PROYECTO DE IMPLEMENTACION DE MEJORAS A LOS SISTEMAS DEL ENTORNO DIGITAL PRESENTES EN TICBRIDGE S.A.S.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

José Sebastián Pinilla Romero

Universidad Distrital Francisco José de Caldas

Facultad de Ingeniería

Bogotá D.C., Colombia

2021

Trabajo de Grado Presentado para Optar por el Título de:
Ingeniero Electrónico

Informe Final de Grado
Modalidad: Pasantía.

Elaborado Por:
José Sebastián Pinilla Romero
Código: 20151005097

Director Interno:
Ing. Gustavo Adolfo Puerto Leguizamón, PhD

Director Externo:
Ing. Harold Castillo Marín

Universidad Distrital Francisco José de Caldas
Facultad de Ingeniería
Bogotá D.C., Colombia
2021

Contenido

Lista de Figuras

Lista de Tablas

1. Resumen

TICBRIDGE S.A.S. es una empresa integradora de soluciones de telecomunicaciones e informática, sus principales proyectos se basan en el diseño, implementación y prestación servicios relacionados con la electrónica. Recientemente se sumaron servicios como software as a servicies (SaaS), seguridad informática y telefonía en la nube.

Este proyecto da cuenta de las implementaciones realizadas durante los meses de junio a diciembre del año 2021, su principal objetivo es mejorar los sistemas del entorno digital de TICBRIDGE S.A.S., los cuales son importantes para la consolidación de nuevos negocios, la implementación de soluciones y la prestación de servicios. Para ello se identificó el estado actual de la red tanto física como lógica para después realizar el respectivo estudio, implementación y prueba de mejoras; como la transferencia de la central telefónica a la nube, la implementación de un dispositivo Gateway con funciones de SD-WAN, la implementación de un firewall con sus respectivas políticas de seguridad y la gestión tanto para el rediseño como para la transferencia de hosting de la página web.

En este proyecto se hicieron uso de conocimientos y aptitudes adquiridos durante la carrera de ingeniería electrónica como lo son la telemática, las telecomunicaciones, programación y la gestión de proyectos.

2. Identificación del problema

2.1. Planteamiento del problema

Para toda empresa en el área tecnológica es de vital importancia realizar constantes mejoras a los sistemas ya existentes, ya que esto permite: 1. Un funcionamiento empresarial adecuado. 2. Mejores servicios y productos para sus clientes; hacer mejoras en el área digital es fundamental debido a que permite competir en un mercado que demanda mayor calidad.

Dentro del portafolio TICBRIDGE S.A.S. se encuentran soluciones enfocadas en las redes, por lo cual es necesario comprender el funcionamiento de estas y su implementación. De tal manera que el proceso de mejoramiento en la infraestructura de su sede principal es fundamental tanto para conectar adecuadamente a las personas que trabajan dentro de la sede principal como a las personas que trabajan en una sucursal o una vivienda. En este proyecto se realiza el respectivo estudio e implementación de un dispositivo Gateway con funciones de SD-WAN y la transferencia de una central telefónica a la nube con el fin de poder mejorar la infraestructura de la sede principal y a su vez de todos los trabajadores a lo largo del país.

Sumado a lo anterior para TICBRIDGE S.A.S. es importante responder a las necesidades de seguridad informática, ya que en los últimos años se ha evidenciado un crecimiento en los delitos cibernéticos, por esto es fundamental proteger las redes y dispositivos que conforman a cualquier empresa. En este proyecto se estudia e implementa una solución de seguridad informática con la cual se puedan establecer mecanismos de seguridad dentro de la misma.

Por último, en este proyecto se toma la página web como una herramienta fundamental para cualquier empresa hoy en día, ya que el posicionamiento web incide en un gran número de personas y a su vez generar nuevos clientes, por lo anterior en este proyecto se gestiona el rediseño de la página web y la respectiva transferencia del hosting.

2.2. Justificación

TICBRIDGE S.A.S. es una empresa enfocada en las áreas de telecomunicaciones e informática, la cual se ha caracterizado por el diseño e implementación de soluciones enfocadas en la alta calidad y eficiencia, por lo cual el realizar mejoras en sus diferentes áreas es fundamental por la naturaleza de estas.

Es así como se hace fundamental el estudio, implementación y prueba de nuevas tecnologías que permitan mejorar el funcionamiento interno de la compañía, principalmente para su sede en Bogotá D.C. desde la cual se realiza la administración de las diferentes sedes, por esto el trabajo está enfocado en el mejoramiento de la red local de la sede principal, la seguridad informática y la respectiva gestión para el rediseño de la página web.

El objetivo principal de esta pasantía es hacer uso de los conocimientos y aptitudes adquiridos durante la carrera de Ingeniería electrónica para generar un proyecto específico y a su vez obtener experiencia en el mercado laboral desempeñando actividades relacionadas con la gestión de proyectos, la telemática y las telecomunicaciones.

3. Objetivos

3.1. Objetivo general

Analizar el entorno digital actual de TICBRIDGE S.A.S. a nivel lógico y funcional con el fin de implementar mejoras a los sistemas del entorno digital utilizados para la correcta entrega de soluciones provista por la empresa.

3.2. Objetivos específicos

- Analizar el estado actual de las redes presentes en la empresa TICBRIDGE S.A.S con el fin de incorporar mejoras de funcionamiento en los sistemas LAN, WiFi, y servidores NAS, entre otros.
- Implementar y administrar plataformas virtuales utilizadas para ofrecer soluciones como lo son share point, página web y servicios en la nube.
- Examinar sistemas utilizados para la seguridad propia de la empresa TICBRIDGE S.A.S como lo son los sistemas CCTV, control de acceso y seguridad informática, para la incorporación de mejoras tanto a nivel lógico como funcional.

4. Desarrollo y análisis de resultados de las mejoras implementadas

4.1. Identificación de la red

El proyecto de implementación de mejoras a los sistemas del entorno digital presentes en TICBRIDGE S.A.S. da inicio con el respectivo estudio de la red local presente en la sede de Bogotá D.C, con el fin de determinar cuáles son las modificaciones realizadas en anteriores proyectos y cuáles serán las posibles mejoras por realizar, de tal manera que se realizó un levantamiento de las pasantías y proyectos realizados anteriormente.

Tomando en cuenta los anteriores proyectos se procede a realizar un estudio tanto físico como lógico del estado de la red, basado en el levantamiento de los documentos y en el reconocimiento tanto lógico como físico propio.

Donde se destaca la división de la red en 3 VLAN diferentes, mejoras en el servidor, en las cuales se encuentran la configuración de muchos de los servicios sumado a la mejora del hardware del servidor como lo son la Board, el procesador y la memoria RAM.

4.1.1. Estudio físico

Se procede a realizar la caracterización física de los diferentes dispositivos presentes en la sede principal de TICBRIDGE S.A.S. ubicada en Bogotá D.C., identificando cada dispositivo perteneciente a la red y su respectiva ubicación en la sede. Los dispositivos se encuentran divididos por 3 VLAN diferentes las cuales fueron creados en proyectos anteriores y caracterizadas [1], se procede a realizar el modelado físico del lugar teniendo en cuenta algunas modificaciones realizadas durante el periodo de tiempo intermedio en los proyectos.

Tomando en cuenta las VLAN implementadas en la red para el modelado se le da un determinado color a cada una de ellas y a sus respectivos dispositivos, como se puede observar a continuación.

- Rojo: VLAN 40 (CCTV).
- Azul: VLAN 20 (Administrativo).
- Verde: VLAN 30 (Telefonía IP).

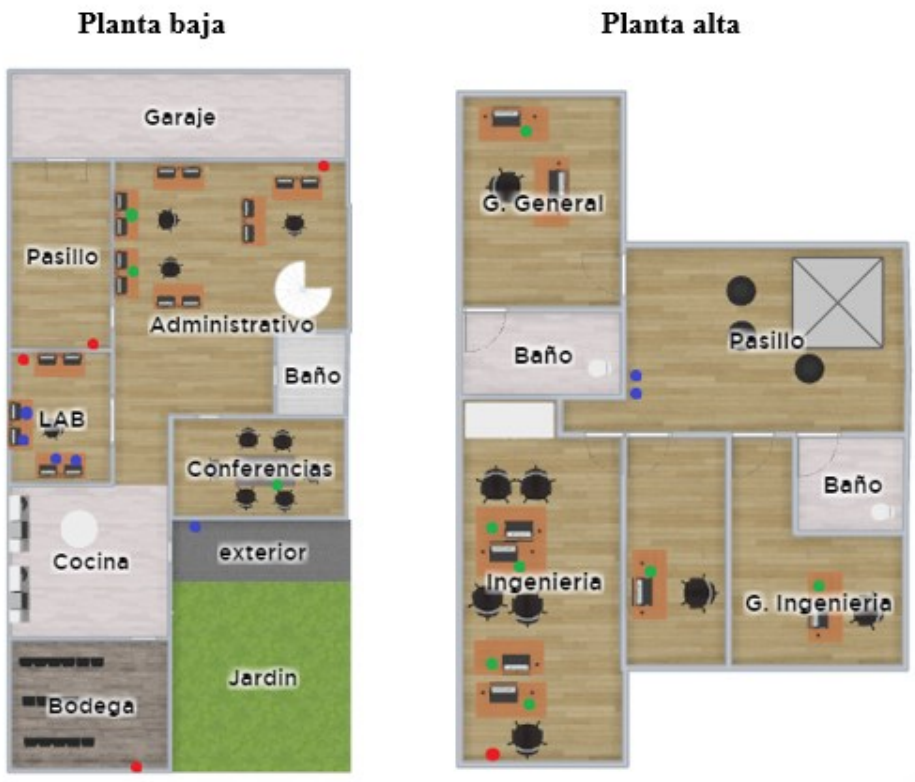

Figura 1: Modelado sede principal TICBRIDGE S.A.S.

4.1.2. Reconocimiento lógico

Posteriormente se realiza el reconocimiento lógico de la infraestructura de TICBRDGE S.A.S. teniendo en cuenta las 3 VLAN anteriormente mencionadas, este proceso se realiza por medio del levantamiento de los proyectos anteriores [1].

SUB-RED	Direccionamiento
Planta Telefónica	VLAN 30: 172.30.30.10/24
Red Administrativa	VLAN 20: 172.16.20.10/24
CCTV	VLAN 40: 172.40.40.11/24

Tabla 1. Subredes TICBRIDGE S.A.S.

Teniendo en cuenta lo anterior se procede la respectiva diagramación lógica de los diferentes dispositivos de la empresa, donde se observa cuales se encuentran conectados alambricamente a la red y los que se encuentran conectados de forma inalámbrica, dado que en su mayoría son Lap-Top.

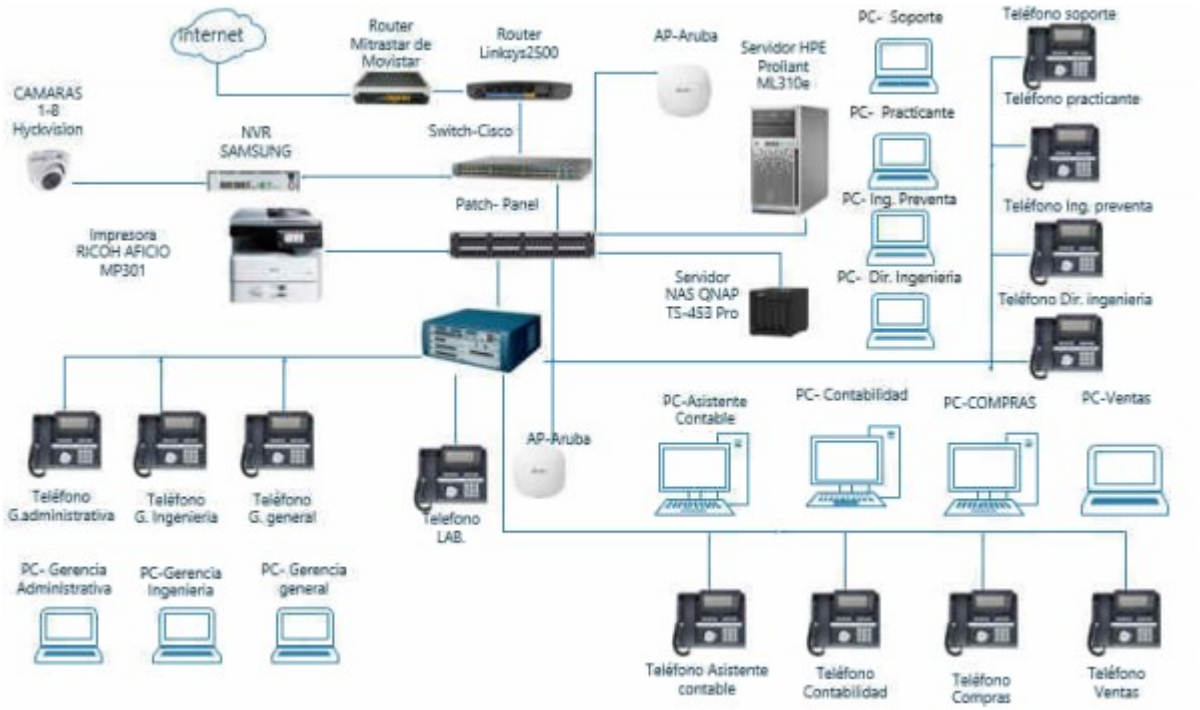

Figura 2. Diagrama lógico TICBRIDGE S.A.S.

Con el fin de determinar si los dispositivos se encuentran en correcto funcionamiento y con la dirección IP de los anteriores proyectos [1], se procede a realizar la respectiva verificación por medio un Ping (comando que permite determinar si hay conexión entre dos dispositivos) a cada una de las direcciones IP de los dispositivos desde un dispositivo que se encuentre conectado a la misma red, ya sea de manera inalámbrica para la red VLAN 20 o de manera alámbrica como lo fue para la VLAN 30 Y VLAN 40 .

SUB-RED	Dispositivo	IP	Conexión
VLAN 20-Administrativa	Impresora	172.16.20.15	Si
VLAN 20 – Administrativa	Server	172.16.20.119	No
VLAN 20 – Administrativa	AP- PISO 1	172.16.20.12	Si
VLAN 20 – Administrativa	AP- PISO 2	172.16.20.13	Si
VLAN 20 – Administrativa	NAS	172.16.20.14	Si
VLAN 20 – Administrativa	ROUTER LINKSYS_GATEWAY	172.16.20.6	Si
VLAN 30 – VoIP	Planta Telefónica	172.30.30.11	Si
VLAN 30 - VoIP	Telefonía Pruebas	172.30.30.14	Si
VLAN 30 - VoIP	Ge. Administrativa	172.30.30.15	Si
VLAN 30 - VoIP	Ge. General	172.30.30.18	Si
VLAN 30 - VoIP	Ge. Ingeniería	172.30.30.17	Si
VLAN 30 - VoIP	Asist. Contable	172.30.30.19	Si
VLAN 30 - VoIP	Asist. Administrativa	172.30.30.20	Si
VLAN 30 - VoIP	Puesto Compras	172.30.30.21	Si
VLAN 30 - VoIP	Ing. Preventa	172.30.30.22	Si
VLAN 30 - VoIP	Account Manager Sr.	172.30.30.24	Si
VLAN 30 - VoIP	Practicante	172.30.30.25	Si
VLAN 40 - CCTV	NVR	172.40.40.20	Si
VLAN 40 - CCTV	CAM1 RECEPCION	192.168.231.8	Si
VLAN 40 - CCTV	CAM2 BODEGA	192.168.231.3	Si
VLAN 40 - CCTV	CAM3 SALA REUNIONES	192.168.231.5	Si
VLAN 40 - CCTV	CAM4 PASILLO PISO 2	192.168.231.7	Si
VLAN 40 - CCTV	CAM 5 LAB	192.168.231.6	Si
VLAN 40 - CCTV	CAM 7 ENTRADA	192.168.231.2	Si
VLAN 40 - CCTV	CAM 8 SALA INGENIERIA	192.168.231.4	Si

Tabla 2. Dispositivos TICBRIDGE S.A.S.

4.2. Mejoras en la red

Tomando el estado de la red y los nuevos servicios que se encuentran en el portafolio de TICBRIDGE S.A.S. se propone realizar dos mejoras a la red, la respectiva transferencia de la central telefónica física a una en la nube dado que recientemente la empresa se convirtió en aliado de Fortinet y la implementación de un dispositivo Gateway con funciones de SD-WAN, cada una de estas mejoras se realizara teniendo en cuenta, el estado actual de los elementos que serán reemplazados o que intervienen directamente con ella, el estudio de la mejora y su respectiva implementación.

4.2.1. Transferencia de la central telefónica a la nube.

Las telecomunicaciones son una parte fundamental para la sociedad, estas han ido creciendo y evolucionado formando parte de nuestra cotidianidad, para las empresas el poder brindar una buena calidad de servicio se ha convertido en sinónimo de un buen sistema de telefonía, por lo cual la implementación de tecnología de vanguardia que hace uso de herramientas como la nube, es fundamental para el crecimiento de las entidades que requieren de estar en constante contacto con sus clientes.

Tomando lo anterior en cuenta TICBRIDGE S.A.S. ha decidido implementar un sistema de telefonía en la nube como lo es 3CX, dado que dicho sistema es una solución completa de comunicaciones unificadas multiplataforma. Se escoge principalmente 3CX por que permite hacer uso de servicios de la telefonía tradicional sumado a la posibilidad de usar diferentes plataformas y las propiedades que de por sí ya contiene los servicios en la nube.

4.2.1.1. Estudio central telefónica Siemens Hipath 3500

Con el fin de evidenciar las mejoras y realizar una transferencia correcta de la central telefónica, se realiza un estudio de la utilizada actualmente, en la cual se puedan evidenciar las diferentes características que esta posee. Ya que en el estudio anterior de la red se pudo observar la determinada configuración lógica, de la respectiva central y de los teléfonos que se encuentran conectados directamente a ella y la subred VLAN 20 creada específicamente para los dispositivos de VOIP.

Se pudo observar que la central telefónica utilizada era la Siemens Hipath 3500 la cual estaba siendo utilizada principalmente para el funcionamiento de las diferentes líneas internas y la conexión a esta a la red pública.

Figura 3:Siemens Hipath 3500 tomado de [2].

Dicho dispositivo es de la serie Hipath 3000 diseñada específicamente para un gabinete de 19 pulgadas, con disponibilidad de diferentes dispositivos de la gama Hipath como lo son:

- Teléfonos analógicos
- Microteléfono digital Optipoint
- Teléfonos IP Optipoint
- Teléfonos inalámbricos Optipoint DECT

Adicionado a lo anterior en cuanto a sus características de funcionamiento se observa que:

	Siemens Hipath 3500
Usuarios analógicos, máximo	44
Usuarios digitales (UPO/E), máximo	48
Usuarios IP, máximo	192
Usuarios HiPath Cordless, máximo	32
Estaciones base Cordless, máximo	7
Interfaces V.24	1
Sistemas enlazados por IP	64

Tabla 3. Características Hipath 3500 tomado de [2].

4.2.1.2. Estudio de solución

Tomando en cuenta el estudio anterior de la central telefónica, en el cual se pudo evidenciar algunas limitaciones que esta poseía se procede a realizar un estudio de las soluciones y como estas presentan algunas mejoras en cuanto a capacidad sumado a múltiples herramientas en la nube y su aplicación para la telefonía en la nube como lo hace 3CX.

4.2.1.2.1. Telefonía en la nube

La telefonía en la nube permite la implementación de lo que sería un PBX haciendo uso de todas las diferentes cualidades que cuenta la nube las cuales son:

- La implementación de nuevos modelos de pago como lo es el "pago por uso", en el cual se cobra únicamente por la cantidad de procesamiento requerido.
- Permite realizar modificaciones en poco tiempo y agregar nuevos dispositivos, por lo cual facilita la escalabilidad de las propias organizaciones que hagan uso de esta.
- Las modificaciones se pueden realizar sin la necesidad de que se tenga que hacer interacción directa con el hardware.
- Permite realizar una jerarquía en cuanto a los usuarios que hagan uso de ella por lo cual se generan roles con sus propias funciones.
- Permite su acceso desde cualquier lugar con diferentes dispositivos a los que se les puede dar la respectiva extensión.
- Manejo y recolección de una gran cantidad de información.

