# IMPLEMENTACIÓN DE HERRAMIENTA DE CONTROL DE ACCESO Y ADMINISTRACIÓN REMOTA SEGURA

JULIAN FERNANDO RINCÓN CRUZ
JOHN ALEXANDER ALARCÓN GUZMAN

UNIVERSIDAD SANTO TOMÁS DE AQUINO
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ, D.C.
2016

# IMPLEMENTACIÓN DE HERRAMIENTA DE CONTROL DE ACCESO Y ADMINISTRACIÓN REMOTA SEGURA

JULIAN FERNANDO RINCÓN CRUZ
JOHN ALEXANDER ALARCÓN GUZMAN

Tesis presentada para optar al título de Especialista en Gerencia de Proyectos de Ingeniería de Telecomunicaciones

Director ingeniero SILVIO HERNAN GIRALDO GOMÉZ

UNIVERSIDAD SANTO TOMÁS DE AQUINO
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ, D.C.
2016

Contenido

# LISTA DE TABLAS

# LISTA DE ILUSTRACIONES

# INTRODUCCIÓN

Dadas las vulnerabilidades que se tienen hoy en día a nivel de red y para dar cumplimiento a la normativa de seguridad AAA acrónimo de Authentication, Authorization y Accounting (Autenticación, Autorización y Contabilización), los cuales fueron diseñados como mecanismos de control de acceso remoto y provisión de servicios de red, se pretende realizar mediante una herramienta de gestión que la autenticación con la base de datos local de los routers gestionados por Telefónica se realice de una manera segura, donde se tenga una administración centralizada de los usuarios y un inventario de cada uno de los equipos instalados.

RADIUS es el acrónimo en inglés de Remote Authentication Dial-In User Server, el cual recibirá la información a través de un servidor NAS (Network Access Server), donde RADIUS comprueba que la información sea correcta mediante otros mecanismos de autenticación y, en caso de ser aceptada, autoriza al cliente a acceder al sistema y le provee los recursos necesarios para iniciar con la interacción del equipo remoto.

Esto permitiría que cada password vaya encriptado, se tenga acceso inmediato a los routers y se administre un control de cambios a través de equipos instalados en datacenter, donde se registre que usuarios han realizado modificaciones en las plantillas y se generen alarmas de cambios no autorizados.

# 1 ALCANCE

## 1.1 ALCANCE TOTAL

Por medio de unos servidores SSH adquiridos e instalados en Telefónica se pretende realizar la respectiva configuración, homologación e instalación del servicio de administración remota segura para luego realizar pruebas de failover y por ultimo realizar la migración total de los equipos instalados en las sedes del cliente gestionados por telefónica

Para habilitar la administración remota segura de los servicios de Datos e Internet, se debe validar la conectividad con los servidores SSH y RADIUS antes de aplicar la configuración en los CPE indicada. Esta configuración se aplica inmediatamente, por lo tanto, antes de salvar los cambios sobre los CPE, se debe confirmar la gestión a través del servidor SSH para luego sí salvar la nueva configuración.

El proyecto está pensado en una primera fase, limitado a los servicios monitoreados por Movistar Más, altas y modificaciones realizadas por el área de implantación y servicios que se atiendan por soporte técnico sobre los canales de datos e internet que se tengan aprovisionados y se vayan a instalar. Para esto simplemente se configurarán las políticas de importación en el BGP que se establece entre las VPRN de clientes y el router de interconexión Gestión Clientes, para aprender los segmentos asociados con cada uno de los servidores Movistar MAS, SSH, RADIUS y NTP.

Finalmente generar un documento técnico y su respectiva socialización con las áreas involucradas donde se muestre cada una de las labores realizadas y procesos que se deben cumplir para los servicios que posteriormente se van a instalar y configurar. Todo lo anterior legalizado en un acta de entrega y firmado por las respectivas jefaturas de operación y aprovisionamiento.

## 1.2 FASES DEL PROYECTO

Este proyecto consta de tres fases las cuales son: planificación, implementación y cierre las cuales se van documentando en el desarrollo de ese documento.

