console# configure

console(config)# interface vlan 1

console(config-if)# ip address 10.60.1.xx 255.255.252.0

console(config-if)# exit

console(config)# ip default-gateway 10.60.1.2

console(config)#exit

console# exit

- Una vez fijada la dirección **IP** ingresamos a la interface **WEB** para su configuración con el mismo usuario y contraseña que accedimos por consola.

NOTA: Configuraciones por consola…

- **Rango de puertos a XXX Vlan**

  console#configure

  console(config)#interface range Ethernet e1-48

  console(config-if)#switchport access vlan XXX

- **Crear una Vlan**

  console# configure

  console(config)# vlandatabase

  console(config-vlan)#vlan XXX

  console(config-vlan)#exiT

  console(config)# exit

  console# show vlan

- **Borrarunavlan**

  console# configure

  console(config)# vlan database

  console(config-vlan)# no vlan XXX

  console(config-vlan)# exit

console(config)# exit

console# show vlan

- **Verconfiguracion y version**

  console# show running-config

  console# show version

- **Configurar nombre de SW (hostname)**

  console# configure

  console(config)# hostname Piso_1_1

  Piso_1_1(config)#

- **Configuracion Stack: al enchufar un SW apretar enter y entrar al menú, seguir los pasos:**

  Stack ID (1y 2 master) (3 a 6 slave)

  Mode (standalone o stacking)

  Desarmar stacking (ID =0) Mode: standalone

- **Reiniciar switch por putty:**

  Primero dar save por web para guardar cambios

  #RELOAD

NOTA: Antes de continuar con la configuración, salvar los cambios, de lo contrario necesitaremos realizar los pasos marcados en el punto 1 nuevamente.