Ahora en cuanto al funcionamiento propio de la telefonía en la nube es importante tener en cuenta que todo se basa en la central para la recepción y control de llamadas, a su vez es necesario de personas que hagan uso de la nube desde cualquier lugar.
Teniendo en cuenta lo anterior, se pueden observar los siguientes requerimientos para la correcta implementación de la telefonía en la nube:

- **Empresa proveedora del servicio de telefonía en la nube:** este aspecto es fundamental, ya que se requiere de un buen servicio por si se presenta un problema y se requiere de soporte. Sumando a que se debe requerir que el software sea el adecuado para la correcta implementación.
- **Conectividad a internet:** Se quiere hacer uso de la nube, para ello es necesario una buena conexión a la misma tanto por la data center como los receptores de las llamadas, adicionado a esto se debe tener en cuenta como esta aplicación requiere de un determinado ancho de banda del que se utiliza en la cotidianidad.
- **Dispositivos:** El correcto uso de dispositivos que permitan mantener una constante conexión con el PBX en la nube. [3]

4.2.1.2.2. 3CX

3CX es una de las empresas líderes en las comunicaciones empresariales, ya que permite realizar la implementación de varias plataformas como los son chat en vivo, llamada y video, adicionalmente esta hace uso de sus servicios desde diferentes modelos ya sea on premise (se instala el software en un equipo local) o en la nube.
cuenta dicho dispositivo son:

Central telefónica: 3CX cuenta con una central telefónica diseñada especialmente para otorgar un buen servicio al cliente y para hacer el trabajo de los empleados sea más fácil, dada la gran cantidad de funcionalidades con las que cuenta: colas de llamadas, video llamadas integradas, conferencias web y mucho más. Adicional a integrar mensajes desde diferentes plataformas como lo son chat en vivo del sitio web o Facebook.

Central virtual: 3CX permite realizar la migración de la central física a una en la nube, de tal manera que aún se pueda hacer uso de ellas sin que genere problemas en el normal funcionamiento de la compañía agregado a la suma de aplicaciones que da 3CX, sin tener en cuenta costos, la central de 3CX muchas veces más económicas que una central on premise de otras compañías.

Call center integrado: 3CX ofrece la solución enfocada en mejorar el servicio de grandes plataformas telefónicas como lo son los Call Center, con el fin de mejorar varios de los servicios prestados, como aumentar la capacidad de los usuarios que pueden llegar a ser atendidos gracias a la automatización de procedimientos y al enfoque al buen servicio. [4]

Tomando en cuenta tanto la información del respectivo funcionamiento de las centrales telefónicas en la nube sumado al propio de 3CX, se evidencia que esta funciona de tal manera que los usuarios pueden ingresar a la misma, ya se encuentren dentro de la red local empresarial, desde una oficina de manera remota.

Figura 4. Funcionamiento 3CX.

4.2.1.3. Procedimiento de mejora

Habiendo evidencia de las ventajas con las que cuenta tanto la telefonía en la nube como la propia 3CX se procede a realizar la transferencia de la central telefónica a la nube, este proceso requiere de varios pasos como lo son la respectiva creación de la máquina virtual, la configuración de la central en la nube y el aprovisionamiento de los teléfonos para que funcionen correctamente.

4.2.1.3.1. Creación máquina virtual 3CX

El primer paso para la implementación de la central telefónica en la nube es la respectiva creación de la máquina virtual, en la cual esta se encontrara alojada, para esto es fundamental tener en cuenta que se debió adquirir anteriormente un proveedor de servicios en la nube como en este caso lo es para TICBRIDGE S.A.S. la empresa Microsoft, la cual cuenta con servicios de alojamiento para máquinas virtuales, los pasos para la creación de la máquina virtual se pueden observar a continuación:

- Se selecciona la creación de una nueva central telefónica y se ingresa la siguiente información acerca de la persona encargada de la administración de este:
    - Nombre
    - Apellido
    - Empresa
    - País
    - Zona horaria
    - Idioma
    - Teléfono
    - Localización.

- Selección de implementación (nube u on premise):
    - Self-host in your cloud
- Seleccionar Información propia de la central telefónica de la nube:
    - País: Estados unidos
    - Zona horaria: Centro sur estados unidos (UTC-8)
    - Lenguaje: español
- Tomar un dominio para la administración de la máquina virtual desde la web:
    - Nombre del HOST: sipticbridge
    - Grupo de Dominio: sipticbridge.3cx
    - Dominio: sipticbridge.3cx.co.
- Escoger número de extensiones que se utilizaran en la central telefónica:
    - Numero de extensiones: 1000 (000-999)
- Seleccionar el proveedor, en este paso es fundamental tener en cuenta que en esta parte se ingresa la información de la máquina virtual creada anteriormente:
    - Hosting: Microsoft Azure
    - ID de suscripción: **********
    - Región: Centro sur de estados unidos
    - Tipo de maquina: 1 VCPU Y 2GiB

4.2.1.3.2. Instalación de SBC virtual

Se instala un SBC (Session Border Controller) virtual en el servidor de la empresa, ya que este permite la combinación de paquetes de VOIP y RTP, para la conexión entre los teléfonos y la central telefónica 3cx en la nube, disminuyendo la complejidad y evitando que se generen problemas de seguridad a la hora de acceder a los teléfonos en la red por parte de 3CX. Adicionalmente este dispositivo permite mejorar las comunicaciones que se realicen de manera interna, ya que permiten que se hagan llamadas internas sin necesidad de que se utilicen un enlace a internet.

Para la instalación se realiza el siguiente procedimiento, se ingresa a la consola de administración vía el entrono web de la central telefónica creada anteriormente en la nube y en troncales SIP se crea la SBC. A la hora de crear dicha SBC es necesario ingresar información como el respectivo nombre, contraseña, IP publica: 161.18.217.220 y la IP privada: 172.16.20.119 del alojamiento de la SBC.

Al terminar de crear la SBC se obtiene la URL de aprovisionamiento y la KEY ID de autenticación las cuales fueron utilizadas cuando se instaló el programa en SBC 3CX en el servidor de la empresa.

4.2.1.3.3. Configuración PBX en la nube

Luego de tener la respectiva configuración de la máquina virtual y un almacenamiento definido se procede a la configuración de la central telefónica en la nube. Los pasos para realizar se pueden observar a continuación:

1. Configuración de los usuarios donde se debe ingresar la información de cada uno de los usuarios que harán uso de las extensiones de la central telefónica, para eso se debe ingresar información como la respectiva extensión, nombre, apellidos, correo, número de celular.

Ext.	Nombre	Apellido	Correo	Numero
100	Auxiliar	Contable	alejandra.torres@ticbridge.com	3165254609
101	Gerencia	General	pedro.baron@ticbridge.com	3138026449
102	Gerencia	Administrativa	yulieth.pastran@ticbridge.com	3183349248
103	Ingeniería	y servicios	harold.castillo@ticbridge.com	3103090029
104	Dirección	de ingeniería	michael.reyes@ticbridge.com	3183349243
106	Soporte		servicios.bog@ticbridge.com	3176478793
107	Sala	Conferencias	servicios.bog@ticbridge.com	
108	Compras		compras@ticbridge.com	3183539790
109	Prueba	Check In	servicios.bog@ticbridge.com	
110	Pre	Venta	proyectos1@ticbridge.com	3124579010
111	Pasante	Ticbridge	practicante@ticbridge.com	
112	Ventas	Bogotá	Ventas2@ticbridge.com	316454356
117	Soporte	Cali	merardo.arias@ticbridge.com	3174311847
120	Portero	Ticbridge	merardo.arias@ticbridge.com	3174311847
200	Ingeniería	Cali	alvaro.gutierrez@ticbridge.com	033124579011

Tabla 4. Configuración Usuarios.

2. Configuración de las diferentes troncales SIP, este paso es fundamental ya que gracias a este podremos utilizar los protocolos SIP (protocolo para el establecimiento entre dispositivos), de tal manera que se procede a realizar la configuración de varias troncales una de ellas para el proveedor de telefonía como lo es ETB y la respectiva SBC para 3CX-

   Para esto se llena la información de la respectiva troncal como la respectiva dirección IP del HOST, el tipo de troncal, el número de llamadas simultaneas y el número de la troncal (en cuanto al tipo SBC este espacio se llena con la versión de la SBC).

Nombre	Host	Tipo	Llamadas simultaneas	No° Principal troncal
ETB	201.245.193.140	Provider	5	7705230
WebMeeting Bridge	----------	Web master-Direct	50	90000
TICBRIDGE SBC	161.18.115.83	SBC	0	Versión: 18.030

Tabla 5. Configuración SIP.

3. Configuración de las reglas entrantes, estas reglas se usan principalmente para el direccionamiento de las llamadas y para que se pueda dar un respectivo trato dependiendo si la llamada se realiza dentro o fuera de la oficina, para esto es necesario ingresar la información como tipo de regla, nombre, troncal, número telefónico, ruta de direccionamiento tanto dentro como fuera del horario de oficina.
   Principalmente se crean dos reglas las cuales son utilizadas para cuando se ingresen llamadas a la empresa, una de ellas rutea extensión 800 reproduce un mensaje automático que recomienda digitar las respectivas direcciones que desea o directamente lo conecta con la extensión 100 la cual es contestada por la auxiliar contable, por otro lado, la entrada 018000 reproduce un mensaje grabado definido para el área técnica de TICBRIDGE S.A.S.

Tipo	Nombre	Troncal	Número DID/DDI	Ruteo en oficina	Ruteo Fuera de Oficina
DID	ENTRADA_TB	ETB	7705230	800 MSG_PPL	802 horario no hábil
DID	ENTRADA 018000	ETB	7705232	801 LINEA 018000	801 LINEA 018000

Tabla 6. Reglas entrantes.

4. Configuración de las reglas salientes, las cuales son las reglas de las diferentes rutas y procedimientos que se realizaran cuando se realicen llamadas desde dentro de la empresa al exterior, por lo cual para la configuración se ingresa el nombre de la regla, prefijo, longitud y la ruta.

   En esta parte es fundamental tener en cuenta que durante la pasantía se establecieron nuevos métodos de marcación a nivel nacional de tal manera que hay que plantear las reglas de salida concorde a dichas modificaciones. La nueva marcación se basa en marcar 60+indicativo de ciudad; por lo cual se crean varias reglas con los prefijos del marcaje a varias ciudades diferentes. Adicionalmente se crea una regla para las llamadas celulares Teniendo en cuenta la longitud del marcaje y su prefijo que en este caso seria 3.

Nombre	Prefijo	Longitud	Ruta 1
Salida local ETB	601	10	ETB
Celular	3	10	ETB
Salida NAL ETB 602	602	10	ETB
Salida NAL ETB 603	603	10	ETB
Salida NAL ETB 604	604	10	ETB
Salida NAL ETB 605	605	10	ETB
Salida NAL ETB 606	606	10	ETB
SALIDA NAL 607	607	10	ETB
Salida NAL ETB 608	608	10	ETB
SALIDA 018000	018000	12	ETB
3 digitos	0-9	3	ETB

Tabla 7. Reglas salientes.

5. Configuración de la recepcionista virtual, la cual es un mensaje pregrabado dependiendo de las extensiones de que se marquen para esto se requiere ingresar la respectiva extensión, nombre del mensaje, el tipo de recepcionista, el mensaje que por lo general es un archivo.wav y la acción a realizar si no se ingresa ninguna extensión durante el tiempo que el mensaje se reproduzca.

Ext	Nombre	Tipo	Mensaje	Sin Entrada
HOL	Out off office IVR	Estándar	Officeclosed.wav	End call
800	MSG_PPL	Estándar	Ticbridge.wav	Extensión 100 Alejandra torres
801	Línea 018000	Estándar	Coverted_linea018000.wav	Extensión 200 Alvaro Gutierrez
802	Horario no hábil	Estándar	Coverted_Horarionohabil.wav	Voice mail 100 Alejandra torres

Tabla 8. Configuración recepcionista virtual.

4.2.1.3.4. Aprovisionamiento de teléfonos

Los dispositivos telefónicos necesitan acceder a la nube y a su vez a internet, por ello se le asigna una IP estática a los teléfonos en la VLAN 20 para el respectivo ingreso a internet, de tal manera que quedan registrados de la siguiente manera los teléfonos.

USUARIO	REFERENCIA	MAC	DIRECCION IP
G. General	OPENSTAGE 60	001AE84FC3C7	172.16.20.31
G. Administrativa	OPENSTAGE 60	001AE84FC3C2	172.16.20.32
G. Ingenieria	OPENSTAGE 60	001AE84FC3CF	172.16.20.37
D. Ingenieria	OPENSTAGE 40	001AE84638EE	172.16.20.38
Aux. Contable	OPENSTAGE 80	001AE8454918	172.16.20.30
Compras	OPENSTAGE 40	001AE8478B08	172.16.20.36
Ing. Soporte	YEALINK T21 E2	001565E7A0FB	172.16.20.34
Ing. Preventa	OPENSTAGE 40	001AE81B11E1	172.16.20.33
Ventas	YEALINK T21 E2	001565E79F50	172.16.20.35

Tabla 9. Asignación de direcciones IP estáticas.

Dado que en la empresa se encuentran dos teléfonos IP de diferente proveedor se realiza el debido estudio de cada uno y su aprovisionamiento, teniendo en cuenta que es debido realizar un procedimiento diferente para cada dispositivo.

4.2.1.3.4.1. OPENSTAGE

Adicional a esto se observa que los dispositivos telefónicos para cada una de estas direcciones es Siemens OpenStage 40hfa, entre las funciones que permite el dispositivo se encuentran:

- Aceptar, rechazar y reenviar llamadas
- Dejar llamadas en espera
- Realizar conferencias
- Capturar las llamadas
- Creación y manejo de diferentes perfiles de usuario. [5]

4.2.1.3.4.1.1. Aprovisionamiento OPENSTAGE

Los teléfonos Open Stage funcionan con un firmware HFA, el cual es exclusivo de Siemens y no es compatible con terminales SIP, por ello es necesario realizar la actualización del firmware como la respectiva restauración de fábrica.

Mediante el entorno web del teléfono se ingresa a la sección de sistema y en ella, al registro donde se da la respectiva FQDN del SIP de TICBRIDGE S.A.S. Posteriormente se configura la sesión de SIP donde se ingresan los valores determinados para el usuario que va a hacer uso de este dispositivo por medio de 3CX, estos valores se obtienen directamente de la interfaz administrativa de 3CX, se configura el SIP Survivality, y se ingresa la información del SBC creado y por último se configura el Standar CSTA, en el cual se da tanto la dirección del servidor como el puerto que se va a utilizar.

4.2.1.3.4.2. YEALINK

Adicionalmente para las extensiones nuevas se hace uso de teléfonos Yealink T21P_E2, los cuales se caracterizan principalmente por sus altos estándares en cuanto a la seguridad informática y a facilidad para el aprovisionamiento de estos.

Las principales características de los dispositivos anteriormente descritos son:

- Gestión de llamadas: permite programar botones y estructuras propias con el fin de ayudar a los usuarios a mejorar la gestión de las llamadas añadido a la implementación y compatibilidad para la gestión de dispositivos externos como los son los auriculares.
- Instalación y aprovisionamiento eficiente: Cuenta con una gran variedad de protocolos para él transporte de información con diferente naturaleza algunos de los protocolos mencionados anteriormente son s FTP, TFTP, HTTP, y HTTPS.
- Seguridad: Utiliza el protocolo a SIP over Transport Layer Security (TLS/SSL) los cuales aseguran que se puedan realizar comunicaciones con altos estándares de calidad, haciendo que este dispositivo sea compatible con 3CX, Asterisk y Broadsoft Broaworks. [6]

4.2.1.3.4.2.1. Aprovisionamiento YEALINK

Como los teléfonos YEALINK si son compatibles con 3CX se realiza un proceso de una manera más sencilla, el método implementado se llama PnP (Plug and Play), basado en que los teléfonos están conectados a la red y estos envían un mensaje multicast, el cual al ser recibido por la central 3CX, permite su aprovisionamiento desde la central para posteriormente asignar una respectiva extensión al teléfono; por último se puede realizar la respectiva configuración del teléfono como lo es la zona horaria o el idioma.

4.2.2. SD-WAN

El creciente uso de herramientas especializadas y servicios en la nube ha generado que las empresas tengan que cambiar las políticas de conectividad, tradicionalmente se han manejado redes WAN basadas en MPLS, las cuales dado su funcionamiento y enrutamiento ofrecen un ancho de banda limitado. Como solución a las limitaciones de las redes WAN tradicionales han nacido nuevas soluciones de red como lo es la SD-WAN, la cual es una solución más económica que permite a las empresas incorporar y controlar varios enlaces de red diferentes como lo son WAN, redes móviles (4G/5G) y redes virtuales entre otras, con el fin de mejorar la calidad de servicio a un menor coste.

4.2.2.1. Estudio de solución

Las SD-WAN utilizan diferentes enlaces de red como lo son la internet publica, nubes, redes móviles (4G /5G) y otros enlaces. La utilización de dichos enlaces es controlada dependiendo de la aplicación y el respectivo ancho de banda que esta requiera. Dicho control es permitido gracias a que la SD-WAN, detecta desde el primer paquete de datos enviado cual será la aplicación para posteriormente realizar el respectivo enrutamiento automático que permita la selección de enlaces dependiendo de la aplicación.

En cuanto a los beneficios de administración, una red SD-WAN centraliza la gestión de los diferentes enlaces con información del tráfico y su respectivo desempeño. Dicha gestión permite detectar cuando se encuentran anomalías o errores en la red a la vez que permite generar políticas de desempeño para cada uno de los enlaces desde un solo punto.

4.2.2.1.1. SD-WAN VS WAN

Al realizar la comparación con las WAN (Wide Area Network) tradicionales basadas en MPLS (Multiprotocol Label Switching), el cual es un protocolo de enrutamiento que se basa fuertemente en los protocolos IP que permite a las compañías realizar conexiones seguras de punto a punto, a un costo alto se lograron observar las siguientes diferencias:

1. La SD-WAN maneja un buen sistema de control y de hospedaje en la capa de aplicación.
2. Las configuraciones en la red SD-WAN se pueden realizar por medio de software sin la necesidad de que se haga uso de cambios físicos, lo cual facilita el manejo y mantenimiento.
3. En la SD-WAN se adopta el uso de nuevas herramientas para el manejo de las redes como lo es la inteligencia computacional y la virtualización de la misma red.
4. La SD-WAN es menos costosa tanto en su desarrollo como en su mantenimiento.

4.2.2.1.2. Arquitectura SD-WAN

Como cualquier solución en la red, la SD-WAN tiene su propia arquitectura tanto lógica como física, por lo cual se realiza el respectivo estudio de ambas arquitecturas, con el fin de observar su funcionamiento y evaluar si esta es la solución más adecuada a implementar en la empresa TICBRIDGE S.A.S.

4.2.2.1.2.1. Arquitectura lógica

La SD-WAN cuenta con tres diferentes capas lógicas descritas a continuación:

1. Capa de datos: se basa en dos partes como los son la virtualización del ancho de banda y el reenvió de datos.
   - Virtualización de ancho de banda: combina todos los enlaces de red y los une ene un pool de recursos.
   - Reenvió de datos: se hace por medio de Switches los cuales también utilizan tanto el ancho de banda normal como el virtual.
2. Capa de control: monitorea y controla el tráfico con el fin de entregar los mayores estándares de servicio al cliente.
3. Capa de aplicación: esta capa es la encargada de entregar la plataforma más familiar y fácil de manejar para los usuarios de la red.

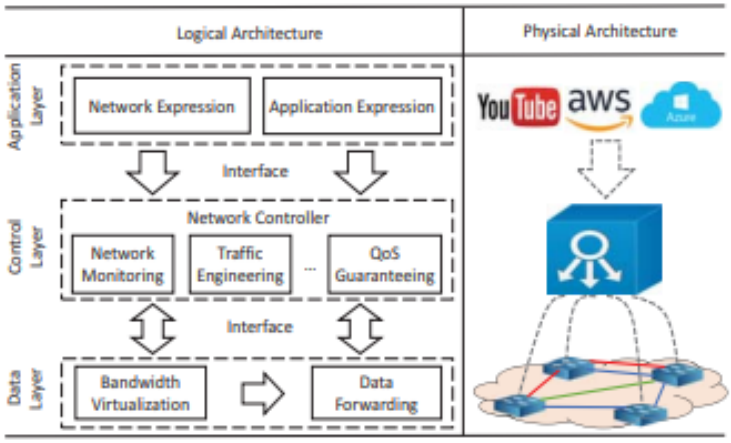

Figura 5:Arquitectura SD-WAN tomado de [7].