### 1.2.1 Planificación.

Dado que el proyecto está orientado a aumentar la seguridad y de crear una mejor forma de administración y control sobre los equipos que se encuentran en el cliente en el momento de realizar algún tipo de cambio o validación sobre los mismos se consideró una planeación muy detallada, la cual se inició con una validación completa de la topología de

red la cual utiliza los recursos de red asignados para la solución de conectividad con la herramienta de monitoreo Movistar_MAS. Para esto simplemente se configuraron las políticas de importación en el BGP que se establece entre las VPRN de clientes y el router de interconexión Gestión Clientes, asegurando con esto que los clientes que se encuentren seleccionados para esta primera fase no presenten inconvenientes en el momento de realizar la configuración en cada uno de los equipos.

Punto a seguir, es la configuración de SSH y RADIUS en los CPE, no sin antes verificar que las VPRN del cliente tengan conectividad con los servidores SSH y RADIUS y adicionalmente haber validado el tipo de interconexión usada (Interconexión por Inter-VPRN, interconexión por Epipe o interconexión por SAP).

Como último punto queda la configuración a realizar en los diferentes tipos de routers usados por los clientes (Cisco y Huawei) los cuales, una vez finalizada, la validación se podrá realizar de forma inmediata, logrando con esto que la configuración se haya realizado de la forma correcta.

### **1.2.2** Implementación.

En esta etapa se contempla la instalación de cada uno de los servidores en el datacenter realizando las pruebas de failover que permitirán, dado el caso que no fallen realizar de forma confiada la configuración en toda la red, incluyendo los equipos instalados en las sedes del cliente. Aun así, de primera mano las pruebas sobre los servidores instalados fallaran, se contempló en la etapa de planificación unos tiempos adicionales, que ayudaran a que no existan retrasos sobre el proyecto.

Se tienen en cuenta unas tablas e informes de seguimiento como se verá más adelante en el documento, los cuales permitirán dar control continuo al proyecto con el fin de realizar ajustes en las actividades que se requiera.

### **1.2.3** Cierre.

Ya en el cierre del proyecto se realizará una socialización con las áreas involucradas para tener una completa información que ayudará a que los servicios nuevos que se instalen o las modificaciones que se realicen se tenga en cuenta el protocolo de seguridad, ya sea para implementarlo o para validar que se encuentre configurado. Adicionalmente se entregará un manual de configuración y verificación para futuras consultas por si se presentan dudas o si se necesita algún tipo de ayuda para validar alguna falla que se presente

Y finalmente se redactará un acta de entrega que servirá de para dar cierre al proyecto, donde quedará constancia de la labor realizada y de la entrega completa del proyecto desarrollado.

## 1.3 LO QUE EL PROYECTO NO INCLUYE

Para el desarrollo de este proyecto se cuenta con los recursos de la herramienta de monitoreo movistar MAS, la cual permite validar el tiempo real el estado de un servicio (datos o internet) que haya contratado un cliente.

La solución dada para este movistar MAS consta de una configuración sobre la MPLS que permite establecer las políticas de importación entre el BGP, las VPRN de clientes y el router de interconexión Gestión Clientes, para aprender los segmentos asociados con cada uno de los servidores.

En base a estos recursos se da inicio a la primera fase de implementación de control de acceso seguro, por tal motivo el desarrollo y explicación más profunda de la herramienta movistar MAS no se tendrá en cuenta sobre este proyecto, ya que no hace parte de la ejecución de este proyecto.

En este proyecto no estuvieron contempladas las fases II, III y IV en la etapa de configuración de los CPE. En la tabla 1 se muestra el listado de actividades de estas fases.

- Fase II – Servicios de datos con CGP y Modelo de Gobierno
- Fase III Servicios de datos sin CGP con Movistar_MAS
- Fase IV – Servicios de datos sin Movistar_MAS

