Guía de Acceso y Servicios de Red

Capital

Julio del 2021

Tabla de Contenido

1 Introducción

"Los equipos suelen formar parte de una red de equipos. Una red permite que los equipos conectados intercambien información. Los equipos conectados a la red pueden acceder a datos y demás recursos de otros equipos de la red. Las redes de equipos crean un entorno informático potente y sofisticado. Sin embargo, las redes complican la seguridad de los equipos. Por ejemplo, dentro de una red de equipos, los sistemas individuales permiten el uso compartido de información. El acceso no autorizado es un riesgo de seguridad, debido a que muchas personas tienen acceso a una red, el acceso no autorizado es más probable, especialmente como consecuencia de errores del usuario. Un mal uso de contraseñas también puede originar el acceso no autorizado."

2 Objetivo

Otorgar el derecho a un servicio a usuarios autorizados, mientras se previene el acceso de usuarios no autorizados. Los procesos de Gestión del Acceso ponen en práctica las políticas definidas por la Gestión de Seguridad de TI. La Gestión del Acceso también es conocida como Gestión de Derechos o Gestión de Identidad.

3 Alcance

Aplica para todos los colaboradores, contratista y terceros de Capital, proveedores y terceros, que sean autorizados a utilizar los servicios de red de la entidad.

4 Gestión de la Seguridad de las Redes

4.1 Controles de Red

- **FIREWALL**: también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red. Si este tráfico cumple con las reglas previamente especificadas podrá acceder y salir de nuestra red, si no las cumple este tráfico es bloqueado.

  De esta manera impedimos que usuarios no autorizados accedan a nuestras redes privadas conectadas a internet, Se puede implementar en forma de hardware, de software o en una combinación de ambos.

- **AD DS (GPO):** es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.

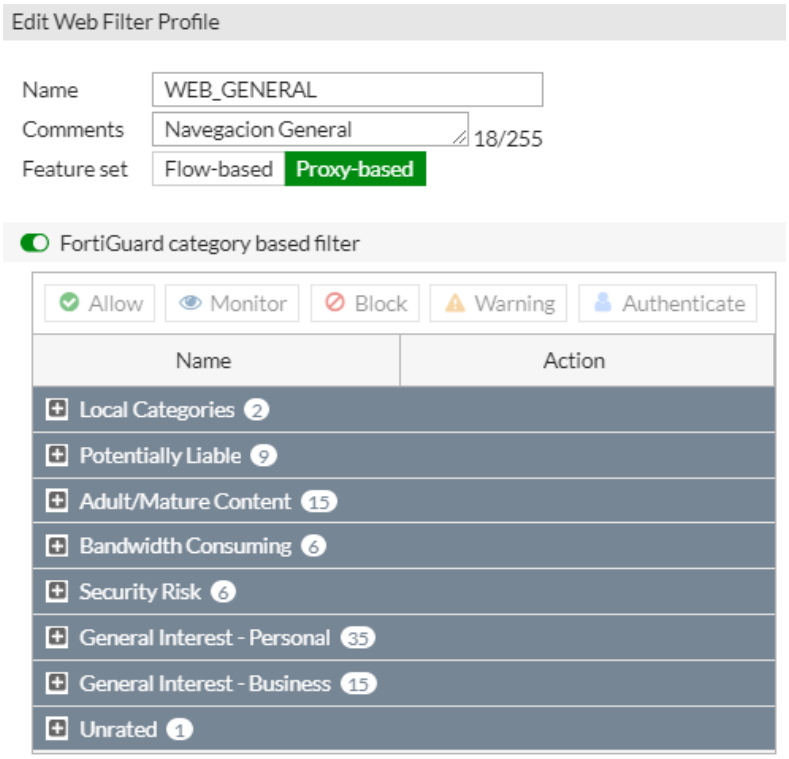
- **VLAN:** es un método para crear redes lógicas independientes dentro de una misma red física. 1 Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local

- **ANTIVIRUS:** son programas cuyo objetivo es detectar y eliminar virus informáticos. Los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos. Actualmente son capaces de reconocer otros tipos de malware como spyware, gusanos, troyanos, rootkits, pseudovirus etc.