4.2.2.1.2.2. Arquitectura física

La SD-WAN cuenta con tres diferentes capas físicas descritas a continuación:

1. Capa de datos: conjunto de SDN conectados entre sí mediante enlaces físicos.
2. Capa de control: normalmente es un servidor o un Cluster, generalmente hay más de un controlador de red distribuido en diferentes sitios, con un controlador maestro y otros llamados controladores de respaldo.
   - Monitoreo de la red: usualmente se utiliza open Flow y Payless, las cuales permiten observar el comportamiento con estadísticas el comportamiento de la red.
   - Ingeniería de tráfico: protocolos distribuidos como OSPF/IS (IS son soluciones de enrutamiento en internet), SWAN 7y SDWAN son dos controladores diseñados tanto por Microsoft como Google los cuales son los encargados del manejo de la red con la finalidad de una mayor optimización.
   - Garantia de QoS: se desarrollan varios sistemas de control dependiendo de la aplicación que se le vaya a dar, por ejemplo, para la transmisión de video se han desarrollado diferentes sistemas para asegurar la satisfacción del consumidor.
3. Capa de aplicación: aplicaciones específicas. [7]

4.2.2.2. Soluciones SD-WAN proveedores

Ya vista las características de la SD-WAN y su funcionamiento, se procede a realizar la búsqueda de la mejor solución dada por las empresas socias de la empresa TICBRIDGE S.A.S., realizando una investigación en el portafolio de dichas empresas sobresalen principalmente dos soluciones: la primera de ellas Fortigate de la empresa Fortinet y la segunda SD-BRANCH de la empresa Aruba. De tal manera que se realiza la investigación de las dos soluciones y se escoge la mejor solución, teniendo en cuenta los objetivos del proyecto y las limitaciones de la propia infraestructura de la empresa.

4.2.2.2.1. Secure SD-WAN Fortinet

En el catálogo de Fortinet, empresa socia de TICBRIDGE S.A.S. se encuentra una solución para las SD-WAN, la cual se llama secure SD-WAN que se encuentra dentro de la línea de dispositivos llamados fortigate , esta cuenta con un gran catálogo de herramientas tanto para la implementación de una SD-WAN y para la seguridad de la misma red, ya que al hacer uso de varios enlaces de red diferentes se requieren soluciones de seguridad específicas para cada enlace como lo son las VPN (red privad virtual); por ejemplo para evitar que al hacer uso de internet público no se generen amenazas para la red.

Secure SD-WAN cuenta con una arquitectura específica, a continuación, sus componentes:

- FortiGate NGFW (New Generation Firewall): Protege de ataques y amenazas tanto a la red como la central de datos.
- FortiManager: Permite realizar una administración centralizada de la red con el fin de mejorar los flujos de trabajo y la detección de amenazas desde un solo dispositivo.
- Fortinet SD-WAN: Permite el despliegue y control de la SD-WAN.
- FortiAnalyzer: Administra los registros y la seguridad basado en el análisis.
- FortiDeploy for Zero-touch Provisioning (ZTP): Utilizado para la apropiada Configuración e implementación de los dispositivos de Fortinet desde el inicio con el fin de garantizar que se puedan realizar dichas configuraciones con la menor complejidad. [8]

Los componentes mencionados anteriormente más algunos necesarios para la implementación de una SD-WAN y su correcto control, se pueden observar en la siguiente imagen:

Figura 6. Secure SD-WAN tomado de [8].

Secure SD-WAN cuenta con una gran variedad de modelos tanto en hardware como en máquina virtual, con el fin de observar cual es la diferencia entre los modelos y concluir cual es el más adecuado para TICBRIDGE S.A.S., se realiza la investigación de los diferentes modelos.

Entre los dispositivos hardware de Fortinet destacan tanto Fortigate 100F, Fortigate 60F y Fortigate 40F.

Fortinet Products Comparison

Download PDF | Imprimir | Solicitar una propuesta

	FortiGate 100F	FortiGate 60F	FortiGate 40F
NGFW Throughput	1.6 Gbps	1 Gbps	800 Mbps
GW to GW IPSec VPN Tunnels	2500	200	200
VPN Performance	11.5 Gbps	6.5 Gbps	4.4 Gbps
1 GbE Interface	26	10	4
10 GbE Interface	2	0	0
Threat Protection throughput	1 Gbps	700 Mbps	600 Mbps
SSL Inspection throughput	1 Gbps	750 Mbps	310 Mbps
High availability configurations	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering
Virtual Domains	10/10	10/10	10/10

Figura 7. Comparación hardware.

Fortigate permite el acceso a máquinas virtuales, las cuales dada su naturaleza virtual agregan algunas aplicaciones, dichas aplicaciones se pueden observar en la siguiente imagen:

Figura 8. Máquina virtual tomado de [8].

Dichas máquinas virtuales se encuentran dentro del servicio de Fortiguard, hay gran variedad de estas las cuales cambian dependiendo del procesamiento que utilicen.

	VM-01/01V/01S	VM-02/02V/02S	VM-04/04V/04S	VM-08/08V/08S	VM-16/16V/16S	VM-32/32V/32S	VM-UL/ULV/ULS
Technical Specifications							
vCPU Support (Minimum / Maximum)	1 / 1	1 / 2	1 / 4	1 / 8	1 / 16	1 / 32	1 / unlimited
Storage Support (Minimum / Maximum)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	32 / 64	512 / 1,024	512 / 1,024	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096
Virtual Domains (Default / Maximum) *	10 / 10	10 / 25	10 / 50	10 / 500	10 / 500	10 / 500	10 / 500
Firewall Policies	10,000	10,000	10,000	200,000	200,000	200,000	200,000
Maximum Number of Registered Endpoints	2,000	2,000	8,000	20,000	20,000	20,000	20,000
Unlimited User License	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Figura 9. Comparación máquina virtual tomado de [9].

Independientemente si se implementa en máquina virtual o Hardware, Fortinet ofrece diferentes packs de servicios, los cuales están enfocados en la seguridad de la SD-WAN, dichos paquetes están diseñados para los diferentes tamaños de empresas, adicionalmente se debe resaltar que algunas aplicaciones como el fortimanager requieren de una mayor cantidad de productos de Fortinet para así conseguir obtener el mayor provecho posible de las aplicaciones.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	ASE [1]	24×7	24×7	24×7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video[2] Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard IoT Detection Service	•	•		
FortiGuard Industrial Service	•	•		
FortiConverter Service	•	•		
SD-WAN Orchestrator Entitlement	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
Fortinet SOCaaS	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

Figura 10. Paquetes de servicios de Fortinet tomado de [9].

Comparación dispositivos

Tomando en cuenta los valores de coste de los equipos tanto hardware como en máquina virtual con su respectivo descuento del 50% al ser TICBRIDGE S.A.S. socio de Fortinet, se procede a realizar la siguiente tabla comparativa con el fin de escoger cual es la más apropiada para ser implementada, cada uno de los dispositivos escogidos cuenta con la respectiva pack de servicios llamado Unified Threat Protection, el cual fue considerado el mejor teniendo en cuenta las necesidades en cuento a la seguridad de la empresa.

	Fortigate 40f +UTP	Fortigate 60f +UTP	Fortigate 100f+UTP	Fortigate VM-01 +UTP+1N	Fortigate VM-02 +UTP+1N	Foritgate VM-08 +UTP+1N
Rendimiento VPN	4.4 Gbps	6.5 Gbps	11.5 Gbps	1 Gbps	1.5 Gbps	5.5 Gbps
Rendimiento NGFW	800 Mbps	1 Gbps	1.6 Gbps	850 Mbps	1.5 Gbps	4.5 Gbps
Rendimiento contra amenazas	600 Mbps	700 Mbps	1 Gbps	700 Mbps	1.2 Gbps	3.5 Gbps
Precio (dólares)	$312,20	$438,34	$1.765,96	$6.593,71	$12.906,37	$25.830,74

Tabla 10. Comparación dispositivos Software.

De la anterior tabla se especifica que:

- UP: Bundle de unified protection
- 1N: 1 año de log en la nube

Luego de la comparación de los diferentes dispositivos se decidió que el dispositivo que debía ser adquirido, seria implementado físicamente, por lo cual se realiza la investigación física de los diferentes objetos y así seleccionar el mejoramiento, en la siguiente tabla se puede observar la diferencia entre las interfaces de los dispositivos hardware:

Fortigate 40F	Fortigate 60F	Fortigate 100F
* 1x USB Port * 1x Console Port * 1x GE RJ45 WAN Port * 1x GE RJ45 FortiLink Port * 3x GE RJ45 Ethernet Ports	*1x USB Port * 1x Console Port * 2x GE RJ45 WAN Ports * 1x GE RJ45 DMZ Port * 2x GE RJ45 FortiLink Ports * 5x GE RJ45 Internal Ports	* 1x USB Port * 1x Console Port * 2xGERJ45 MGMT/DMZ Ports * 2x GE RJ45 WAN Ports * 2x GE RJ45 HA Ports * 12x GE RJ45 Ports * 2x 10 GE SFP+ FortiLink Slots * 4x GE SFP Slots * 4x GE RJ45/SFP Shared Media Pairs

Tabla 11. Comparación dispositivos Hardware.

Por último, se pudo observar que el elemento escogido que mejor se aproximaba a los requerimientos de la empresa tanto por su rendimiento, precio y características físicas, era el Fortigate 60F principalmente porque cumplía con las necesidades en cuanto a rendimiento de una SD-WAN en la empresa, su precio se ajusta a lo requerido y el número de interfaces son las necesarias para la empresa.

4.2.2.2.2. ARUBA SD-BRANCH

Aruba SD-BRANCH es la solución más completa de Aruba para las empresas que cuentan con un gran número de sucursales, de tal manera que esta solución está diseñada desde cualquier elemento que se pueda encontrar en la red hasta control y manejo de SD-WAN, también cuentan con su propia solución en la nube como lo es Aruba central la cual puede ser utilizada para la gestión y control de todas las redes presentes en la infraestructura.

Entre los dispositivos que ofrece Aruba se encuentran los siguientes:

- Puntos de acceso: son compatibles con wifi5 y wifi6, con una gran adaptabilidad para los diferentes trabajos, utilizan inteligencia artificial para mejorar la administración y los diferentes componentes, por último, utilizan WPA3 y Enchanced Open en los datos para aumentar la seguridad en la red.
- Switches de agregación: Aruba maneja una gran variedad de switches, los cuales son utilizados para una actividad específica como lo son los switches de acceso, estos son utilizados para la conexión de diferentes puntos de acceso y cableado, switches de agregación utilizados comúnmente para redes de campus, los cuales se encargan de la interconexión de switches de acceso y por ultimo están los switches centrales los cuales son encargados de agregar tráfico en la capa de distribución en redes muy grandes.
- Gateway y controladores Aruba: realizan el control de tráfico por lo cual enrutan los datos, controlan el tráfico y permiten la segmentación dinámica todo esto con altos niveles de seguridad debido a su firewall y a sus múltiples herramientas para la unificación de la aplicación de políticas en las redes de diferente tipo.

Con Aruba central se logra realizar una gestión en cuanto a infraestructura basada en la nube ejecutando las siguientes acciones:

- Realizar instalación, configuración y mantenimiento de una forma sencilla y para múltiples tipos de redes.
- Utilizar inteligencia artificial con el fin de predecir y detectar problemas en la red antes que el usuario final se dé cuenta.
- Ser compatible con varios otros sistemas en la nube y permitir la personalización de características de seguridad o administrativas.

En cuanto a la seguridad, Aruba ofrece un catálogo de seguridad ya sea en cuanto al hardware o en el Aruba central.

- Access control: Aruba central tiene su propio sistema de identificación basado en usuarios y contraseñas, los cuales cuentan con sus propios roles y actividades dentro de la plataforma.

- Auditorias de seguridad: En cuanto a la identificación Aruba central guarda un registro de los procesos realizados por los usuarios en la plataforma, dichos registros pueden ser utilizados para procesos de auditoria internos.
- Encriptación: Todos los datos que son encriptados con TLS 1.2. de extremo a extremo con el fin de mejorar la seguridad por todos los usuarios. [10]

4.2.2.2.2.1. Precios productos Aruba

Con el fin de obtener unas cotizaciones de los equipos necesarios para la implementación de la SD-Branch para cada una de las sedes de TICBRIDGE S.A.S., se hace un reconocimiento de los dispositivos, los culaes se pueden observar a continuación:

- Un (1) Aruba 7010 (RW) Controller para la sede central.
- Un (1) Aruba 9004(RW) para una sede.
- Un (1) Aruba 9004(RW) LTE para una sede con requerimientos de conexión a redes móviles.
- Una licencia de Aruba central cloud para la administración de la SD-BRANCH.
- Tres (3) Switches Aruba 6300M 24G 4SFP56, para cada una de las sedes.
- Puntos de acceso Aruba AP-505.
- Un (1) Aruba Clearpass c100 s-1200 R4 HW Appliance con su repsectiva licencia "Aruba Clear Pass Policy Manager", para la gestión de seguridad.

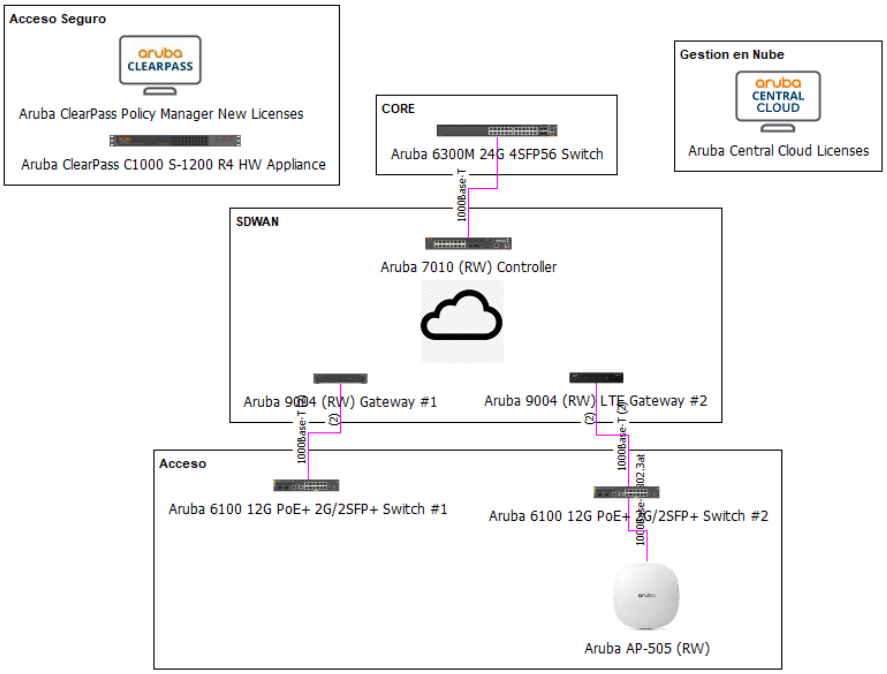

Figura 11. Arquitectura para implementación de SD-BRANCH.

De los productos anteriormente mencionados, hay que tener en cuenta que algunos ya se encontraban dentro de las instalaciones como lo son los switches y los diferentes Puntos de Acceso. Por lo cual su adquisición no es obligatoria. Teniendo lo anterior en cuenta en la siguiente tabla se puede observar el precio de los dispositivos necesario para la implementación de una SD-BRANCH con tres sedes:

Linea	N° Parte	Descripcion	Cant.	Vlr. Unitario	Vlr. Total Venta
Acceso					
1.0	JL679A	Aruba 6100 12G CIA 2SFP+ 139W Switch	2	USD 589,48	USD 1.178,93
1.1	JL679A ABA	INCLUDED: Power Cord - US. Localization	2	USD -	USD -
1.2	HY2K5E	Aruba 1Y FC NBD Exch 6100 12G CIA SVC [for JL679A]	2	USD 126,96	USD 253,91
2.0	R2H28A	Aruba AP-505 (RW) Unified AP	1	USD 337,10	USD 337,10
2.1	H9V9E	Aruba 1Y FC NBD Exch AP-505 SVC [for R2H28A]	1	USD 23,23	USD 23,23
2.2	R3J13A	AP-MNT-D AP mount bracket individual D1 solid surface	1	USD 16,47	USD 16,47
		Acceso Subtotal			USD 1.387,47
Acceso Seguro					
3.0	JZ509A	Aruba ClearPass C1000S-1200 R1 HW Appliance	1	USD 4.994,39	USD 4.994,39
3.1	H9TT3E	Aruba 1Y FC NBD Exch CPCHS1200HWAppl SVC [for JZ	1	USD 1.995,53	USD 1.995,53
4.0	JZ400AAE	Aruba ClearPass NL AC 100 CE E-LTU	1	USD 2.457,45	USD 2.457,45
4.1	H9WT2E	Aruba 1Y FC SW CP NL AC 100 CE E-L SVC [for JZ400AA	1	USD 231,51	USD 231,51
4.2	JZ436AAE	Aruba ClearPass NL CM 100 USR E-LTU	1	USD 2.457,45	USD 2.457,45
4.3	H9WY2E	Aruba 1Y FC SW CP NLCM100 USR E-L SVC [for JZ436AA	1	USD 231,51	USD 231,51
4.4	JZ472AAE	Aruba ClearPass NL OG100 EP E-LTU	1	USD 1.579,79	USD 1.579,79
4.5	H9WR2E	Aruba 1Y FC SW CP NL OG100 EP E-L SVC [for JZ472AA	1	USD 156,83	USD 156,83
		Acceso Seguro Subtotal			USD 13.874,96
CORE					
5.0	JL664A	Aruba 6300M 24G 4SFP56 Switch	1	USD 5.122,10	USD 5.122,10
5.1	HL7G3E	Aruba 1Y FC NBD Exch 6300M 24 SVC [for JL664A]	1	USD 388,37	USD 388,37
5.2	JL085A	Aruba X371 12VDC 250W Power Supply	1	USD 439,53	USD 439,53
5.3	JL085A ABA	INCLUDED: Power Cord - US. Localization	1	USD -	USD -
		CORE Subtotal			USD 5.952,43
Gestion en Nube					
6.0	R4G91AAE	Aruba Central WLAN Gateway Foundation 3y Sub E-STU	3	USD 249,26	USD 747,77
6.1	Q9Y59AAE	Aruba Central AP Foundation 3y Sub E-STU	1	USD 169,95	USD 169,95
6.2	Q9Y69AAE	Aruba Central 25xx/6100/8-12p Switch Foundation 3y Sub	2	USD 379,15	USD 758,30
6.3	Q9Y79AAE	Aruba Central 63xx/83xx Switch Foundation 3y Sub E-STU	1	USD 1.092,66	USD 1.092,66
		Gestion en Nube Subtotal			USD 2.768,67
SDWAN					
7.0	R8R21A	Aruba 9004 (RW) Gateway	1	USD 1.888,57	USD 1.888,57
7.1	H9E8E	Aruba 1Y FC NBD Exch 9004 Gtwy SVC [for R8R21A]	1	USD 191,68	USD 191,68
7.2	JW124A	PC-AC-NA Nordic America AC Power Cord	1	USD 3,33	USD 3,33
7.3	R4D94AAE	Aruba 9xxx Gateway Foundation Base plus Security 3yr Su	1	USD 1.689,11	USD 1.689,11
8.0	R3V90A	Aruba 9004 (RW) LTE Hourly Gateway	1	USD 1.488,74	USD 1.488,74
8.1	H8R2A5E	Aruba 1Y FC NBD Exch 9004 LTE SVC [for R3V90A]	1	USD 235,66	USD 235,66
8.2	JW124A	PC-AC-NA Nordic America AC Power Cord	1	USD 3,33	USD 3,33
8.3	R4D94AAE	Aruba 9xxx Gateway Foundation Base plus Security 3yr Su	1	USD 1.689,11	USD 1.689,11
9.0	JW678A	Aruba 7010 (RW) 16p 150W PoE+ 10/100/1000BASE-T 1G-1	1	USD 3.197,49	USD 3.197,49
9.1	H3AM9E	Aruba 1Y FC NBD Exch 7010 Chsis SVC [for JW678A]	1	USD 501,15	USD 501,15
9.2	JZ122AAE	Aruba 7xxx or 9xxx Gateway Advanced 3yr Sub E-STU	1	USD 3.429,19	USD 3.429,19
		SDWAN Subtotal			USD 13.791,36
		SUBTOTAL			USD 36.835,88
		IVA			USD 6.998,82
		TOTAL			USD 43.834,70

Figura 12. Cotización SD-BRANCH.

4.2.2.3. Implementación Fortigate

Luego de realizar el estudio de las diferentes cotizaciones y de las diferentes soluciones de SD-WAN se opta por la solución de Fortinet por encima de la de Aruba, esto debido a que esta solución se enfoca más a la seguridad y no se requiere la adquisición de un gran número de dispositivos para su despliegue.