Tabla 1. Actividades que el proyecto no incluye

| Actividades | Tiempo de ejecución | Responsables |
|---|---|---|
| **Fase II** | 61 días | Por definir |
| Migración Fase II | 30 días | Por definir |
| Inventario Fase II | 30 días | Por definir |
| Solución servicios no configurados Fase II | 30 días | Por definir |
| Acta migración Fase II | 1 día | Por definir |
| **Fase III** | 61 días | Por definir |

| Actividades | Tiempo de ejecución | Responsables |
|---|---|---|
| Migración Fase III | 30 días | Por definir |
| Inventario Fase III | 30 días | Por definir |
| Solución servicios no configurados Fase III | 30 días | Por definir |
| Acta migración Fase IIII | 1 día | Por definir |
| **Migración Fase IV** | 61 días | Por definir |
| Migración Fase IV | 30 días | Por definir |
| Inventario Fase IV | 30 días | Por definir |
| Solución servicios no configurados Fase IV | 30 días | Por definir |
| Acta migración Fase IV | 1 día | Por definir |
| Acta Plan de Migración | 5 días | Por definir |

## 1.4 ENTREGABLES

### 1.4.1 Renovación tecnológica.

Se debe entregar un listado de los equipos cotizados con sus respectivos precios y especificaciones además de los proveedores. Posteriormente se debe hacer la compra de los equipos.

### 1.4.2 Integración Nueva Plataforma.

Documento en la cual se describe el proceso de instalación de los equipos que se adquirieron y la integración en la nueva plataforma.

### 1.4.3 Configuración red Telefónica.

Documento que contiene la configuración de los diferentes equipos dependiendo del tipo de servicio. Proceso de aprovisionamiento, redundancia y conectividad.

### 1.4.4 Anexo Técnico Configuración SSH&RADIUS CPE.

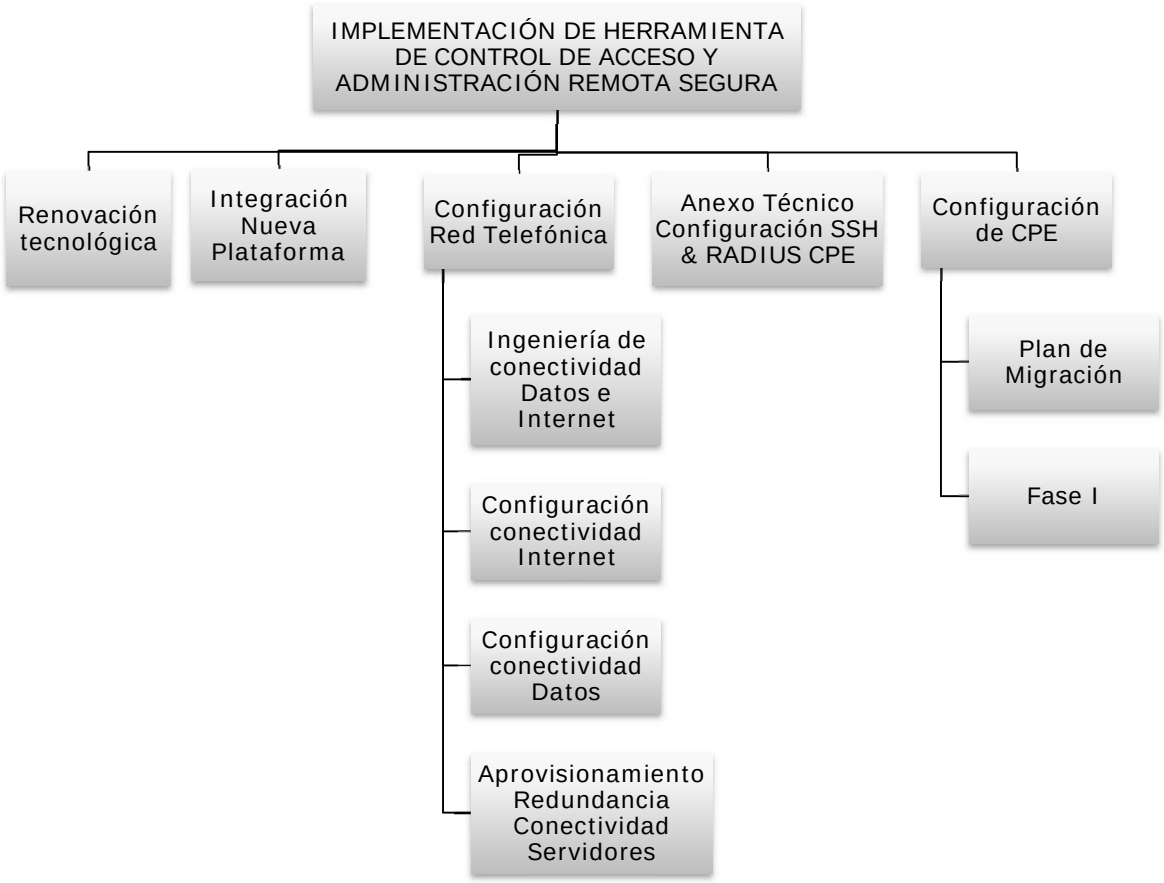
Se debe elaborar un manual con las diferentes configuraciones que se deben hacer en los equipos finales instalados en la sede de los clientes. También se deben especificar las pruebas que se deben hacer para confirmar la correcta configuración.