4.1.1 Acceso a Internet

El acceso a servicios de Internet de Capital está controlado a través de un sistema de soluciones de administración de amenazas (UTM), appliance de firewall que permite proteger y minimizar los riesgos de ataque a las redes Wifi y LAN de la entidad, controlando de esta manera el acceso a sitios Web que estén catalogados como perjudiciales y que pongan en riesgo la seguridad de la información, el consumo excesivo de recursos o impidan la realización de las actividades laborales.

El acceso a Internet se establece a través de políticas expresas en el Firewall y se basa en categorías de acceso dispuestas por el Fortinet y una matriz de acceso dispuesta a continuación:



Captura de Sistema de Seguridad Perimetral, Firewall Fortigate

4.2 Mecanismos de seguridad asociados a los servicios de Red

1. Autenticación y control de acceso a través del directorio activo de Canal Capital, allí es donde se definen las credenciales de acceso a los recursos compartidos sobre la red de Canal Capital.
2. http://newintranet.canalcapital.gov.co/intranet/solicitud-de-servicios-tic/
3. Acceso remoto por VPN definidas, a través del UTM Fortinet.
4. Disponibilidad y redundancia de los servicios de Internet, Firewall (HA), Switch Core, Servidor de Dominio de Directorio Activo (AD-DS) definidos a través de las políticas del UTM Fortinet, garantizando la conmutación por error y balanceo de cargas del ancho de banda.

5. Gestión Remota Equipos Activos: SSH (o Secure SHell) es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

4.3 Segmentación Red LAN Canal Capital IPv4/IPv6

En la sede 1 principal ubicada en la Av. el Dorado #66 – 63 y sede 2 Chapinero calle 69 Cra. 11ª No. 69-43, se tienes las siguientes VLANs:

4.3.1 Segmentación IPv4

RED	MASCARA	NOMBRE SEDE	DESCRIPCIÓN VLAN	ID VLAN
172.16.0.0	/24	SEDE_01_TECNICA	GESTION	500
172.16.1.0	/24	SEDE_01_TECNICA	DATOS-TEC	502
172.16.2.0	/24	SEDE_01_TECNICA	DATOS-TEC	502
172.16.3.0	/24	SEDE_01_TECNICA	DATOS-TEC	172
172.16.4.0	/24	SEDE_01_TECNICA	DATOS-TEC	502
172.16.5.0	/24	SEDE_01_SISTEMAS	DATOS-USUARIOS	504
172.16.6.0	/24	SEDE_01_SISTEMAS	DATOS-USUARIOS	504
172.16.11.0	/24	SEDE_01_SISTEMAS	LIBRE	LIBRE
172.16.12.0	/24	SEDE_01_SISTEMAS	LIBRE	LIBRE
172.16.13.0	/24	SEDE_01_SISTEMAS	LIBRE	LIBRE
172.16.14.0	/24	SEDE_01_SISTEMAS	LIBRE	LIBRE
10.223.101.0	/25	SEDE_02_SISTEMAS	TELEFONÍA	220
10.10.10.0	/24	SEDE_01_SISTEMAS	ALMACENAMIENTO	?
192.168.0.0	/23	SEDE_01_SISTEMAS	SERVIDORES	?
RED	MASCARA	NOMBRE SEDE	DESCRIPCIÓN VLAN	ID VLAN
172.16.20.0	/24	SEDE_02_CHAPINERO	DATOS_USUARIOS	504
172.16.21.0	/24	SEDE_02_CHAPINERO	DATOS_USUARIOS	504
10.223.101.0	/25	SEDE_02_CHAPINERO	TELEFONÍA	220