Adicionalmente, al observar las diferentes características de los dispositivos ofrecidos por Fortinet se llegó a la conclusión que el dispositivo a adquirir debería ser el Fortigate 60F, ya que cuenta con el número de interfaces como el procesamiento requerido por la empresa.

Para la implementación del Fortigate 60F, lo primero que se realiza es la conexión de este dispositivo tanto a el respectivo Router que suministra el servicio de internet vía una empresa proveedora (movistar), como a un PC el cual será el encargado de entrar vía el entorno web para la configuración, el proceso anteriormente mencionado se puede observar en la siguiente imagen:

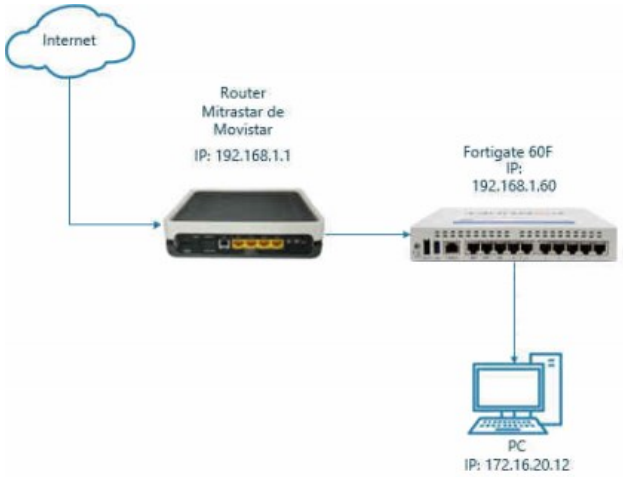

Figura 13. Configuración Fortigate.

Lo primero a realiza es revisar el correcto direccionamiento en el puerto de Ethernet del computador por medio del comando ipconfig (comando que da información de cada adaptador enlazado con TCP/IP) de tal manera que se pueda obtener la respectiva dirección IP del dispositivo Fortigate.