### 1.4.5 Configuración CPE.

Documento que contiene el listado de los clientes con las ip que se configuraron, referencia de los equipos y versión del software. Listado de los servicios que no pudieron ser configurados y la razón del por qué.

## 1.5 ESQUEMA DE DESGLOSE DE TRABAJO. EDT

Ilustración 1 Esquema de desglose de trabajo. EDT



## 1.6 RESTRICCIONES, SUPOSICIONES Y DEPENDENCIAS.

En la revisión de los equipos CPE se encontraron inconvenientes al realizar la configuración en algunos router por lo que en estos equipos no se permiten los protocolos de autenticación. A continuación, mencionamos los equipos con restricción:

- Plataforma Huawei (Quidway – H3com - Hp). Atributo Login Service No estandarizado para protocolo SSH
- Caso CISCO SR 636423903 – Modificar el diccionario IETF para agregar atributo que autorice la gestión por SSH
- Caso Huawei SR 5214266 – Actualización de VRP que se ajuste al estándar. Respuesta del proveedor "Cambio de equipos por AR G3 o 1200"

El proyecto supone que el costo de mano de obra de las personas involucradas en las diferentes actividades no se tendrá en cuenta a la hora se sacar el presupuesto general del proyecto ya que son empleados de la compañía que actualmente están laborando en la empresa y sin importar si participan o no en el proyecto seguirán devengando el mismo sueldo. Tampoco se hará ninguna contratación adicional en este proyecto.

## 1.7 INGENIERÍA DE DISEÑO

### 1.7.1 Servicio de datos

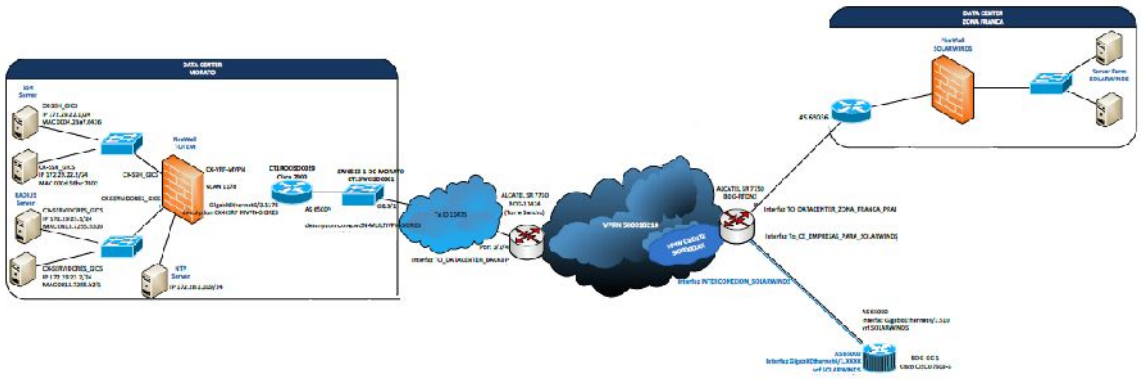
La solución de conectividad de la VPRN de clientes con los servidores SSH y RADIUS, se basa en la interconexión principal sobre el PE BOG-RTDN3 hacia el router de Gestión Clientes Cisco BOG-GC-1 (CISCO7609-S) y la interconexión backup sobre el PE BOG-41000 hacia el router de Gestión Clientes Cisco BOG-GC-2 (CISCO7609-S).