4.3.2 Segmentación IPv6

SEDE	DIRECCIONAMIENTO /58	/56	FUNCIONALIDAD	VLAN
BOGOTA SEDE 01	2801:0016:6800:0000:0000:0000:0000:0000	/56	FIREWALL	500
	2801:0016:6800:0100:0000:0000:0000:0000	/56	LUMEN	502
	2801:0016:6800:0200:0000:0000:0000:0000	/56	COLUMBUS	504
	2801:0016:6800:0300:0000:0000:0000:0000	/56	WLAN-VISITANTES	506
	2801:0016:6800:0400:0000:0000:0000:0000	/56	WLAN-DIRECTIVOS	508
	2801:0016:6800:0500:0000:0000:0000:0000	/56	WLAN-TIC	510
	2801:0016:6800:0600:0000:0000:0000:0000	/56	WLAN-INTERNET-LIBRE	512
	2801:0016:6800:0700:0000:0000:0000:0000	/56	TELEFONÍA	514
	2801:0016:6800:0800:0000:0000:0000:0000	/56	PRUEBAS-1	516
	2801:0016:6800:0900:0000:0000:0000:0000	/56	PRUEBAS-2	518
	2801:0016:6800:0a00:0000:0000:0000:0000	/56	IPv6 PUBLICAS	520
	2801:0016:6800:0b00:0000:0000:0000:0000	/56	PRUEBAS-4	522
	…….	/56	LIBRE	
	2801:0016:6800:0f80:0000:0000:0000:0000	/56		
	2801:0016:6800:0fc0:0000:0000:0000:0000	/56		
		/56		
		/56		
BOGOTA SEDE 02	2801:0016:6800:2000:0000:0000:0000:0000	/56	GESTION	500
	2801:0016:6800:2040:0000:0000:0000:0000	/56	DATOS-USUARIOS	502
	2801:0016:6800:2080:0000:0000:0000:0000	/56	WLAN-USUARIOS	504
	2801:0016:6800:20c0:0000:0000:0000:0000	/56	WLAN-VISITANTES	506
	2801:0016:6800:2100:0000:0000:0000:0000	/56	WLAN-DIRECTIVOS	508
	2801:0016:6800:2140:0000:0000:0000:0000	/56	WLAN-TIC	510
	2801:0016:6800:2180:0000:0000:0000:0000	/56	WLAN-INTERNET-LIBRE	512
	2801:0016:6800:21c0:0000:0000:0000:0000	/56	TELEFONÍA	514
	2801:0016:6800:2200:0000:0000:0000:0000	/56	PRUEBAS-1	516
	…….	/56	LIBRE	
	2801:0016:6800:2f80::0000:0000:0000:0000	/56		
		/56		

4.4 Segmentación redes WLAN

Los servicios de red WLAN de Canal Capital están gestionados desde una controladora WLAN por el software Unifi, los AP son Unifi en los cuales está segmentada la red inalámbrica del Canal en tres categorías:

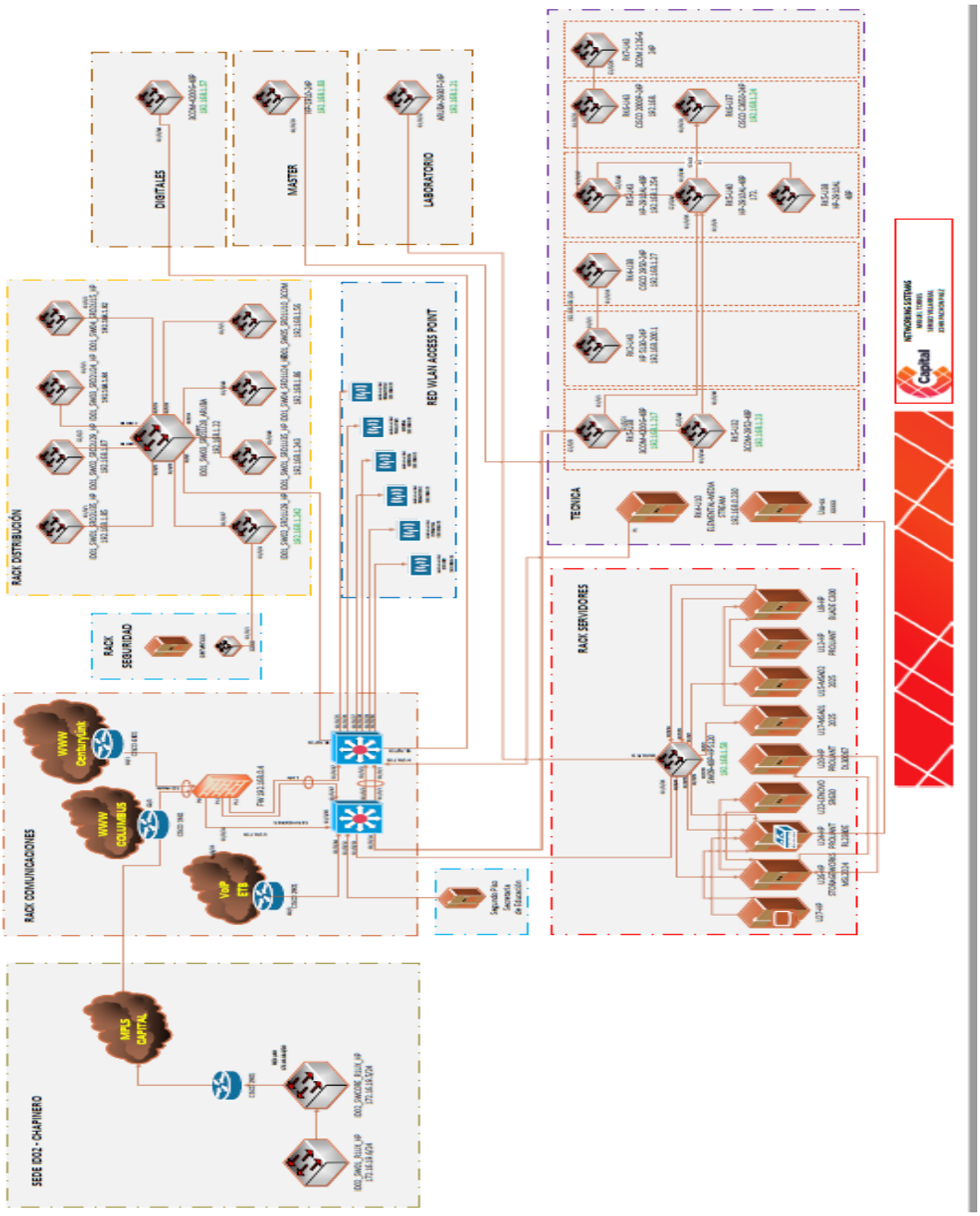
Móviles: Para la conexión de Smartphone y Tablet.

Portátiles: Para la conexión de computadores portátiles pertenecientes a Canal Capital o Invitados.

Directivos: Para la conexión de computadores portátiles, Smartphone y Tablet pertenecientes a los directores y líderes de área de Capital.

RED	MÁSCARA	SSID	DESCRIPCIÓN VLAN	ID VLAN
192.168.206.0	/24	CANAL CAPITAL-PORTÁTILES	WLAN-USUARIOS	202
192.168.206.0	/23	CANAL CAPITAL-VISITANTES	WLAN-VISITANTES	202
10.10.10.0	/24	CANAL CAPITAL-DIRECTIVOS	WLAN-DIRECTIVOS	202