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::7cb3:6550:23f2:6ea3%12
   Dirección IPv4. . . . . . . . . . . . : 192.168.1.60
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.0.0.1
```

Figura 14. Adaptador Ethernet.

Luego desde el computador se ingresa vía entorno web la respectiva dirección IP del dispositivo Fortigate (192.168.1.60) con el fin de realizar la respectiva configuración, ya dentro del entorno web se ingresan las credenciales por defecto de administración del dispositivo, en este caso se ingresa en usuario admin y en contraseña no se escribe ningún carácter.

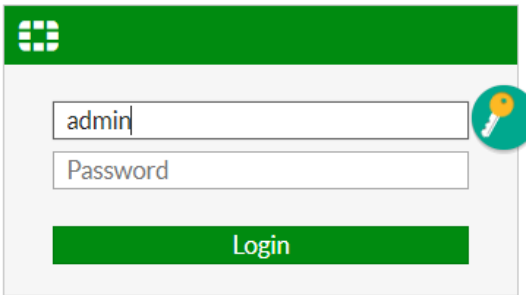

Figura 15. Ingreso a la interfaz web.

Posteriormente se registra tanto en Forticloud como FortiCare con el fin de obtener soporte y cubrimiento en caso de fallas. Se hacen algunas configuraciones básicas como el nombre que tendrá el dispositivo y la configuración del dashboard.

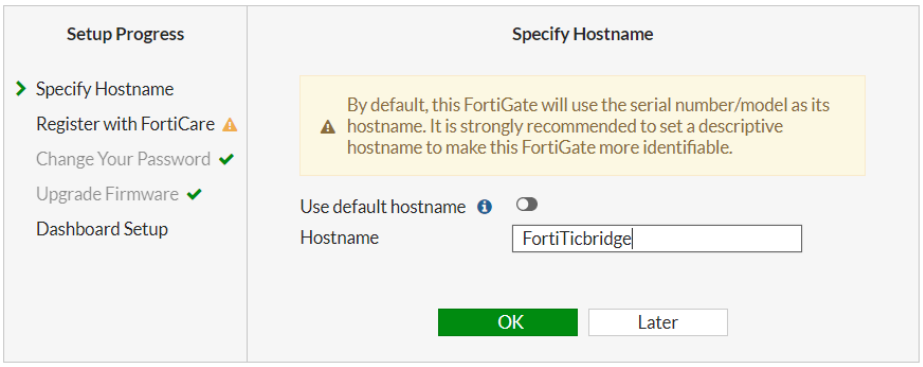

Figura 16. Forticare.

Luego Ingresa a las configuraciones del sistema, en donde se realiza la configuración del tiempo, se activa el servidor NTP (Protocolo de internet para sincronizar la hora de los dispositivos), se selecciona fortilink para las interfaces, ya que este permite a los puertos ser extensiones de los servicios de seguridad de Fortinet y por último se seleccionan los respectivos puertos tanto para HTTP como HTTPS.

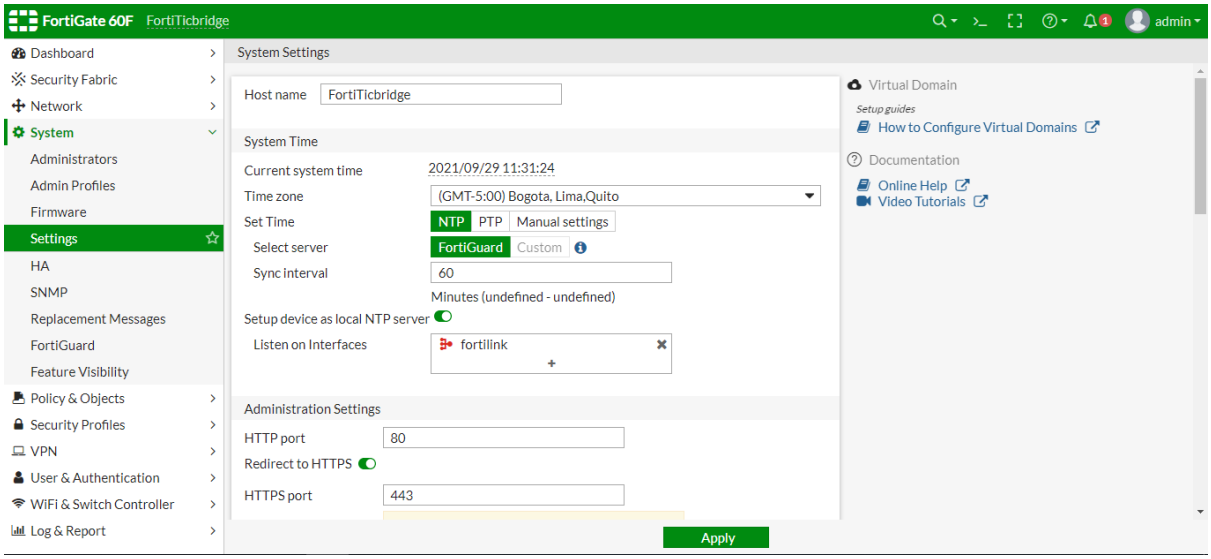

Figura 17. Configuración del sistema.

Ya teniendo las respectivas configuraciones del sistema, se procede a la respectiva edición de interfaces en donde se cambia el direccionamiento IP del port1 para que sea aplicada a la red interna (LAN). Para que el cambio sea transparente a capa 3, se le deja el mismo segmento de red utilizado anteriormente, por lo cual se selecciona la misma dirección IP (172.16.20.6) y mascara (255.255.255.0) del dispositivo linksys que anteriormente utilizaba como Gateway en la empresa.

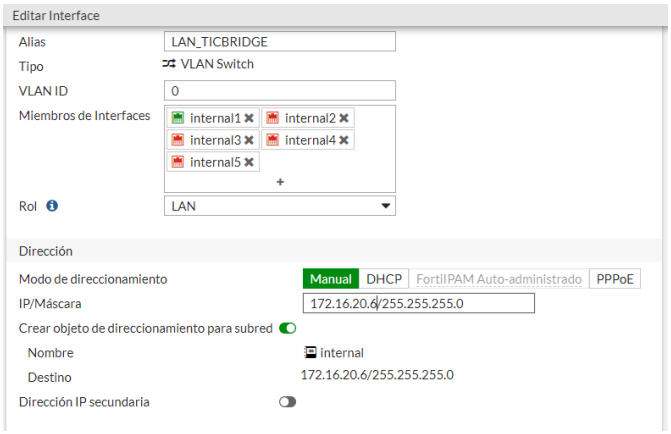

Figura 18. Edición de interfaces.

Teniendo en cuenta lo anterior se hace la configuración para el acceso administrativo donde se ingresan los respectivos protocolos de IPV4, esta parte es muy importante, ya que dependiendo de los respectivos protocolos que sean activados se podrá realizar el ingreso al entorno administrativo del dispositivo Fortigate, en este caso se priorizan los protocolos HTTPS Y HTTP ya que con estos se puede realizar la administración por el entorno web.

Luego se toma la configuración VDOM para recibir y transmitir LLDP (protocolo de capa dos el cual permite tener información de los dispositivos cercanos), se escoge VDOM porque es el protocolo de detección de propio de la empresa Fortinet.

Por último, se realiza la configuración del servidor DHCP (servidor encargado de proveer a los dispositivos conectados una determinada dirección IP), de tal manera que se deja el mismo rango que el dispositivo Gateway anterior (172.16.10.100-172.16.20.249), la máscara (255.255.255.0), la puerta de enlace, el servidor DNS y tiempo de asignación.

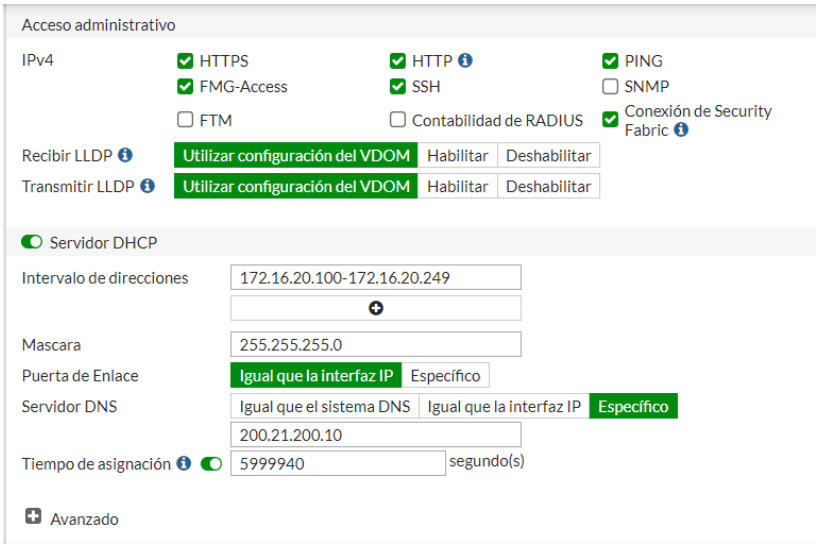

Figura 19. Acceso administrativo.

Se configura la interfaz WAN para que el dispositivo tenga acceso a internet, de tal manera que se usa la interfaz Wan1 y se le da el nombre de puerto_Movistar, ya que esta ira directamente conectada con el Router de dicho proveedor. Esta interfaz se pone en el mismo segmento que el router ISP de Ticbridge de tal manera que queda configurado con la IP de 192.168.1.15 y mascara de 255.255.255.0.

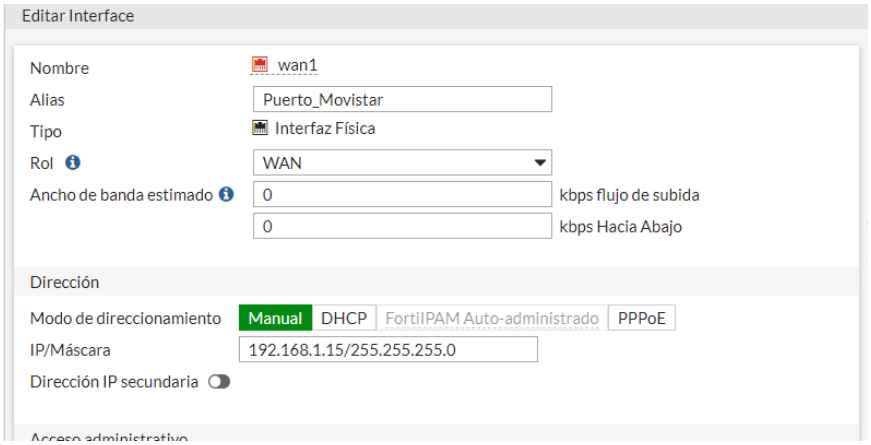

Figura 20. Configuración Fortigate.

También se configuran las rutas estáticas del dispositivo, de tal manera que se da la dirección del puerto de enlace, el cual está directamente ligado con el Router del proveedor Movistar, la respectiva interfaz y la distancia administrativa.

Figura 21. Configuración Fortigate.

Por último, se configuran las políticas de conexión, donde se escogen las interfaces de entrada (LAN_Ticbridge) y salida (Puerto_Movistar) Todo esto con el fin de que se pueda acceder desde la red interna de la empresa a internet y se puedan inspeccionar posibles amenazas que transiten por la red.

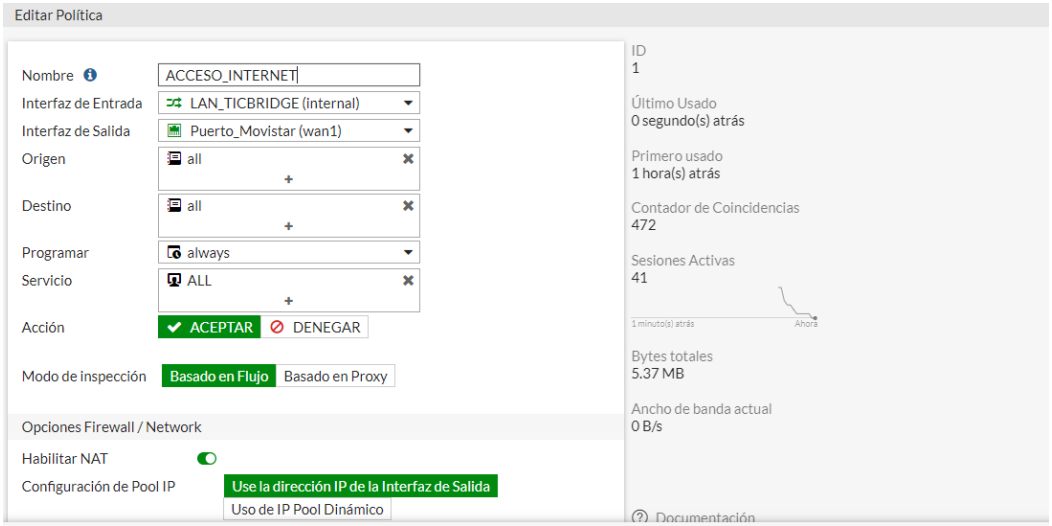

Figura 22. Configuración Fortigate.

4.2.2.4. Prueba FORTIGATE 60F

Con el fin de comprobar que se realizó adecuadamente la configuración del dispositivo Fortigate 60F se hace uso del comando PING, el cual permite establecer si hay una conexión adecuada con la dirección deseada, dichos PING se envían desde un dispositivo puesto en la red administrativa (VLAN 20) a direcciones dentro de la red administrativa como fuera de la red Local.

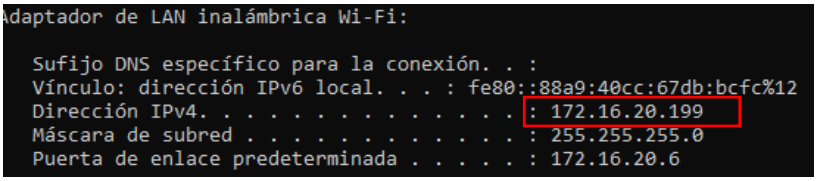

Figura 23. Dirección IP del dispositivo de prueba.

Se envía un Ping a los AP1 (IP: 172.16.20.12)y AP2 (IP: 172.16.20.12) con el fin de comprobar que estos tienen conexión y si logran proveer de W-Fi a los diferentes dispositivos inalámbricos que se encuentran en la sede.

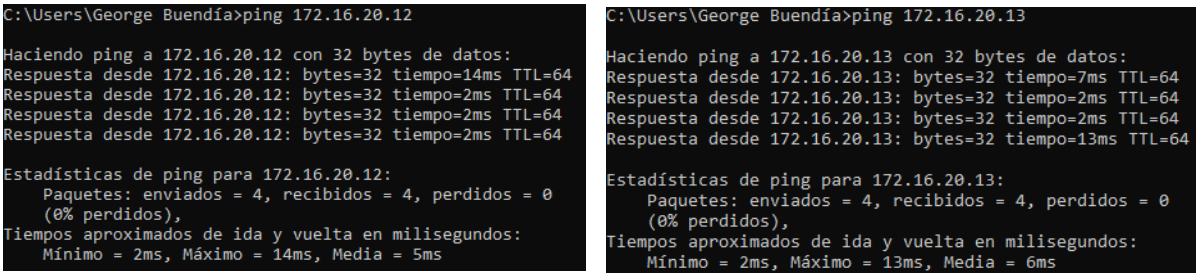

Figura 24. Prueba Fprtigate60F con los AP.

Luego se envía un PING a el dispositivo Fortigate 60F (IP: 172.16.20.6) con el fin de determinar si se puede establecer conexión de forma correcta y si queda configurado con la dirección establecida anteriormente.

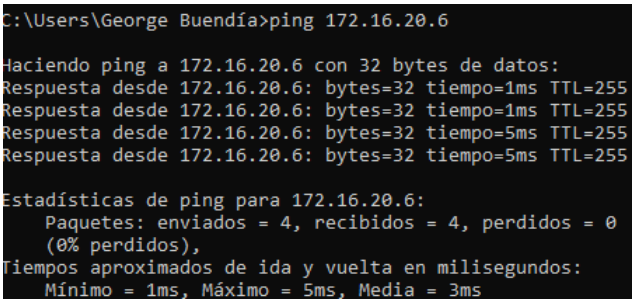

Figura 25. Prueba Fortigate60F con fortigate 60F.

Por último, se envía un Ping a una dirección externa como los es la de la página web de Google (142.250.78.46) con el fin de que la función SD-WAN del Fortigate 60F funcione adecuadamente y que este direccionando a puntos de internet externos mediante los enlaces que se encuentran configurados.

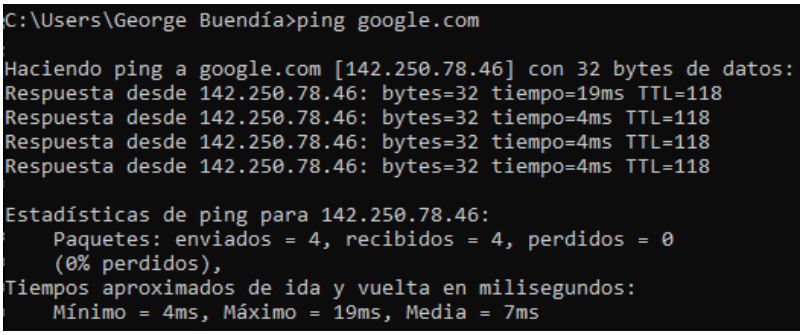

Figura 26. Prueba Fortigate60F con página web.

4.3. Mejoras seguridad

4.3.1. Estado actual

Con el fin de determinar cuáles son las herramientas utilizadas anteriormente dentro de la empresa TICBRIDGE S.A.S. para la seguridad informática se realiza un levantamiento de los proyectos anteriormente desarrollados, adicionalmente se realiza un estudio en algunas vulnerabilidades teniendo en cuenta que estas pueden ser explotadas para dañar el funcionamiento de la empresa.

4.3.1.1. Levantamiento de documentos

Dentro de los documentos investigados se determinó que se han implementado varias estrategias y modificaciones que aumentan la seguridad de la red local de la sede principal de TICBRIDGE S.A.S. de manera directa o indirecta, dichas modificaciones y estrategias se mencionan a continuación:

- Se instaló un router adicional a la entrada de la red con el de que este fuera el encargado de recibir el tráfico entrante, mejorando la seguridad de la empresa, con esto se consigue realizar un mejor control de tráfico. Adicionalmente se observó en la sección de estado actual de la red, que esta se encuentra segmentadas en 3 VLAN diferentes las cuales mejoran el tráfico dentro de la sede y adicionalmente dificulta el acceso a determinados dispositivos ante un ataque a la red. [1]
- En los dispositivos de la compañía se encuentran instalado un antivirus llamado Kasperky, el cual es comprado como solución de la empresa, sus principales características son:

    - **Protección contra ramsomware**: Kasperky cuenta con su propio sistema de Back Up que evita que, si dado el caso algún equipo se encuentra secuestrado por un programa malicioso, la información que se encuentre en este pueda ser recuperada, adicionalmente kasperky cuenta con su propio filtro web el cual está diseñado para evitar que los empleados ingresen a paginas maliciosas en la red.

    - **Multiplataforma**: Dado que se busca que la seguridad sea implementada para todas las facetas del trabajo, Kasperky está diseñado para asegurar cualquier dispositivo, ya sean computadores de los diferentes sistemas operativos, smarthphones o tablets.

- **Transacciones confiables:** Adicionado al filtro web tradicional, kasperky tiene una función enfocada en el acceder de forma segura a las páginas bancarias y a cualquiera en la que se vaya a realizar una transacción monetaria.

- **Administrador de contraseñas:** Cuenta con su propio programa para la administración de contraseñas y a su vez hacer uso de un gran número de contraseñas, evitando que individuos puedan entrar a las cuentas empresariales por medio del conocimiento de contraseñas.

- La implementación de políticas de seguridad y Back-Up, se basan en realizar un almacenamiento periódico de los dispositivos para evitar un posible ataque o problemas en los dispositivos logrando que se pierda información y por ende el funcionamiento de la empresa se vea afectado.
  Para la implementación de políticas de seguridad y Back-Up se realizaron tres procedimientos específicos como los son:

  - Sincronización de documentos y carpetas de uso empresarial en el OneDrive de la empresa.
  - Sincronización de la información presente en cada equipo de la sede de Bogotá con el servidor NAS mediante la aplicación QSync.
  - Integración y administración de usuarios mediante la creación de un Active Directory.
  -

4.3.2. Estudio de Solución

Tomando en cuenta los elementos adquiridos y sus diferentes características se procede a realizar un estudio de los diferentes atributos de los elementos que se van a utilizar, ya que se realizara un debido manejo de las diferentes aplicaciones y políticas que se pueden implementar.

4.3.2.1. NEXT GENERATION FIREWALL

Una de las características principales por las que se escogió la solución SD-WAN de FORTINET es por la solución enfocada en la seguridad de la red, esta solución cuenta con NEXT GENERATION FIREWALL (NGFW), el cual tiene un grupo de herramientas diseñadas para proteger la red de intrusos y de posibles ataques que pueden afectar el funcionamiento de la empresa.

En los dispositivos de Fortigate las funciones de NGFW funcionan como una unidad de procesamiento de seguridad con múltiples aplicaciones, mencionadas a continuación:

- **Fortimanager:** Permite realizar la administración centralizada de la seguridad de la red; es decir, se evidencia desde el estado de la misma red y los diferentes dispositivos que se encuentran conectadas a la mismas, este permite su vez poder realizar la debida administración de la SD-WAN y su respectivo monitoreo.
- **Fortianalyzer:** Dada la complejidad de algunas redes y la dificultad para estar en constante monitoreo Fortianalayzer ofrece una gran cantidad de informes acerca del estado de la red y las posibles vulneraciones que se encuentren en ella.

- **Control de aplicaciones:** Permite realizar un manejo de las aplicaciones a las cuales pueden ingresar los diferentes usuarios en la organización, esta función está unida al último modelo de procesamiento de Fortigate y aumenta la seguridad, ya que no solo protege puertos o direcciones, también el uso de diferentes aplicaciones que puedan generar problemas en la red.
- **Ips (prevención de intrusiones):** Fortigate contiene su propio sistema para evitar que se realice la intrusión de individuos no deseados a la red, teniendo en si diferentes 13000 diferentes firmas de IPS que contienen tanto vulnerabilidades como exploits conocidos, también este está diseñado para evitar y proteger de posibles ataques de día cero.
- **Antivirus**: detecta malware proveniente de alguna descarga o procedimiento dentro de los equipos de la red. A su vez tiene las herramientas para eliminar algunos de los más comunes virus y software espía.
- **Filtrado web**: distingue según las bases de datos de Fortinet cuáles son las páginas maliciosas y evitar su ingreso por medio de los dispositivos que se encuentren en la red. Este sistema puede ser ejecutado para evitar el ingreso a páginas específicas en la organización que puedan evitar su debido funcionamiento.
- **SSL inspection**: identifica y certifica los diferentes usuarios que entran a la red, así como los propios dispositivos.
- **Sandboxing:** Por medio de sandboxing se pone en cuarentena a los archivos que ya sean detectados como malware, por medio de una base de datos de fortinet como diferentes elementos que transiten por la red y sean sospechosos, esta herramienta al ponerlos en cuarentena permite que estos sean estudiados y se verifica si en realidad representan un peligro para la red. (Todo el procedimiento anteriormente mencionado se realiza en la nube)
- **Anti-botnet:** Dado el crecimiento de ataques basados en botnet y gusanos cada vez más sofisticados, Fortigate cuenta con su propio sistema de protección el cual evita que estos no solo ingresen al sistema por medio del reconocimiento de IP peligrosas.

Es importante mencionar que, aunque todas estas aplicaciones se encuentran dentro del NGFW algunas de ellas solo se activan con los paquetes de aplicaciones que se adquieren con el Fortigate.

4.3.3. Implementación de mejora

Luego de haber realizados las diferentes configuraciones en el Fortigate 60F se procede a realizar la debida configuración de los servicios a utilizar como el antivirus, filtro web, filtro DNS, control de aplicaciones, IPS e Inspección SSL y la configuración de para el acceso a la red de los rabajadores de TICBRIDGE S.A.S. mediante un portal y aplicativo VPN.

4.3.3.1. Perfiles de seguridad

El Fortigate 60F permite la creación y configuración de diferentes perfiles de seguridad con la respectiva implementación de varios servicios con los que cuenta, cada uno de estos perfiles debe se configuraron teniendo en cuenta las necesidades de la red propia de la empresa.

4.3.3.1.1. Antivirus

El antivirus es principalmente configurado con el fin de mejorar y evitar cualquier ataque, basado en el ingreso de elementos de maliciosos a la red, de tal manera que este funciona como filtro dentro de la red inspeccionando protocolos y el contenido de los elementos que se transfieren por ellos.

Se procede a crear un perfil de antivirus en el cual es nombrado “Antivirus_1” para el cual es necesario implementar las siguientes configuraciones:

- **Procedimiento para desarrollar cuando se detecten virus**: Bloquear.
- **Modo de inspección**: Basado en el flujo, ya que este es el modo de inspección más rápido, el cual evalúa los paquetes de forma superficial y no interrumpe la sesión TCP ente el usuario y el servidor.
- **Protocolos que inspeccionar**: Se escogen los protocolos HTTP, SMTP, POP3 y IMAP. Debido a que estos son protocolos que su inspección no generan ni retrasos en la red ni problemas en el funcionamiento interno normal de la empresa, en cambio los protocolos FTP Y CIF no son escogidos dado que estos son utilizados constantemente tanto para a actualización como para el mantenimiento de los equipos utilizados por la empresa y el inspeccionarlos generaría retrasos en la red de la empresa.