Dependiendo si la VPRN del cliente está aprovisionada o no en alguno de los PE de interconexión se tienen dos tipos de topología que son: SAP y Epipe.

#### 1.7.1.1 Topología con interconexión SAP

Este tipo de interconexión se tiene a través de un SAP asociado a una VLAN de interconexión asignada al cliente como se observa en la siguiente figura. Ver ilustración 2.

Ilustración 2 Interconexión SAP

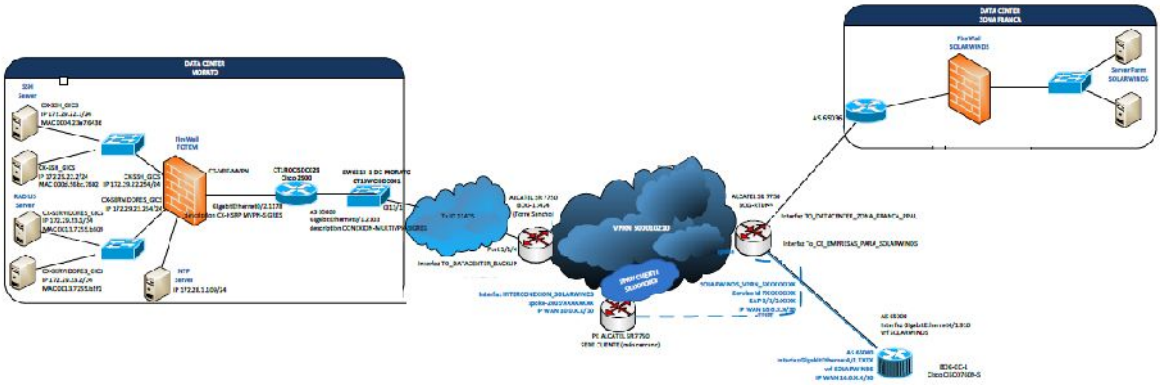


Diseño realizado en Visio

### 1.7.1.2 Topología con interconexión Epipe

En este tipo de interconexión la VPRN no se encuentra aprovisionada en el P.E de interconexión backup o principal, la interconexión se tiene a través de un Epipe en el P.E más cercano a los P.E de interconexión como se muestra en la ilustración 3.

Ilustración 3 Interconexión Epipe



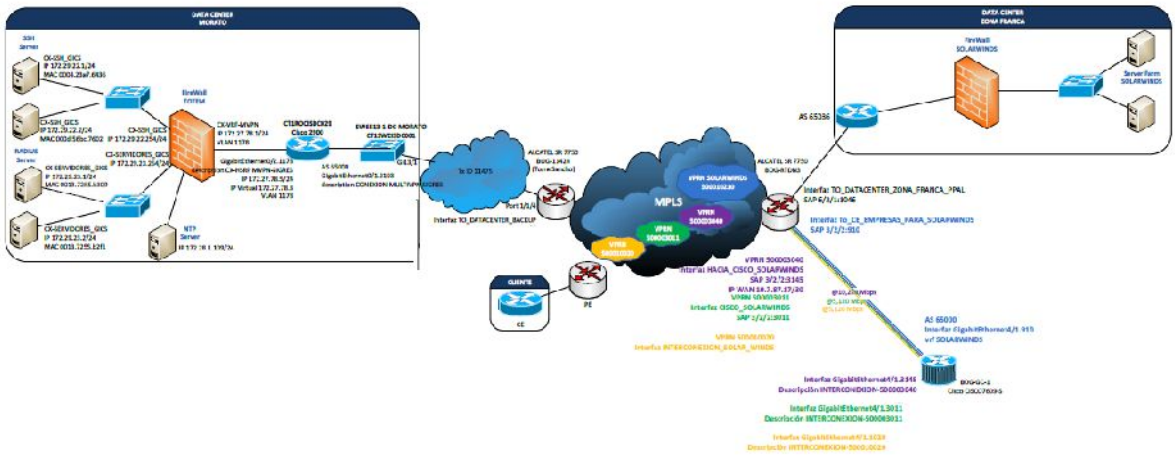
Diseño realizado en Visio

### 1.7.2 Servicio de internet

La solución de conectividad de las VPRN de Internet con los servidores SSH y RADIUS, se basa en las tres (3) interconexiones fijas en BOG-RTDN3 puerto 3/2/2 hacia las VPRN de Internet que son: 50000XXXX.