ConfiguracionRouters Actuales

Router:

```
!
service password-encryption
!
hostname router-PG
!
no banner motd
!
username manager privilege 15 password 8
$1$bJo4US4D$vT/0IdtbFYW609exb4bPS/
!
log host 10.200.7.9
log host 10.60.14.230
!
no service ssh
!
service telnet
!
service http
!
clocktimezoneutc minus 3:00
!
snmp-server
snmp-server contact Eduardo/Emiliano Tel:7573
snmp-server location Uruguay 400 - Procuracion - 1er Piso Of. 3
snmp-server enabletrapauth
snmp-server community procura.*123 rw
```

```
snmp-server community solar
snmp-server community public
snmp-server community proc-uru.*440 rw
snmp-server host 10.60.13.103 proc-uru.*440
snmp-server host 10.60.15.210 proc-uru.*440
snmp-server host 10.60.6.10 proc-uru.*440
snmp-server host 10.60.14.230 proc-uru.*440
snmp-server host 10.200.7.10 proc-uru.*440
snmp-server host 10.200.7.202 proc-uru.*440
snmp-server host 10.200.7.21 proc-uru.*440
snmp-server host 10.200.7.199 proc-uru.*440
snmp-server host 10.200.7.71 proc-uru.*440
snmp-server host 10.200.7.200 proc-uru.*440
snmp-server host 10.200.7.77 proc-uru.*440
snmp-server host 10.200.7.25 procura.*123
snmp-server host 10.60.14.230 procura.*123
snmp-server host 10.60.15.210 procura.*123
snmp-server host 10.200.7.97 procura.*123
snmp-server host 10.200.7.77 procura.*123
snmp-server host 10.200.7.207 procura.*123
snmp-server host 10.60.6.10 procura.*123
snmp-server host 10.60.13.5 solar
snmp-server host 10.60.15.220 solar
snmp-server host 10.60.13.103 public
!
!
aaa authentication enable default local
aaa authentication login default local
!
!
ntp peer 10.10.1.102
!
ip name-server 10.60.6.10
ip name-server 10.10.1.180
ipdomain-lookup
!
ipdhcp pool Planta-Baja
```

```
network 10.60.68.0 255.255.252.0
range 10.60.69.51 10.60.69.251
range 10.60.71.1 10.60.71.254
dns-server 10.60.6.10
default-router 10.60.68.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
ipdhcp pool Piso-1
network 10.60.76.0 255.255.252.0
range 10.60.77.51 10.60.77.251
range 10.60.79.1 10.60.79.254
dns-server 10.60.6.10
default-router 10.60.76.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
ipdhcp pool Piso-2
network 10.60.28.0 255.255.252.0
range 10.60.29.51 10.60.29.251
range 10.60.31.1 10.60.31.254
host 10.60.29.65 000c.2971.39f5
dns-server 10.60.6.10
default-router 10.60.28.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
ipdhcp pool Piso-3
network 10.60.20.0 255.255.252.0
range 10.60.21.51 10.60.21.251
range 10.60.23.1 10.60.23.254
host 10.60.21.34 0008.54a9.3c8d
dns-server 10.60.6.10
default-router 10.60.20.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
```

```
ipdhcp pool Piso-4
network 10.60.60.0 255.255.252.0
range 10.60.61.51 10.60.61.251
range 10.60.63.1 10.60.63.254
dns-server 10.60.6.10
default-router 10.60.60.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
ipdhcp pool Piso-5
network 10.60.36.0 255.255.252.0
range 10.60.37.51 10.60.37.251
range 10.60.39.1 10.60.39.254
dns-server 10.60.6.10
default-router 10.60.36.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
ipdhcp pool Piso-6
network 10.60.52.0 255.255.252.0
range 10.60.53.51 10.60.53.251
range 10.60.55.1 10.60.55.254
dns-server 10.60.6.10
default-router 10.60.52.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
ipdhcp pool Piso-7
network 10.60.84.0 255.255.252.0
range 10.60.85.51 10.60.85.251
range 10.60.87.1 10.60.87.254
dns-server 10.60.6.10
default-router 10.60.84.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
```

```
ipdhcp pool Piso-8
network 10.60.92.0 255.255.252.0
range 10.60.93.51 10.60.93.251
range 10.60.95.1 10.60.95.254
dns-server 10.60.6.10
default-router 10.60.92.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
ipdhcp pool Piso-9
network 10.60.100.0 255.255.252.0
range 10.60.101.51 10.60.101.251
range 10.60.103.1 10.60.103.254
dns-server 10.60.6.10
default-router 10.60.100.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
ipdhcp pool Telefonia
network 10.60.44.0 255.255.252.0
range 10.60.45.1 10.60.45.254
range 10.60.47.1 10.60.47.254
host 10.60.45.250 000e.aa00.818a
host 10.60.45.251 0018.2701.95b3
host 10.60.45.252 0090.8f8b.70e4
host 10.60.45.253 6cf0.4985.30f6
dns-server 10.60.6.10
default-router 10.60.44.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
ipdhcp pool Informatica
network 10.60.12.0 255.255.252.0
range 10.60.13.1 10.60.13.254
range 10.60.15.1 10.60.15.254
host 10.60.13.13 6cf0.4985.2f98
```

```
host 10.60.13.134 6cae.8b51.6c35
host 10.60.13.169 50e5.4989.e005
host 10.60.13.216 7427.ea04.2860
host 10.60.15.96 001b.a943.4b12
host 10.60.15.201 f44d.30aa.d09c
host 10.60.15.202 0000.aad8.1fe0
host 10.60.15.212 902b.34d5.a09a
host 10.60.15.213 902b.34d6.6934
host 10.60.15.215 bc5f.f4c4.2aaa
host 10.60.15.216 6cf0.49a7.df96
host 10.60.15.220 1c1b.0da1.55f7
dns-server 10.60.6.10
default-router 10.60.12.2
lease 90 0 0
domain-name pg.gcba.gov.ar
!
!
!
servicedhcp-server
!
noip multicast-routing
!
location civic-location identifier 1
country AR
city CABA
house-number 440
floor 1
room 3
primary-road-name Uruguay
!
spanning-tree mode rstp
spanning-tree priority 16384
!
service power-inline
nolacp global-passive-mode enable
!
```

```
vlandatabase
vlan 600 name Monitoreo
vlan 604 nameGservidores
vlan 612 nameInformatica
vlan 620 name Piso-3
vlan 628 name Piso-2
vlan 636 name Piso-5
vlan 644 nameTelefonia
vlan 652 name Piso-6
vlan 660 name Piso-4
vlan 668 name Planta-Baja
vlan 676 name Piso-1
vlan 684 name Piso-7
vlan 692 name Piso-8
vlan 700 name Piso-9
vlan 1000 name Provisorio
vlan 1060 name managment
vlan 600,604,612,620,628,636,644,652,660,668,676,684,692,700,1000,1060
state enable
!
interface port1.0.1-1.0.26
switchport
switchportmodeaccess
!
interface port2.0.1-2.0.26
switchport
switchport mode access
!
interface port3.0.1-3.0.26
switchport
switchport mode access
!
interface vlan600
ip address 10.60.1.2/22
!
interface vlan604
```

```
ip address 10.60.4.2/22
!
interface vlan612
ip address 10.60.12.2/22
!
interface vlan620
ip address 10.60.20.2/22
!
interface vlan628
ip address 10.60.28.2/22
!
interface vlan636
ip address 10.60.36.2/22
!
interface vlan644
ip address 10.60.44.2/22
!
interface vlan652
ip address 10.60.52.2/22
!
interface vlan660
ip address 10.60.60.2/22
!
interface vlan668
ip address 10.60.68.2/22
!
interface vlan676
ip address 10.60.76.2/22
!
interface vlan684
ip address 10.60.84.2/22
!
interface vlan692
ip address 10.60.92.2/22
!
interface vlan700
```

```
ip address 10.60.100.2/22
!
interface vlan1000
ip address 10.200.61.4/24
!
interface vlan1060
ip address 10.60.254.4/24
!
ip route 0.0.0.0/0 10.60.254.2
ip route 192.168.206.123/32 10.60.5.10
!
ipdns forwarding
!
line con 0
linevty 0 4
!
end
```