- **Configuración para amenazas APT(amenaza avanzada persistente):** Se activa la protección de malware para dispositivos móviles, dado que actualmente en la empresa se utilizan varios equipos inalámbricos a los cuales están constante evaluación para evitar que se realicen ataques a largo plazo, utilizando las vulnerabilidades de dichos dispositivos; En cambio no se hace uso de opción de manjar ejecutables de Windows adjuntos de E-mail como virus ya que permanentemente se hace uso de estos para la instalación o actualización de programas dentro de la empresa y activarlo generaría retrasos.

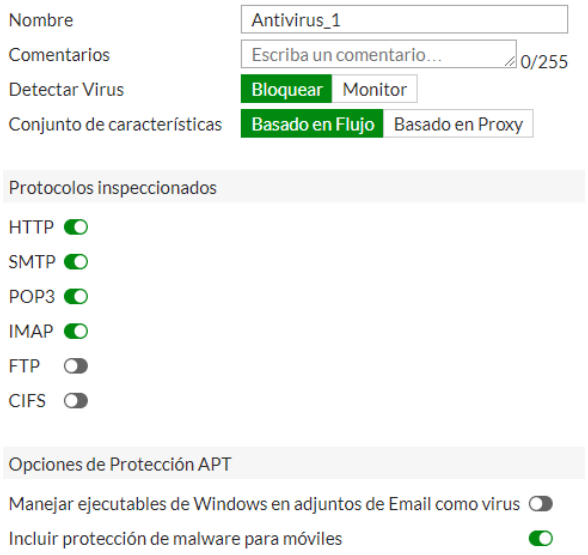

Figura 27. Configuración antivirus.

4.3.3.1.2. Filtro web

El filtrado web es utilizado principalmente para evitar que los usuarios de la red caigan en posibles ataques debido al ingreso a sitios web peligrosos, adicionalmente se pueden configurar políticas de acuerdo con el entorno laboral evitando el ingreso a los empleados a ciertas páginas web que no se relacionada con el trabajo propio de la empresa.

De tal manera que se crea un perfil de configuración web con el nombre “Webfilter1” con las siguientes configuraciones:

- **Método de inspección**: Igual que en el perfil de antivirus se escoge que sea basado en flujo principalmente por su rendimiento en comparación con el basado en proxy.
- **Habilitación si el filtro es basado en categorías Fortiguard:** Se habilitan y seleccionan las categorías de Fortiguard, las cuales cuentan con un gran número de páginas web previamente seleccionadas y así se evita seleccionar página por página, adicionalmente para cada categoría se puede seleccionar el procedimiento a realizar para cada categoría ya sea si se desea monitorear, alertar, autenticar, permitir o bloquear.
  Las categorías escogidas tanto para alerta y bloquear principalmente son:

  -**Potencialmente riesgoso:** Páginas relacionadas con actividades como Hacking, Evasión de proxies y Abuso de drogas.
  -Contenido para adulto: Páginas relacionadas con actividades como apuestas alcohol y venta de armas.
  -Violación de seguridad: Páginas relacionadas con actividades como Pishing, DNS dinámico y sitios web maliciosos.

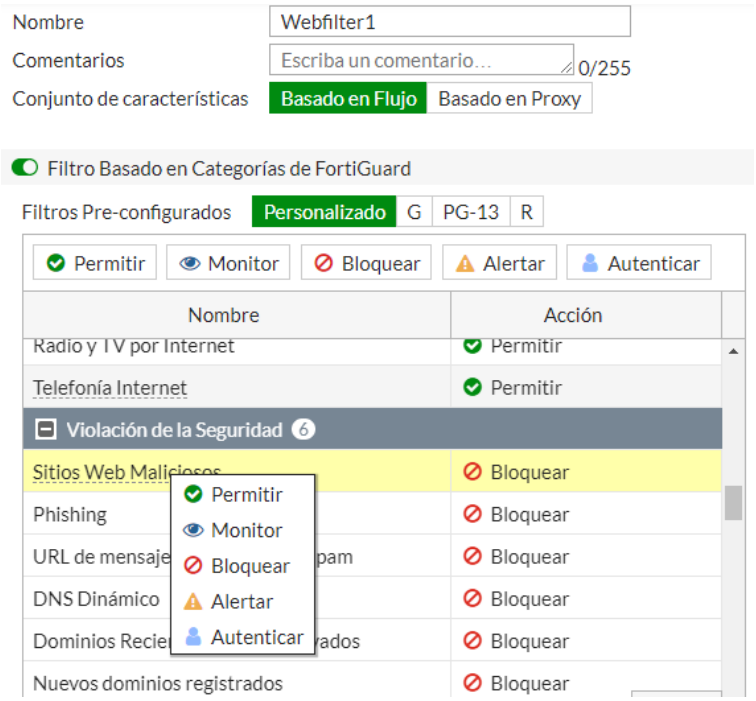

Figura 28. Configuración filtro web.

4.3.3.1.3. Filtro DNS

El filtro DNS cumple las mismas funciones que el filtro web, se diferencian en este caso este se encarga de clasificar y bloquear de dominios específicamente, se procede a realizar la creación de un perfil llamado “filtroDNS_1” para el cual se realiza la siguiente configuración:

- Habilitar el filtro basado en categorías de Fortiguard, Dichas categorías son muy parecidas a la del filtro web, as acciones a realizar con dichas categorías en este caso son únicamente permitir, monitorear y bloquear. Las categorías seleccionadas son las siguientes:

- **Contenido para adulto**: Categoría de dominios relacionados con contenido como venta de armas, desnudez y marihuana.
- **Potencialmente riesgoso:** Categoría de dominios relacionados con contenido como violencia explícita, grupos extremistas y abuso de drogas.
- **Violación de seguridad: Categoría** de dominios relacionados con contenido como Phisisng, sitios web maliciosos y DNS dinámico.

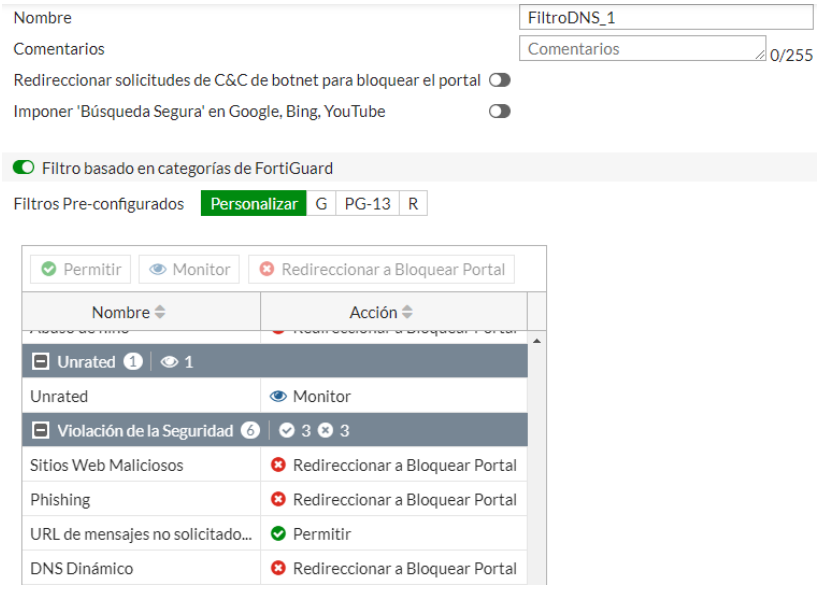

Figura 29. Configuración filtro DNS.

4.3.3.1.4. Control de aplicaciones

Para el control de aplicaciones se tuvo un enfoque especial, ya que se debe tener en cuenta que hay varias aplicaciones que se utilizan en TICBRIDGE S.A.S. que, aunque el sistema lo pueda definir como peligroso, pero no lo son, como se evidencio durante la pasantía con la aplicación AnyDesk, el cual es utilizado para el acceso a los dispositivos de manera remota, de tal manera que dicho perfil es desactivado ya que mucha de las categorías contienen aplicaciones utilizadas en la empresa.

Para la configuración de dicho perfil de control de aplicaciones.

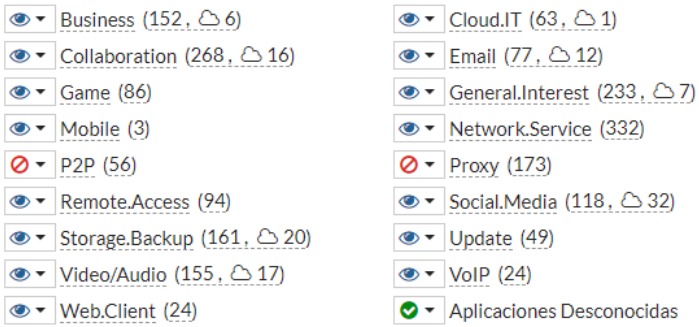

Figura 30. Categorías control de APP.

4.3.3.1.5. Prevención de intrusiones

La prevención de intrusiones es una herramienta muy valiosa, gracias a esta se logra evitar que a la red ingresen individuos no deseados, para su configuración se pueden agregar firmas relacionadas con atacantes no conocidos; A la hora de realizar la pasantía no se encontraba con una base de datos de individuos no deseados por TICBRIDGE S.A.S. por lo cual se activa el perfil por defecto, el cual ya cuenta con una gran base de datos de firmas de individuos maliciosos detectados por Fortinet.

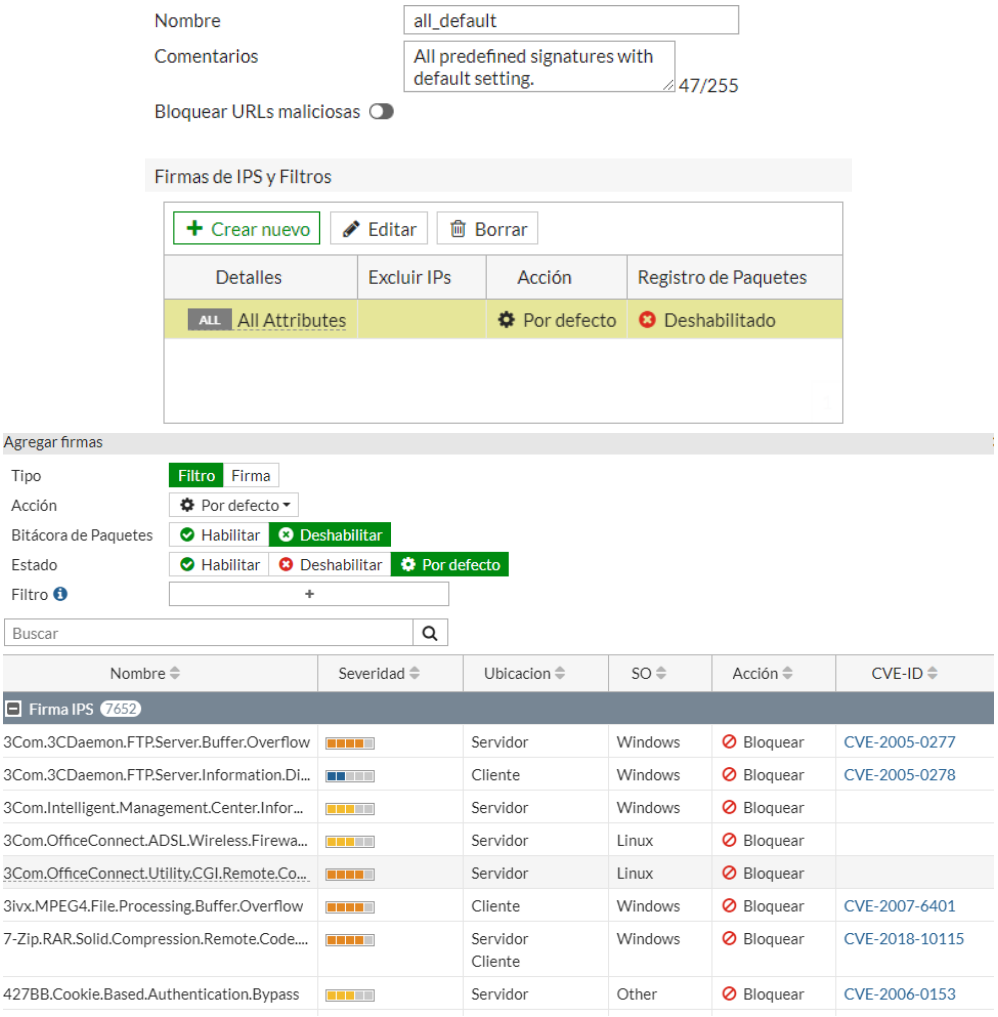

Figura 31. Configuración por defecto de prevención de intrusiones.

4.3.3.2. Prueba perfiles de seguridad

Con el fin de probar que algunos de los perfiles creados estén funcionando adecuadamente se procede a realizar a debida prueba, en este caso se realiza la prueba del perfil tanto de filtro web como de DNS, ya que ambos cuentan con el perfil similares, a la prueba se intentara ingresar a la página Wplay,com, la cual se encuentra dentro de las páginas y dominios bloqueados dentro de la categoría de apuestas.

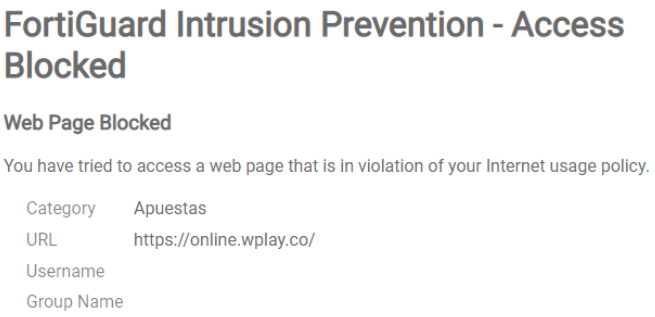

Figura 32. Prueba filtro web.

Como se puede observar al intentar ingresar el firewall bloquea el ingreso a la página e imprime en pantalla un mensaje de la razón por la cual la página se encuentra bloqueada.

4.3.3.3. Implementaciones políticas de seguridad

Con el fin de hacer uso de los diferentes perfiles de seguridad creados se hace uso de una política de seguridad con la cual se permita el acceso a internet a las personas que hacen parte de la empresa, adicionalmente se activa la central SNAT en la cual también habrá que crear políticas de acceso para poder definir cuáles serán las direcciones de origen que deben ser modificadas.

Se crea la respectiva política de seguridad en este caso se seleccionan las respectivas interfaces tanto de entrada como de salida, origen, destino, el método de inspección. Adicionalmente se seleccionan los diferentes perfiles de seguridad en los cuales se hará uso de las políticas anteriormente creadas.

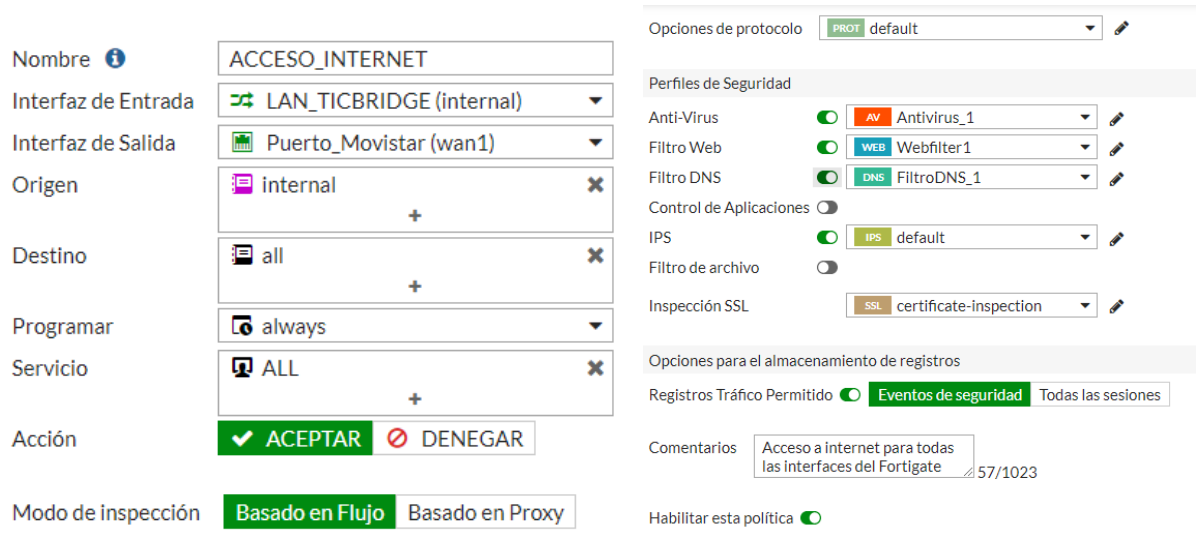

Figura 33. Configuración política de seguridad.

En cambio, para la configuración de la central SNAT únicamente es necesario realizar la respectiva activación y selección de las interfaces para la conexión, en este caso serán las misma seleccionadas para las políticas de seguridad.

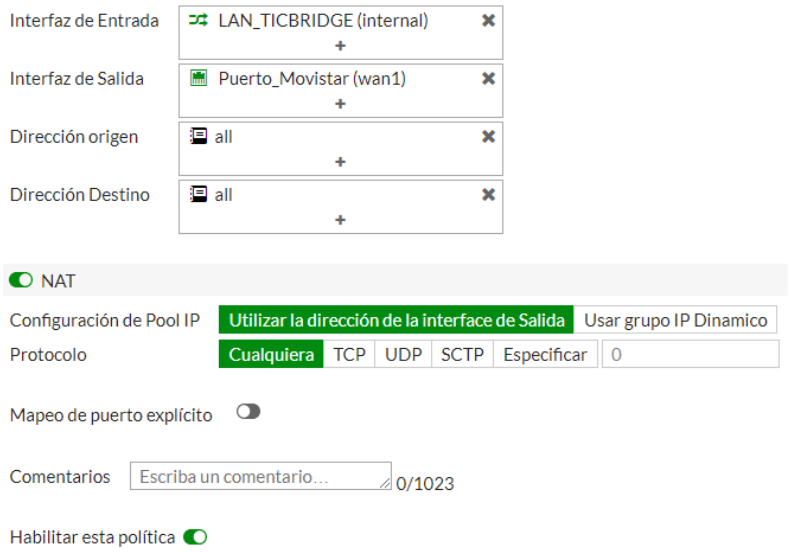

Figura 34. Configuración SNAT.

4.3.3.4. Implementación VPN

Teniendo creados los respectivos perfiles de seguridad y las políticas de seguridad para la empresa, se procede a realizar la debida configuración para el ingreso a la red por medio de una VPN.

Para dar inicio se crean grupos y usuarios para que puedan acceder a la VPN. Para la creación de los grupos es necesario seleccionar el tipo de grupo en este caso se crea uno tipo firewall con el fin de proteger la red y la VPN; Posteriormente se crean los usuarios ingresando su nombre, contraseña y escoger al grupo al cual se encuentran.

Figura 35. Creación de usuarios y grupos en para la VPN.

Luego se realiza la configuración para el ingreso a al portal de la VPN en este caso dado que para el uso de la VPN se requiere de un IP publica fija que direccione a una IP privada y el proveedor de servicios de movistar en el momento de solicitarlo no prestaba este servicio; se contrató el servicio de internet y IP publica fija a la empresa ETB los cuales se ingresaran al Fortigate en la interfaz wan2 (se realiza el mismo proceso mencionado en la sección de mejoras de la red con la interfaz WAN1).

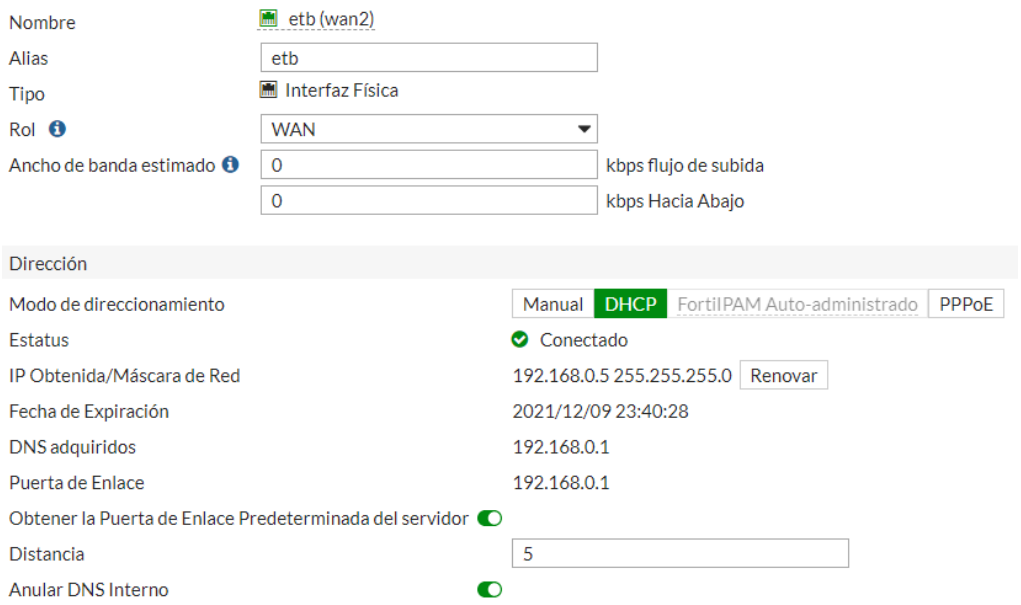

Figura 36. configuración interfaz wan2.

También fue necesario crear la respectiva política para permitir el acceso a internet mediante esta interfaz y cambiar la configuración de DNS debido a que ahora era necesario hacer uso de un servidor público como el de Google que permitiera el acceso a internet sin importar el proveedor que se utilizara.

Adicionalmente se selecciona el puerto a utilizar el puerto que se utilizará, dado que actualmente se utilizaba el puerto 443 para la administración del Fortigate se procede a seleccionará el puerto 10443.

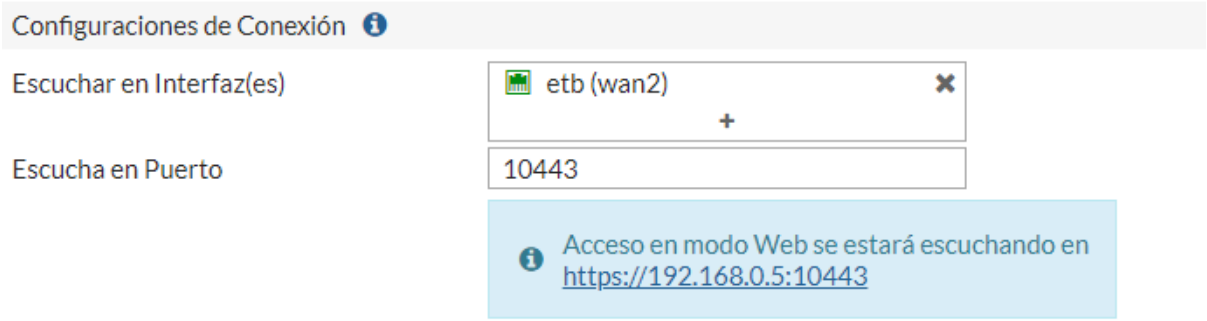

Figura 37. Creación de usuarios y grupos en para la VPN.

Posterior a esto se seleccionan las direcciones IP que se otorgarán a los usuarios vía la VPN en este caso se escoge el predeterminado por la empresa Fortinet y se selecciona el grupo de usuarios que podrán hacer uso del portal VPN.

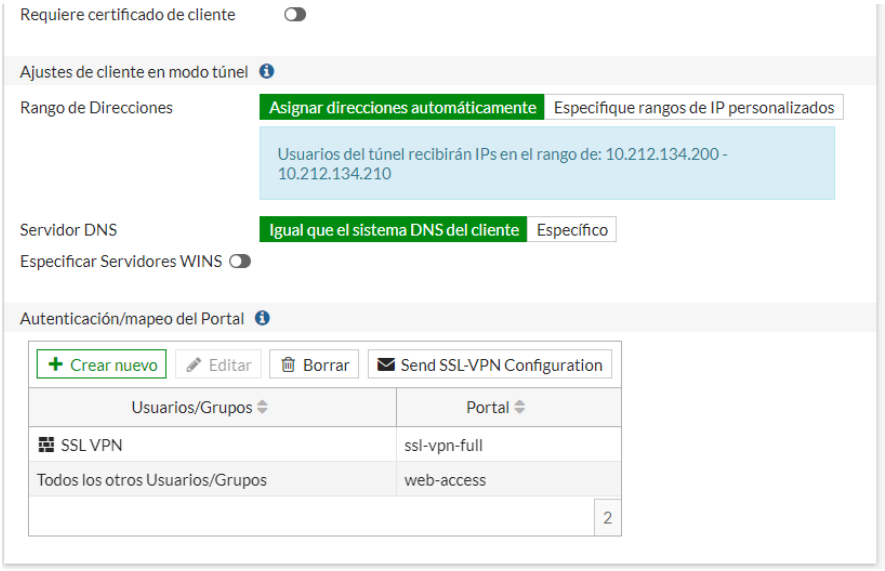

Figura 38. Asignación de direcciones y grupos para el portal de la VPN.

Para la configuración del portal VPN se debe dar un respectivo nombre, la dirección de enrutamiento y el grupo de IP de orígenes, en este caso el enrutamiento se realizaría a una red interna a la cual se ingresará con las direcciones de origen del grupo predeterminado de SSLVPN_TUNNEL_ADDR1 (10.212.134.200-10.212.134.210)creado por default para este tipo de configuraciones, adicionalmente se seleccionan los permisos a los usuarios que hagan uso del portal principalmente en este caso se escoge que hagan uso exclusivamente de guardar la contraseña.

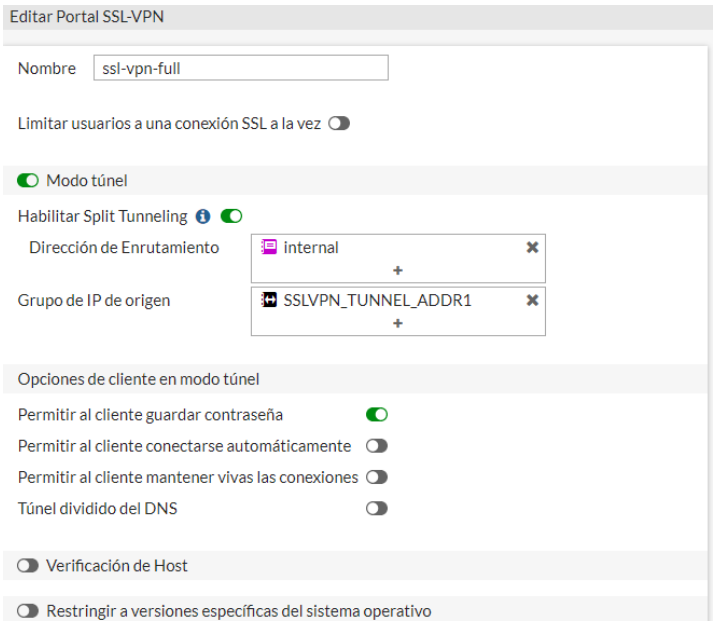

Figura 39. Asignación de direcciones y grupos para el portal de la VPN.

Luego se crea una política de seguridad con el fin de otorgar conexión a la red, en esa política se especifica que el tráfico ingresara desde el túnel VPN a la red interna de la empresa, en esta política de seguridad adicionalmente se asignan los perfiles de seguridad creadas para la red principal, adicionalmente se crea una política en el SNAT, en el cual se describa el mismo funcionamiento de la red principal.

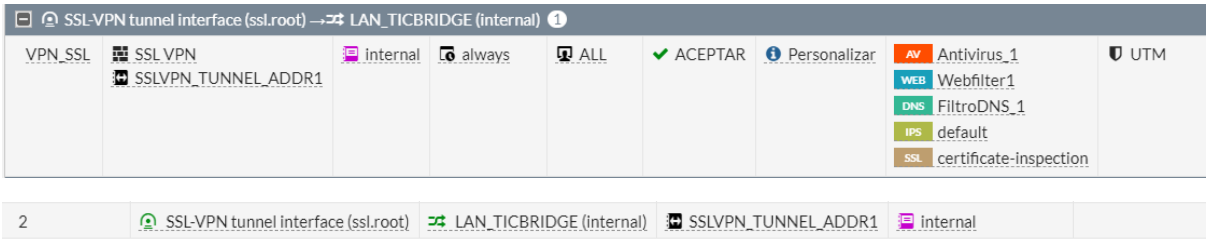

Figura 40. Creación política para la VPN.

4.3.3.5. Ingreso VPN

El ingreso a la VPN se realiza mediante la respectiva dirección pública (190.27.51.54) con el puerto determinado (10443), habiendo ingresado al entorno web de la página se introduce el respectivo usuario y contraseña creado anteriormente para que el acceso a la VPN.

Ya habiendo ingresa do al entorno web de la VPN este permite realizar conexión a la misma de dos diferentes maneras, ya sea mediante una conexión rápida o por medio de la aplicación forticlient. Adicionalmente este permite observar el historial de ingresos a la VPN.

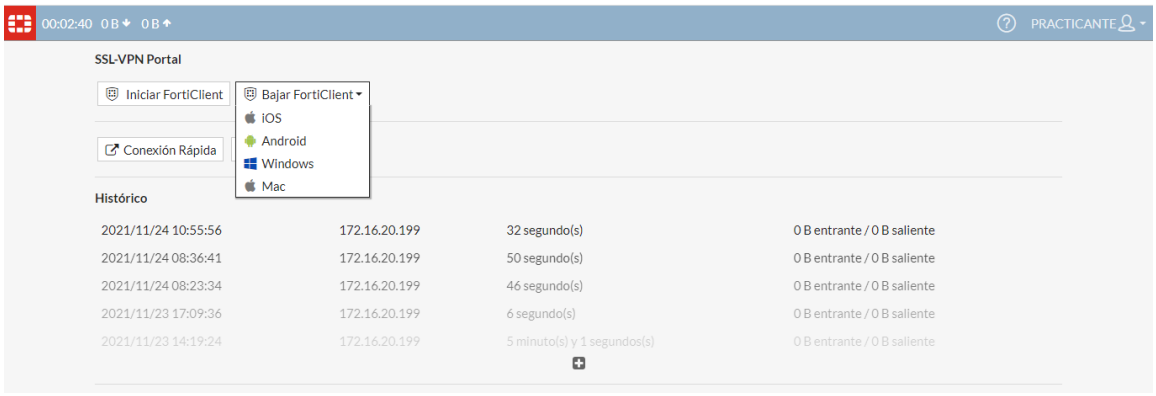

Figura 41.Interfaz web VPN.

En la conexión rápida se puede hacer uso de diferentes herramientas como lo son los protocolos HTTP/HTTPS para el ingreso a Páginas web, FTP/SMB/CIFS/SFTP para él envió de archivos, RDP/VNC para el manejo de dispositivos a distancia y SSH/Telnet/PING para el manejo de la red a distancia.

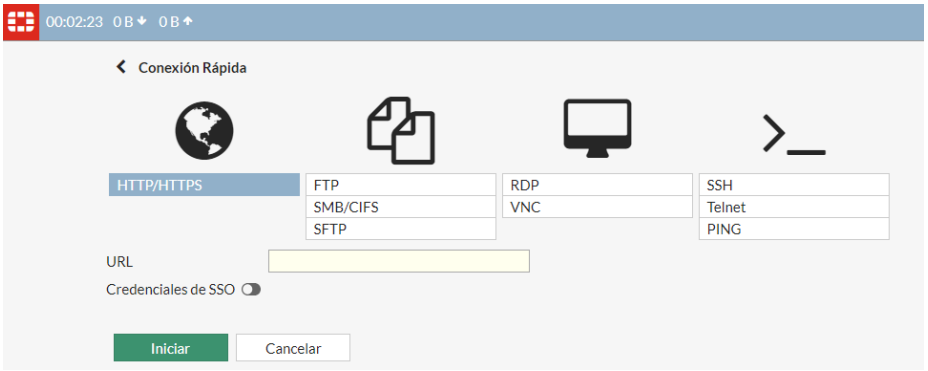

Figura 42.Conexión rápida VPN.

Desde la aplicación Forticlient, se permite el ingreso a la VPN, pero es necesario ingresar información de esta como lo es el respectivo nombre de la conexión, el Gateway remoto y el puerto que se utilizará, por último, se selecciona el nombre del usuario que hará uso de la VPN.

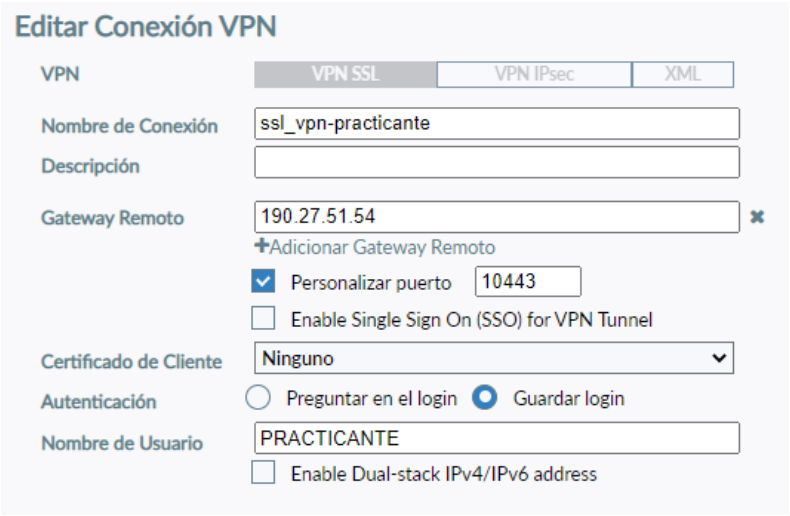

Figura 43. configuración Forticlient.

Luego únicamente es necesario ingresar la respectiva contraseña y después de un tiempo se establecerá conexión con la red.

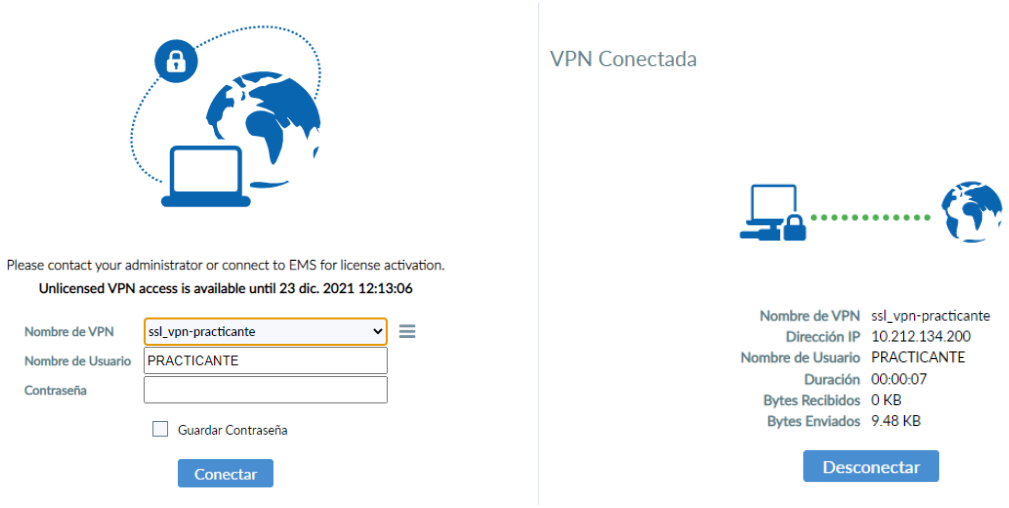

Figura 44. Ingreso Forticlient mediante VPN.

4.4. Mejora Visibilidad Digital

4.4.1. Página web

Las páginas web en la actualidad se han convertido en una herramienta fundamental para el funcionamiento de las empresas, ya que por medio de estas se pueden realizar varias actividades como lo es informar a los usuarios de los productos /servicios que ofrece la empresa, generar canales de comunicación con los posibles clientes y crear medios de pago.

Tomando en cuenta lo anterior TICBRIDGE S.A.S. Decide realizar el rediseño de su página web, en la cual será necesario realizar algunas modificaciones para mejorar la interacción de los clientes con la empresa y a su vez permitir obtener nuevos clientes mediante su posicionamiento.

4.4.1.1. Estado Inicial

Al inicio de la pasantía se identificó la necesidad de mejoras a la página web como: la inserción de un botón de chat, la obtención de un certificado de seguridad, sección de blog y un cambio en cuanto a la estructura de la página.

Dichos cambios son fundamentales tanto para el posicionamiento de la empresa en internet como para su propio funcionamiento, ya que una sección de blog garantiza que se puedan obtener más visitas al sitio de una forma orgánica y a su vez permite posicionar de mejor manera la empresa; Un certificado SSL es de vital importancia para la empresa y la falta de él puede generar muchos problemas comerciales, principalmente porque en la página web actual se utiliza un botón de pago y al no tener un certificado SSL esto puede generar que muchos de los clientes no confíen de a página, dada la ausencia de dicho certificado.

La página aparece en el buscador como sitio no seguro o si utilizan ciertas políticas de seguridad en su antivirus este no les permite observar la página provocando que se pierdan posibles avances comerciales, dicho certificado se obtiene dependiendo del hosting y el nivel de encriptación que este otorgue a las páginas que se encuentren en el mismo. Adicionalmente hoy en día un certificado SSL es fundamental para una página web ya que garantiza un nivel de seguridad básico en cuanto a encriptación de la información.

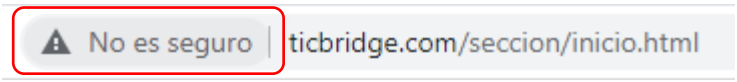

Figura 45. Certificado SSL.

Por último se logra identificar la necesidad de un botón de chat, ya sea WhatsApp o para chat en vivo, los cuales son fundamentales para poder comunicarse con posibles clientes, con cuales se pueden concretar negocios y dar soporte para los determinados servicios, dichos botones en su gran mayoría son servicios dados por compañías, en este caso para la empresa es de vital importancia adquirir uno de estos, ya que una de sus empresas socias “3CX” cuenta con este servicio para chat en vivo, lastimosamente aunque se ha generado en la página el botón este no funciona ni direcciona a ningún lugar.

Figura 46. Botón chat en vivo.

Con el fin de conocer si estas implementaciones eran posibles se contactó con la empresa encargada de la administración de la página, la cual comunico que era necesario hacer un rediseño y actualización, ya que en el entorno en el que se encontraba diseñada no se podían implementar modificaciones como el chat en vivo.