En la iustración 4 se muestra el diagrama de la topología de detalle de la solución de Interconexión entre las VPRN de Internet y la VPRN SOLARWINDS para dar conectividad con los servidores Movistar MAS, SSH, RADIUS y NTP.

Ilustración 4 Interconexión Internet

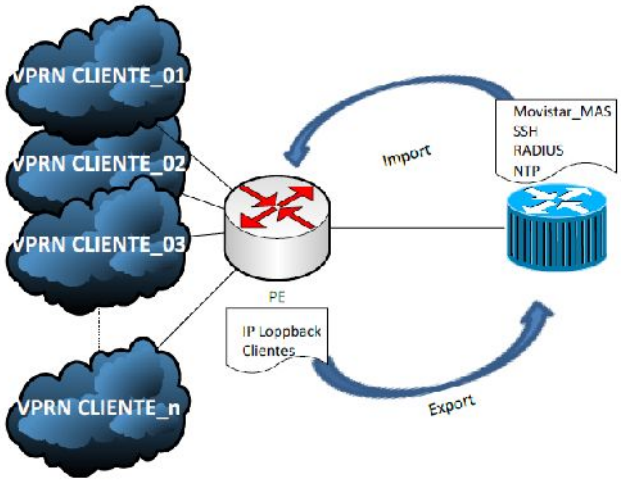



Diseño realizado en Visio

### 1.7.3 Enrutamiento

Se debe modificar la política de importación del BGP entre la VPRN del cliente y el router Cisco Gestión Clientes para importar el segmento de servidores MOVISTAR_MAS, SSH, RADIUS y NTP y así tener conectividad con este servicio como se observa en la ilustración 5.

Ilustración 5 Enrutamiento para políticas de importación




Diseño realizado en Visio

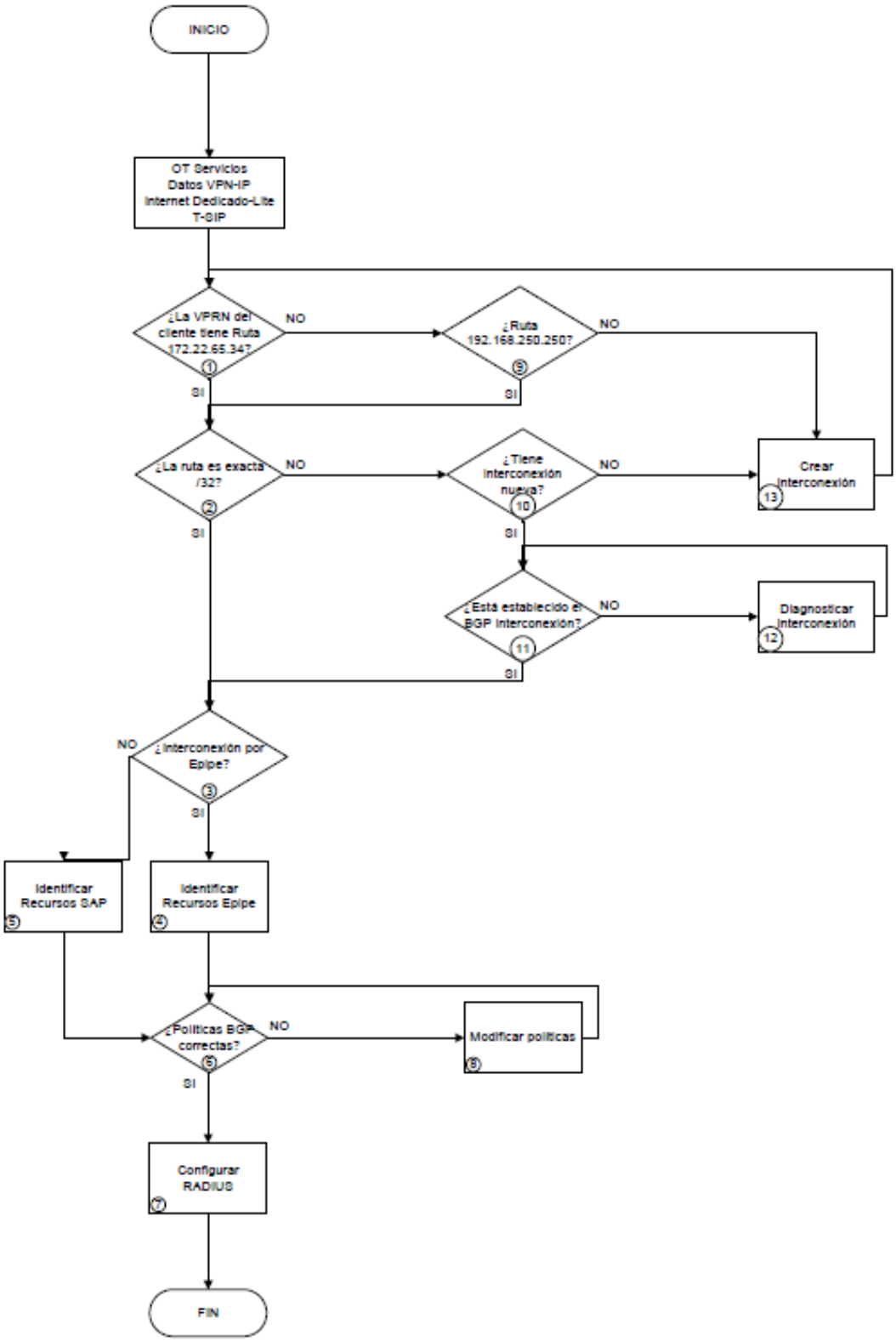
### 1.7.4 Información técnica de configuración SSH & RADIUS CPE