4.3.2 Topología de Red



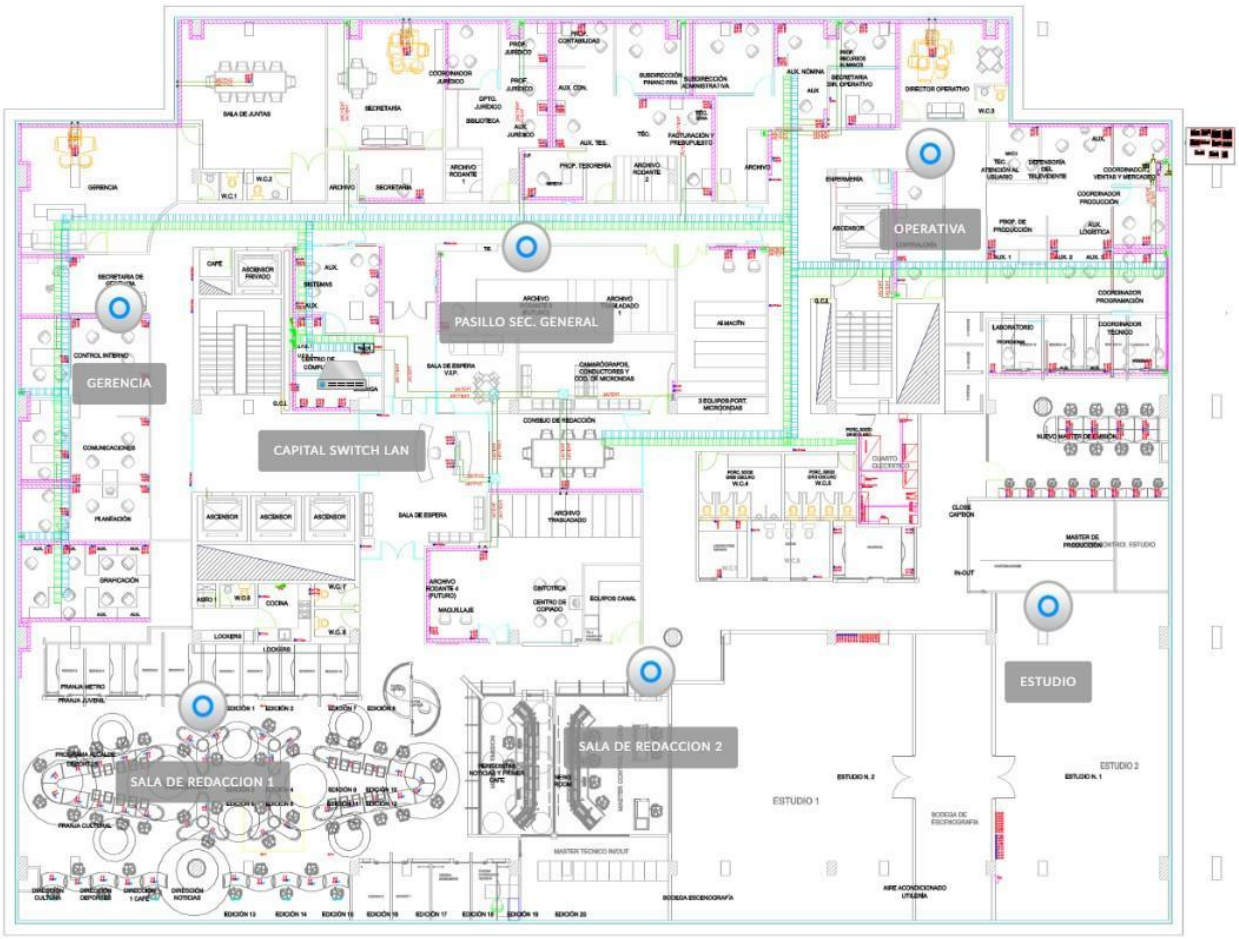
4.3.3 Descripción Topología General

Canal Capital sede principal ubicada en la Av. el Dorado #66 – 63, cuenta con dos canales de internet, Level (150 Mb) como principal y Columbus (90 Mb) como secundario; dos firewalls FortiGate 401E en HA (Alta Disponibilidad), dos switch CORE HP, un switch de distribución para el área de sistemas y el área de técnica y luego encontramos 25 Switch de acceso para usuario final; además se cuenta con un rack de servidores de 25 equipos en producción y un rack de cámaras de seguridad.

Canal Capital sede secundaria en Chapinero calle 69 Cra. 11ª No. 69-43, conectada lógicamente por un canal de datos de 40 mb (MPLS) hacia la sede principal; consumiendo los servicios de la sede principal.

4.3.4 Ubicación AP Red Wifi

El servicio de WLAN para la sede principal esta soportado por dos switch unifi POE y 6 APs unifi los cuales están distribuidos estratégicamente en el piso 5 como se observa en el plano siguiente:



5 Documentos Asociados

AGRI-SI-GU-005 Guía de Teletrabajo y Conexiones Remotas

AGRI-SI-MN-006 Manual de Políticas Complementarias de Seguridad de la Información

AGRI-SI-PO-002 Política de Seguridad y Privacidad de la Información

AGRI-SI-MN-005 Manual de Gestión de Usuarios