Switch

```
Piso_1# show running-config

interfaceethernet 1/g2
port storm-control include-multicast
exit

no spanning-tree
interface port-channel 1
switchport mode trunk
```

```
exit

interface range ethernet 1/g(1-2)
switchport mode trunk
exit

vlan database
vlan 600,604,612,620,644,676
exit

interfaceethernet 1/g2
switchport trunk allowed vlan add 600
exit

interface range ethernet 2/g2,3/g(1-2),4/e(13-15)
switchport access vlan 604
exit

interfaceethernet 1/g2
switchport trunk allowed vlan add 604
exit

interface port-channel 1
switchport trunk allowed vlan add 604
exit

interface range ethernet 1/e31,2/e(3,9,11,18-19,21-22,25,35,45,47-48),3/e(47-
48),4/e22
switchport access vlan 612
exit

interfaceethernet 1/g2
switchport trunk allowed vlan add 612
exit

interface port-channel 1
switchport trunk allowed vlan add 612
```

```
exit

interfaceethernet 2/e46
switchport access vlan 620
exit

interfaceethernet 1/g2
switchport trunk allowed vlan add 620
exit

interface port-channel 1
switchport trunk allowed vlan add 620
exit

interface range ethernet 1/e6,4/e(1-8)
switchport access vlan 644
exit

interfaceethernet 1/g2
switchport trunk allowed vlan add 644
exit

interface port-channel 1
switchport trunk allowed vlan add 644
exit

interface range ethernet 1/e(1-5,7-30,32-48),2/e(1-2,4-8,10,12-17,20,23-
24,26-34,36-44),3/e(1-24),4/e(10,12,16-21)
switchport access vlan 676
exit

interfaceethernet 1/g2
switchport trunk allowed vlan add 676
exit

interface port-channel 1
switchport trunk allowed vlan add 676
```

```
exit

interfacevlan 600
nameMonitoreo
exit

interfacevlan 604
nameGservidores
exit

interfacevlan 612
nameInformatica
exit

interfacevlan 620
nameDGAJur
exit

interfacevlan 644
nameTelefonia
exit

interfacevlan 676
name "Piso 1"
exit

interface range ethernet 1/g1,2/g1,4/g1
channel-group 1 mode auto
exit

interfacevlan 1
ip address 10.60.1.11 255.255.252.0
exit

ip default-gateway 10.60.1.2
hostname Piso_1
```

username admin password d0063fc438866fa1f14b646f43a8b641 level 15 encrypted
snmp-server community procuracion-asiro view Default

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S
"2022 - Año del 40° Aniversario de la Guerra de Malvinas. En homenaje a los veteranos y caídos en la defensa de las Islas Malvinas y el Atlántico Sur"

Hoja Adicional de Firmas
Anexo

Número: IF-2022-22348746-GCABA-DGTALPG

Buenos Aires, Martes 21 de Junio de 2022

Referencia: Anexo II. Manual de Procedimiento sobre Política de Seguridad de Redes de Información.

El documento fue importado por el sistema GEDO con un total de 35 pagina/s.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2022.06.21 12:40:18 -03'00'

JUAN MANUEL GALLO
Director General
D.G. TECNICA ADMINISTRATIVA Y LEGAL
PROCURACION GENERAL

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2022.06.21 12:40:18 -03'00'