Lastimosamente con el proveedor anterior no se logró entablar un acuerdo para el rediseño por lo cual se debe realizar cotizaciones con nuevas empresas para el diseño de la página web, ya que se requiere que esta tenga una plataforma de gestión para que cualquiera en la organización pueda realizar una modificación.

4.4.1.1.1. Cotización

Tomando en cuenta los problemas presentados con la empresa proveedora anteriormente nombrados, se procede a realizar la correspondiente cotización tanto del rediseño como la transferencia de hosting que se realiza actualmente. De tal manera que se realizó el contacto con varias de las empresas que ya habían realizado este procedimiento con algunas empresas del sector a continuación, podemos evidenciar las empresas consultadas, a las cuales se les solicito enviar una cotización en la que se tuviera en cuenta el respectivo rediseño, transferencia de hosting e implementación de herramientas como lo son los botones tanto para WhatsApp como para el de chat normal.

Empresas consultadas:

- **Creando web**
- **321 DISEÑO WEB**
- **Imagen virtual web**
- **PisPos**
- **Sainet**
- **Platino web**

4.4.1.1.2. Evaluación de ofertas

Con el fin de realizar la respectiva comparación en cuanto a las diferentes empresas de diseño de páginas web, se procede a realizar la calificación de varias de las páginas diseñadas anteriormente por las empresas. Dicha calificación se hace por medio de las páginas web insites y web grader las cuales estudian el estado actual de las diferentes páginas y las evalúa del 0 al 100. Se utilizaron estos dos calificadores principalmente por que insites tiene varios parámetros de calificación que se basan en el posicionamiento mientras, web grader le da más valor en su calificación a la estructura de la página.

Adicionalmente se calificó la página actual de TICBRIDGE S.A.S. con el fin de visualizar las falencias actuales, entre las cuales se puede observar principalmente en una correcta optimización de la página para los dispositivos móviles, el rendimiento y estructura de la página no son los ideales, se evidencio la falta de le chat en vivo, el blog y el certificado SSL.

Luego del estudio tanto de las páginas realizadas por las empresas como la propia de TICBRIDGE S.A.S., se realiza una nueva cotización a las empresas creando web, 321 diseño web y platino web, en el cual se tiene en cuenta las todas las falencias observadas tanto por las páginas calificadoras como las observadas al principio de la pasantía. Adicionalmente se procede a realizar una investigación de las empresas con el fin de valorar algunos factores externos a la cotización, dichos factores se enfocan en poder escoger a la empresa, que de mejores garantías en cuanto a servicios prestados; los factores añadidos son: el número de páginas desarrolladas, el lugar donde se realiza el hosting y los años de experiencia en el sector.

Ya teniendo todos los factores de calificación para escoger la empresa que realizara el rediseño, se crea una tabla comparativa con los diferentes factores:

Nombre	Plataforma de administración	Numero de secciones	Tiempo de despliegue	Experiencia	Historial paginas realizadas	Calificación web grader	Calificación insites	Promedio individual	Promedio global	Duración de soporte	Hosting	Texto cotización	Precio
Creando web	Wordpress	10	30 días	14 años	www.voip-mundo.com	72	59	65.5	61.8	1 año	Cali-San Francisco, california	Creando web	$1.720.000(host local).- $2.130.000(host eeuu)
					www.colombiasystems.com	80	58	69					
					https://www.ingenierosmys.com/	77	35	56					
					https://casercolombia.com/	72	45	58.5					
					www.netserviceits.com	67	53	60					
321 Diseño web	Wordpress	15	16 días	11 años	www.axentriacg.com.co	77	46	61.5	61.3	1 año	los angeles, california	321 Diseño web	$1.499.000.
					www.expressbattery.co	65	52	58.5					
					https://sigmaarquitectura.com.co/	77	48	62.5					
					https://conforaires.com/	87	46	66.5					
					www.studionovoa.com	69	46	57.5					
Platino web	Wordpress, Joomla,Drupal	15	25 días	16 años	https://funitel.com.co/	59	49	54	63.5	gratis post venta	Pompano Beach (Florida)	Platino web	$1.889.000- $2.389.000 (Bolsa de horas de soportes)
					https://hlingenieros.com/inicio/	83	54	68.5					
					https://eysglobal.com/	76	64	70					
					https://www.fadalte.com/	77	55	66					
					https://stglogisticssolutions.com/	73	45	59					

Tabla 12. Tabla comparativa cotizaciones.

Tomando en cuenta lo anterior se escogió la empresa platino web principalmente porque esta poseía en su oferta un mayor número de secciones, mejor calificación en páginas realizadas anteriormente y garantizan un soporte gratuito postventa. Adicionalmente estos ofrecen un curso de Wordpress y una bolsa de horas para ayuda experta.

4.4.1.2. Adición nueva secciones

Durante el proceso de estudio de solución, la respectiva cotización y selección delcandidato para el rediseño de la página web, se realizaron la adición de nuevas secciones a la página web tomando en cuenta que durante dicho tiempo se obtuvo tanto nuevos socios como certificaciones.

4.4.1.2.1. Sección 3CX

Durante los últimos años se ha podido observar un crecimiento en el uso de la nube y como esta puede ser utilizada para rebajar tanto la carga laboral como los costos de una empresa, por lo cual una solución como 3CX que hemos explorado e implementada anteriormente. 3CX se convierte en uno de los nuevos socios de TICBRIDGE S.A.S. Con el fin de poder ser ofrecida como solución telefónica en la nube y on premise para sus clientes, ya sea para que estos transfieran sus centrales telefónicas a la nube o la desarrollen desde cero.

De tal manera que se desarrolla una sección en la cual se agregan imágenes dadas por la empresa 3CX y se dio un pequeño resumen enfocado para los clientes en el cual se de una pequeña reseña tanto de sus características principales.

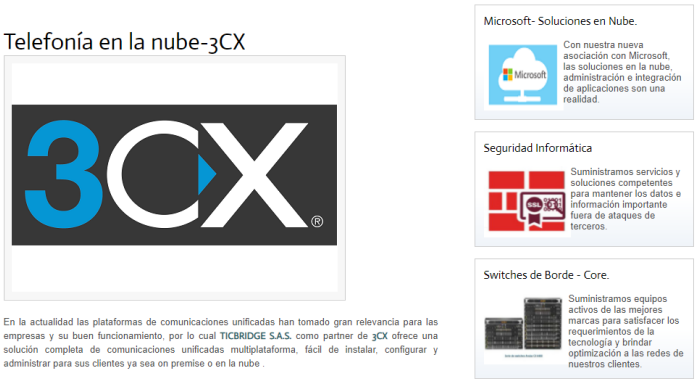

Figura 47. Sección 3CX.

4.4.1.2.2. Sección Wolkvox

En cuanto a soluciones de Contact Center, el mercado ha evolucionado a un punto en el cual cada cliente requiere de una solución especifica tanto para la administración como para la calidad del servicio, lo que convierte a Wolkvox un gran aliado, ya que cuenta con herramientas como la inteligencia computacional y el procesamiento de señales, que permiten dar soluciones especializadas a determinadas solicitudes de los clientes.

Se desarrolla una sección en la cual se agregan imágenes dadas por la empresa Wolkvox y se dio un pequeño resumen enfocado para los clientes con una reseña de sus características principales.

Figura 48. Sección 3CX.

4.4.1.2.3. Sección Proveedor certificado

En el mercado de las telecomunicaciones e informática es muy importante obtener y dar certificaciones a los clientes, ya que gracias a estas se da garantía a los clientes del servicio o producto adquirido es el adecuado, de tal manera que en el último tiempo TICBRIDGE S.A.S. realizo el proceso para adquirir un certificado de proveedor homologado, el cual permitirá que los clientes tengan confianza a la hora de adquirir cualquiera de los servicios y productos de TICBRIDGE S.AS.

Se desarrolla una sección en la cual se agrega el certificado por la empresa certificadora SIGUD y se dio un pequeño resumen enfocado para los clientes y reseña de sus características principales.

Figura 49. Proveedor certificado.

4.4.1.3. Rediseño y transferencia de Hosting

Luego del respectivo proceso para la contratación de los servicios de platino web realizado por el área de compras y por la administración. Se procede a la implementación del rediseño de la página web, propuesto por platino web. Los pasos propuestos por la empresa son:

1. Levantamiento de información
2. Diseño de página web
3. Creación de contenidos
4. programación
5. Ajuste de estilos
6. Cierre
7. Entrega

4.4.1.3.1. Levantamiento de información

Con el fin de determinar los alineamientos visuales que tendrá el inicio del sitio web se entrega la información solicitada como lo es:

- Dominio del sitio web donde se ingresan las respectivas credenciales necesarias para la transferencia del dominio de un Hosting a otro.

  - **Dominio:** ticbridge.com
  - **Hosting:** http://dns.pandacons.com/
  - **Contraseña:** **********
- Descripción breve de la compañía.
  Es un integrador de soluciones relacionadas con **el diseño, la fabricación, la instalación y el mantenimiento en las áreas de la informática y las telecomunicaciones**, que desde hace más de 12 años ha logrado constituir un equipo de trabajo sólido, que ayuda a compañías nacionales y multinacionales con sedes en Colombia de diversos sectores al desarrollo exitoso de **proyectos de tecnología** de gran beneficio para sus negocios, desde nuestras sedes en **Bogotá, Cali y Barranquilla** con la implementación de **soluciones de infraestructura y servicios en telecomunicaciones, seguridad informática, soluciones de Microsoft, adecuación de salas de reuniones, Contact Center, seguridad electrónica ...**

- Definición de frases para el posicionamiento en buscador de Google.

  - Soluciones para Contact Center en la nube en Colombia
  - Implementación de New Generation Firewall en Colombia.
  - Integración de servicios para Microsoft Empresarial en Colombia.
  - Soluciones de infraestructura en telecomunicaciones en Colombia.

- Descripción de a gestión comercial.

  - Voz a voz … sugiere un botón “Recomendar”
  - Brochure … “Descargar Brochure”
  - Redes Sociales … “Botones”
  - Agente comercial …” Contáctenos”

- Perfil de los usuarios de la página web.

  Empresas Privadas
  - Organismos públicos
  - Hoteles
  - Empresas concesionarias de obra pública, Universidades.
  - Hospitales

- Frases para el banner principal.

  - **12 años de experiencia** en las áreas de informática y telecomunicaciones.
  - **Soluciones en la nube** de la mano de las compañías líderes del sector.
  - **Aliados de Fortinet** para ofrecer soluciones en seguridad informática.
  - **Certificado de proveedor** homologado Risks International.
  - **Expertos en soluciones de voz** Unify, Issabel y 3CX.
  -

- Ítems de menú principal.

  - Empresa
    - Quienes somos
    - Proveedor Certificado
  - Portafolio
    - Seguridad informática
    - Soluciones de Microsoft
    - Adecuación de Salas de Conferencia
    - Servicios Profesionales
      - ✓ Consultoría
      - ✓ Diseño
    - Soluciones en Redes
      - ✓ Switches de Borde - Core
      - ✓ UPS
    - Soluciones de voz
      - ✓ VoIP-Híbridos-TDM
    - Soluciones de Contact Center
      - ✓ Telefonía en la nube-3CX
      - ✓ Contact Center en la nube - Wolkvox
    - Proyección Corporativa
      - ✓ Video walls y TV Hospitality
    - Soluciones en Seguridad
      - ✓ Control de acceso y CCTV
  - Blog
  - Contacto

Para esta parte se tuvo en cuenta que el contrato se firmó con un número de secciones igual a 17 de tal manera que, en principio se agregaran pocas secciones con el fin de que en un futuro por medio de las capacitaciones se logre la creación e implementación de las secciones faltantes, estas secciones son principalmente las secciones del portafolio.

- Links redes sociales.
  Facebook: https://www.facebook.com/ticbridgesas/
  LinkedIn: https://co.linkedin.com/company/ticbridge
  WhatsApp: 3165242609

- Elementos que deben encontrarse en la página de inicio.
    - Enlaces a redes sociales
    - Datos de contacto
    - Horario
    - Lunes - viernes 7:30am a 6:00pm
    - Banner principal
    - Link a servicios principales
    - Texto introductorio de la empresa
    - Aliados de negocio (carrusel)
    - Indicadores tales como Proyectos realizados “+600”, Cantidad de clientes felices “+100”, Sedes “3”, Años de experiencia “+12 años”
    - Clientes (carrusel)
    - Certificados (está ubicado en documentos > cartificado.pdf)
    - Chat en Línea
    - Conector de Whats App
    - Contáctenos
    - Mapa de Ubicación
    - Pie de página con datos de contacto
    - Botón de pago

- Datos de contacto al pie de página.
  Bogotá

  Teléfono: (+571) 643-1584
  Correo: ticbridge@ticbridge.com
  Dirección: Carrera 57C No 127D-24
  Las Villas

  Cali

  Teléfono: (+572) 486-2961 Extensión 9152
  Correo: ticbridge@ticbridge.com
  Dirección: Carrera 100 No.5 -169, Torre B Pasoancho, Piso 6, Ciudadela Comercial Unicentro.

  Barranquilla

  Teléfono: (+575) 385-9784
  Correo: ticbridge@ticbridge.com
  Dirección: Carrera 51 No. 76 - 199 Piso 2

- Preferencias visuales.
    - https://eysglobal.com/ : Nos gusta el dinamismo de la página, como desde el principio con el video llaman la atención de esta y como sus diferentes partes se encuentran en movimiento e interaccionan con los movimientos del mouse.

- https://hlingenieros.com/ : Nos gusta tanto el diseño de la página como el manejo de los colores corporativos, haciendo que estos se encuentren y resaltan en la página sin la necesidad de que estos llamen mucho la atención.

- Estilos de diseño deseados, tanto para el encabezado como para el blog.
  - Encabezado

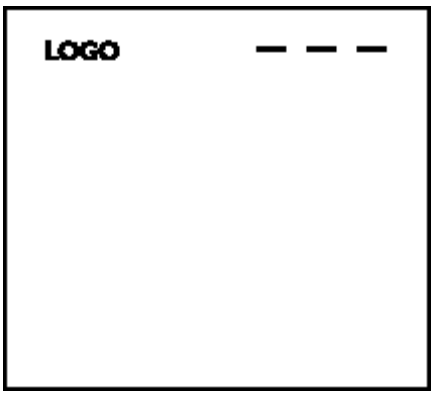

Figura 50. Formato de encabezado escogido.

  - Blog

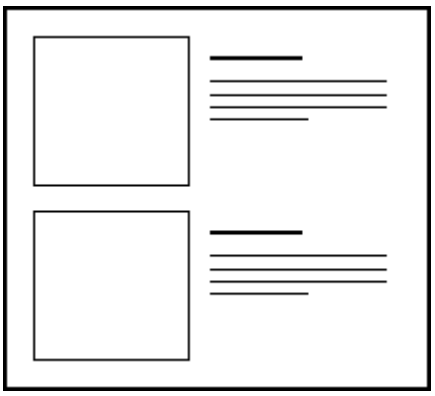

Figura 51. Formato de Blog escogido.

4.4.1.3.2. Diseño

Con el fin de iniciar el diseño de la página web por parte de platino web se realiza la diagramación de la página de inicio, se define cuáles serán las secciones y boxes que deberá tener la página web; Para la cual se tiene en cuenta principalmente la información entregada en la sección de levantamiento de información.

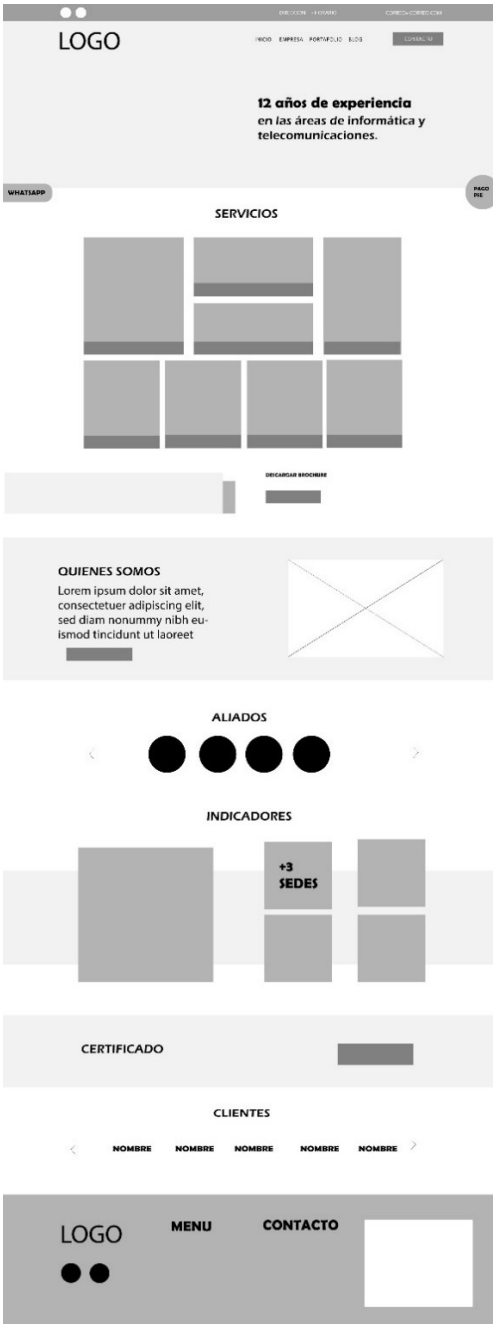

Figura 52. Diagramación sección de Inicio página web.

Teniendo en cuenta la diagramación y varios de las solicitudes en cuanto a diseño, platino web por parte de su área de diseño proponen algunos bocetos y se realiza el acompañamiento para dichos diseños teniendo en cuenta algunas de las directrices dadas por TICBRIDGE S.A.S. como dinamismo, información importante y rendimiento.

El diseño principalmente se baso en la pagina inicial de la pagina web, ya que en esta es donde las personas suelen tener mayor interacción, por lo cual se busca que esta sea lo sufiente mente llamativa y informativa.

A continuación se describen el disñeo de las paginas programadas en Wordpress, principalmente las secciones de la pagina principal y la pagina interna.

Banner

En el diseño del banner se busco que este fuera llamativo, por lo cual en lugar de tener una imagen estacionaria o un carrusel de imágenes, se selecciono un video de un planeta girando compuesto por particula, adicionalmente en este banner se tuvo en cuenta que era necesario contar con un menú, con el fin de poder direccionar a los usuarios a las paginas internas y así poder navegar por la pagina adecuadamente, este menú ira conformado por los siguientes elementos:

- Inicio: Permite volver a la pagina de inicio cuando este sea precionado.
- Empresa: Direcciona a la seccion de empresa en la cual se entrega la información importante sobre la propia empresa y su funcionamiento.
- Portafolio: Despliega de si, un menu en el cual se podra observar un listado de servicios de TICBRIDGE S.A.S.
- Blog: LLeva a la seccion de blog, para a su vez poder observar los artculos relacionados con los servcios de la empresa.
- Contacto: Direcciona a la seccion de contacto y en este podra tramitar un formulario con la respectiva petición o mensaje para los entes de la emresa.

Luego en la parte del medio del banner podremos encontrar un titulo de carrusel, el cual cambiara mostrando diferentes textos, los cuales mostraran información de la empresa y los servicios prestados por la misma, debajo de este se podra encontrar un boton “soluciones a tu medida”, el cual direccionara al usuario a la pagana interna del servicio mencionado.

Adicionalmente a la parte del banner se ha agregado un boton de pagos, el cual redireccionara a una pagina especifica de la empresa de PSE, para realizar pagos a la empresa, a la izquierda del boton de pagos, hay un mensaje con el TRM actualizado, este se actualiza diariamente con el nuevo precio del dólar con el finde poder dar informacion a los clientes de la converción del mismo.

Figura 53. Diseño Banner.

Portafolio

Luego en la sección de portafolio se encuentran botones con todos los diferentes servicios de la empresa, en este a diferencia de la página anterior se decide que se deben separar los servicios de Contact Center y de telefonía en dos, por lo cual se agrega adicionalmente el servicio de Contact Center; la función principal es que los botones redireccionaran a la página interna de cada servicio.

Figura 54. Diseño portafolio.

Descargables

Luego en la sección de descargables se encuentran dos botones que funcionan de tal manera que al seleccionar uno permita descargar el brochure de la empresa con todos los servicios y el segundo permitirá descargar certificado de proveedor autorizado entregado por la entidad SIGUD.

Figura 55. Diseños descargables.

Conócenos

Luego por recomendación de los diseñadores se implementa un respectivo descanso visual, por lo cual se pone un box con dos imágenes grandes a sus lados como lo son el logo de TICBRIDGE S.AS. En gris y una persona, en el centro se podrá observar un texto con las diferentes soluciones de la empresa y por último un botón de contacto el cual tendrá la utilidad de enviar a las personas a la sección de empresa.

Figura 56. Diseño Conócenos.

Aliados

Con el fin de dar información de los diferentes aliados de la empresa, se crea un carrusel con los logos de los diferentes socios de la empresa, estas imágenes fueron obtenidas contactando a cada uno de los diferentes aliados. Cada uno de los botones que se mueven en el carrusel direcciona a los servicios que se relacionan directamente. Atrás de dicho carrusel hay una imagen en movimiento la cual está creada por recomendación de los diseñadores tanto para dar dinamismo a la página como para hacer un contraste con el carrusel y los logos de las empresas.

Figura 57. Diseños aliados.

Información empresarial

Para dar información de la empresa, sus magnitudes y trayectoria, de una forma sencilla se añade un box la cual contenga información numérica de la empresa como proyectos realizados, clientes felices, sedes y años de experiencia. Estos números tendrán una animación la cual será el aumento de los números de tal manera que le dé dinamismo a la página y llame la atención de los usuarios.

Figura 58. Diseño información empresarial.

Blog

Se agrega adicionalmente una sección en la cual se muestren los diferentes blogs, esta fue diseñada de tal manera que se pudieran observar tanto la imagen como un pequeño resumen de los artículos más recientes, al hacer clic sobre los diferentes resúmenes de los artículos, se direccionara al usuario a el respectivo artículo; Esta parte es muy importante, ya que con ella también se logrará que los artículos se posicionen en los buscadores de internet.

Figura 59. Diseño Blog.

Carrusel clientes

Para dar información de los clientes de los diferentes servicios prestados por TICBRIDGE S.A.S. se agrega un carrusel con los nombres de las empresas y entidades con las que se ha trabajado. Lastimosamente a la hora de finalizar esta pasantía no se logró adquirir las imágenes de la mayoría de las empresas por lo cual se ponen únicamente imágenes con los nombres, se espera que en un futuro las empresas se pueda realizarla inserción de los diferentes logotipos.

Figura 60.Diseño carrusel clientes.

Footer

Por último, en el footer de la página web se agrega información de contacto de las diferentes sedes de la empresa, información de contacto como correo, número de teléfono y horario de trabajo. También en esta parte del footer podemos observar los botones de WhatsApp y de chat en vivo estos dos botones se encontrarán todo el tiempo en pantalla y se moverán de acuerdo con el scroll que haga el usuario. Dicho servicio de chat en vivo será creado desde 3CX con el fin de poder unificar los servicios de telefonía de dicha empresa.

Figura 61. Diseño Footer.

Pagina interna

Para el diseño de las páginas internas se tiene en cuenta varias de las recomendaciones de platino web ya que en este se busca mejorar el posicionamiento de la página, en este se tiene en cuenta tanto la fuente y el tamaño del texto.

Figura 62. Diseño página interna.

4.4.1.3.3. Transferencia de dominio

Dado que se quiere obtener un certificado SSL es necesario realizar la transferencia de hosting lo que incluye a su vez la transferencia del dominio, para esto es necesario tener en cuenta varias normas que han sido establecidas, dado que el registro de los dominios y sus estados son regulados por ICANN (Corporación de Internet para Nombres y Números Asignados).

Se procede a realizar la transferencia de dominio web para la cual fue necesario obtener la siguiente información por parte del registrador anterior:

- **Clave EPP:** También nombrado Auth Code, es el código generado cuando se registran los dominios, este tiene la función de verificar al registrador a la hora de realizar la transferencia.
- **Aprobación de transferencia:** Dado que se va a realizar la transferencia es necesario tener en cuenta que para este procedimiento es necesario que el registrador anterior de la autorización de la transferencia, este procedimiento es opcional pero facilita la transferencia.
- **Credenciales de administración:** Cada registrador posee su respectivo portal de administrador en el cual se encuentra la información del respectivo servidor DNS en el cual se encuentra la página web.

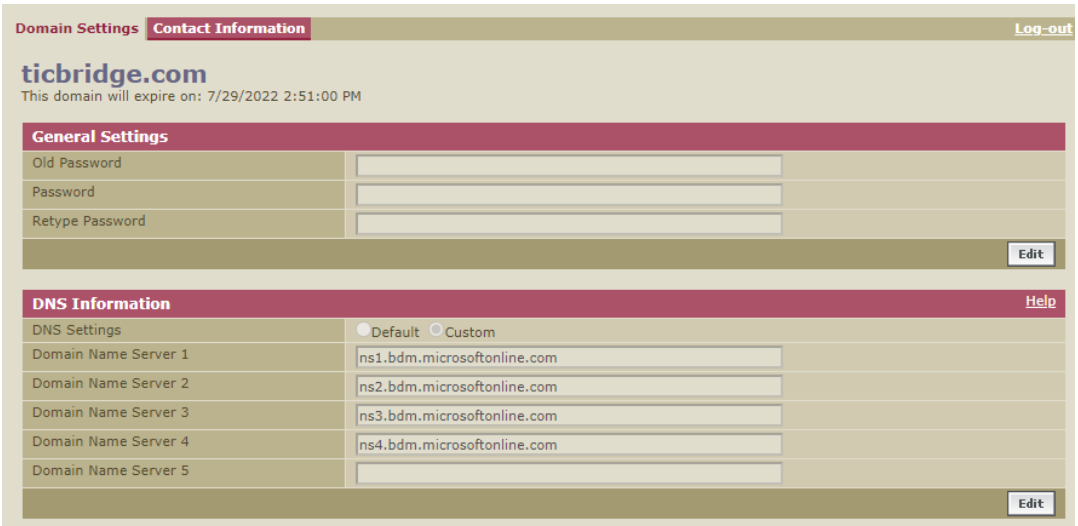

Figura 63. Portal de administración de dominio.

La transferencia de dominio se realizó por medio de la empresa mega web service, en esta se tiene en cuenta que se adquiero el paquete advanced con el cual se incluyen los siguientes servicios.

- Ilimitado Espacio en Disco
- Ilimitado Tráfico Mensual
- 5 dominios Alojados
- Ilimitado Subdominios
- 500 Correos Electrónicos
- 20 bases de Datos MySQL
- 15 GB VPN tráfico
- Certificado SSL
- Transferencia/registro de 1 dominio gratis

Teniendo en cuenta que en este pack solo se incluye la transferencia de un solo dominio se procede a realizar la transferencia cuyo proceso se basa en la sección del dominio, la reactiva transferencia para la transferencia y el completar un formulario con la información del titular que será el encargado de la cuenta.

Figura 64. Portal de administración de dominio.

Dado que se realiza la transferencia de dominio es fundamental ingresar la información del administrador de dominio con el nuevo registrador y así permitir que esta administración se pueda realizar de manera directa.

4.5. Estado Final Red Local TICBRIDGE

Con el fin de evidenciar las modificaciones realizadas y para contextualizar posibles proyectos futuros se realiza la documentación del estado final de la red en la sede de Bogotá D.C. TICBRIDGE S.A.S. teniendo en cuenta todos los cambios realizados para la mejora de la red tanto por la transferencia de la central telefónica de la nube a la central telefónica como la implementación de la SD-WAN.

A continuación, podremos observar u diagrama lógico donde se encentrarán los diferentes dispositivos que hacen parte de la red Local de TICBRIDGE S.A.S. en la sede de Bogotá D.C., en estese puede evidenciar el cambio del dispositivo linksys a el fortigate 60F y la sustitución del dispositivo NVR de tal manera que ahora los teléfonos se encuentran conectados directamente al patch panel.

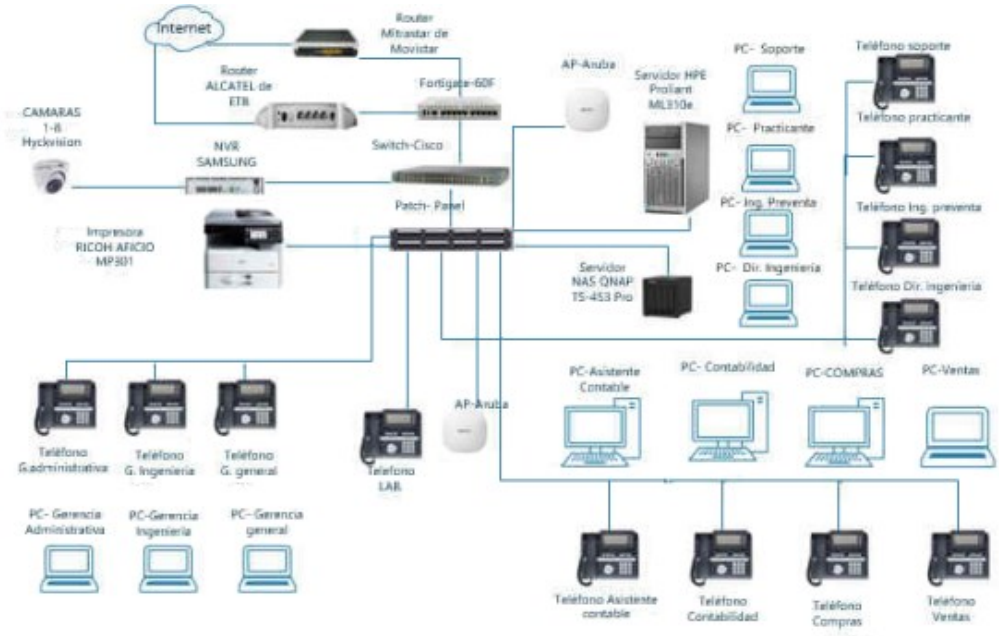

Figura 65. Diagrama lógico estado final TICBRIDGE S.A.S.

Por último, se realiza la respectiva identificación de las direcciones IP de los diferentes dispositivos teniendo en cuenta que durante el procedimiento de la transferencia de los teléfonos de la red local a la red de VO-IP a la red administrativa, adicionado a esto se ve que el dispositivo Fortigate-60F ahora tendrá la dirección del que antes era el dispositivo linksys.

SUB-RED	Dispositivo	IP
VLAN 20-Administrativa	Impresora	172.16.20.15
VLAN 20 – Administrativa	Server	172.16.20.119
VLAN 20 – Administrativa	AP-315 PISO 1	172.16.20.12
VLAN 20 – Administrativa	AP-315 PISO 2	172.16.20.13
VLAN 20 – Administrativa	NAS	172.16.20.14
VLAN 20 – Administrativa	Fortigate 60F	172.16.20.6
VLAN 20 – Administrativa	Ge. Administrativa	172.16.20.32
VLAN 20 – Administrativa	Ge. General	172.16.20.31
VLAN 20 – Administrativa	Ge. Ingeniería	172.16.20.37
VLAN 20 – Administrativa	Asist. Contable	172.16.20.30
VLAN 20 – Administrativa	Asist. Administrativa	
VLAN 20 – Administrativa	Compras	172.16.20.36
VLAN 20 – Administrativa	Ing. Preventa	172.16.20.33
VLAN 20 – Administrativa	Account Manager Sr.	172.16.20.35
VLAN 20 – Administrativa	Practicante	172.16.20.34
VLAN 40 - CCTV	NVR	172.40.40.20
VLAN 40 - CCTV	CAM1 RECEPCION	192.168.231.8
VLAN 40 - CCTV	CAM2 BODEGA	192.168.231.3
VLAN 40 - CCTV	CAM3 SALA REUNIONES	192.168.231.5
VLAN 40 - CCTV	CAM4 PASILLO PISO 2	192.168.231.7
VLAN 40 - CCTV	CAM 5 LAB	192.168.231.6
VLAN 40 - CCTV	CAM 7 ENTRADA	192.168.231.2
VLAN 40 - CCTV	CAM 8 SALA INGENIERIA	192.168.231.4

Tabla 13. Dispositivos TICBRIDGE S.A.S.

5. Conclusiones y recomendaciones

- En el proceso del mejoramiento de la red, se pudo observar los beneficios con los que esta cuenta la nube, los requerimientos necesarios para hacer uso de esta y como esta puede ser enfocada para dar solución a diferentes necesidades en especial en este caso para lo que sería la telefonía corporativa.

- La SD-WAN es una solución novedosa para cualquier empresa que requiera mejorar su conectividad principalmente porque esta permite la administración de diversos enlaces ya establecidos e incorporar algunos nuevos, adicionalmente en el proyecto se pudo observar cómo esta solución puede variar dependiendo del fabricante y como esta debe ser seleccionada dependiendo de las necesidades de este.

- La seguridad informática es muy importante para las empresas ya que permite proteger uno de los bienes más valiosos hoy en día como lo es la información, la empresa Fortinet y en ella los dispositivos Fortigate, demostraron ser herramientas muy poderosas para la protección de la red por medio de los múltiples servicios con los que esta cuenta y el diseño de políticas de seguridad a la medida para la empresa, adicionado a esto se pudo observar como el dispositivo Fortigate 60F permiten el mejoramiento de la red con funciones como la SD-WAN y Gateway.

- La página web es una herramienta muy importante para una empresa como TICBRIDGE S.AS., debido a que con un buen posicionamiento web se pueden llegar a la consolidación de nuevos negocios, de tal manera que se pudo observar la importancia de elementos como el certificado SSL, botones de chat en vivo y WhatsApp; se evidenciaron las diferentes etapas y el procedimiento necesario para realizar la gestión para la contratación de una empresa, el rediseño de la página web y la transferencia del hosting.

- Se recomienda implementar e investigar el uso de herramientas más especializadas para la telefónica como lo son las soluciones dadas por la empresa Wolkvox, sumado a que se recomienda evaluar el uso de inteligencia computacional y sus entornos, ya sea para añadirlo a las soluciones ofrecidas como para utilizarlos en el funcionamiento interno de la empresa.

- Se sugiere plantear en un futuro realizar un pentesting de caja negra con el fin de encontrar las vulnerabilidades que se encuentran presentes en la compañía, de tal manera que se pueda obtener una seguridad informática completa en la empresa.

6. Referencias

[1] A. J. Barrero, «PROYECTO DE INTEGRACIÓN GLOBAL PARA LAS SOLUCIONES DE LOS SERVICIOS PRESTADOS EN TICBRIDGE S.A.S.,» Universidad Distrital Francisco José de Caldas , Bogotá D.C., Colombia , 2021 .

[2] Siemens, «HiPath 3000 V6.0 El sistema IP en tiempo real basado en SIP.,» 2005. [En línea]. Available: https://docplayer.es/622246-Hipath-3000-v6-0-el-sistema-ip-en-tiempo-real-basado-en-sip-hipath-3000-v6-0-plataforma-de-comunicaciones-modular-para-la-pequena-y-mediana-empresa.html. [Último acceso: 2021].

[3] S. M. R. Chóez, *ANÁLISIS DE LA IMPLEMENTACIÓN DE CENTRALITAS VIRTUALES EN LA NUBE COMO ALTERNATIVA AL SERVICIO DE TELEFONÍA FIJA,* GUAYAQUIL: UNIVERSIDAD DE GUAYAQUIL FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA DE INGENIERÍA EN TELEINFORMÁTICA, 2018.

[4] 3CX, «3CX.ES,» 20 Agosto 2021. [En línea]. Available: www.3cx.es/contact-center/call-center/.

[5] UNiFY, «HiPath 8000 Instrucciones de uso Teléfono OpenStage 40,» [En línea]. Available: https://docplayer.es/90273087-Hipath-8000-instrucciones-de-uso-telefono-openstage-40.html. [Último acceso: 2021].

[6] YEALINK NETWORK TECHNOLOGY CO., «SIP-T21(P) E2,» 2017. [En línea]. Available: https://www.yealink.com/upfiles/products/201711/1511945762795.pdf. [Último acceso: 2021].

[7] Z. Yang, Y. Cui, B. Li y Y. Liu, «Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities,» *IEEE,* 2019.

[8] Fortinet, «Fortinet Secure SD-WAN Solution Overview and Architecture Guide,» 27 Febrero 2021. [En línea]. Available: https://www.fortinet.com/. [Último acceso: 2021].

[9] Fortinet, «Fortinet.com,» 14 julio 2021. [En línea]. Available: www.fortinet.com/products/sd-wan?tab=models-specs.

[10] Aruba, «arubanetworks.com,» 14 julio 2021. [En línea]. Available: www.arubanetworks.com/es/productos/sd-wan/sd-branch/ .

[11] Aruba, «arubanetworks.com,» 14 julio 2021. [En línea]. Available: www.arubanetworks.com/es/productos/seguridad/.