Para configurar el servicio SSH y RADIUS en los CPE, se debe verificar si la VPRN del cliente tiene conectividad con los servidores SSH y RADIUS, de ser así se puede proceder a configurar el servicio sobre los CE, en caso contrario, se debe diagnosticar el por qué no se tiene conectividad con estos servidores, realizar los ajustes necesarios a nivel de red para luego proceder a realizar la configuración del servicio sobre los CE.
Si se requiere diagnosticar la conectividad de la VPRN del cliente con los servidores SSH y RADIUS, se debe establecer el tipo de interconexión hacia estos servicios, la cual puede ser:

- Interconexión por Inter-VPRN.
- Interconexión por Epipe.
- Interconexión por SAP.

En el diagrama de flujo ilustración 6 se describe el procedimiento para la configuración del servicio SSH y RADIUS, en él se esboza el paso a paso para diagnosticar el tipo de interconexión, los recursos de interconexión y las políticas de enrutamiento con el fin de determinar los cambios a nivel de red para tener conectividad con estos servicios.

Ilustración 6 Diagrama de flujo de configuración y verificación



### 1.7.5 Configuración plataforma Cisco

La compatibilidad con la versión 2.0 de SSH (SSH v2) se comenzó a incluir en imágenes de IOS desde la versión 12.4 del software Cisco IOS salvo las versiones ipbase de IOS. Igualmente, las versiones de software Cisco IOS 11.1.1 en adelante soportan el protocolo RADIUS. Los comandos de configuración varían ligeramente de una plataforma a otra, siendo este template la base para habilitar el servicio SSH y RADIUS en los routers CISCO.

Se debe asegurar que se tiene conectividad desde el servidor SSH con la IP loopback del CPE a configurar; para tal requerimiento hacer ping desde la consola del servidor SSH hacia la IP loopback del CPE. Luego ingresar al modo de configuración (configure terminal) del router para aplicar los comandos de configuración.

Como de medida de seguridad se recomienda crear un usuario en el router en caso de perder conectividad con los servidores de RADIUS y poder tener gestión local del equipo Como se muestra en la tabla 2. Tener en cuenta que las claves que se usan en este documento son de ejemplo para quien consulte el documento y no hacen parte de ninguna red en específico.

Tabla 2 Medida de seguridad en la configuración del protocolo Cisco

| Comando | Observaciones |
|---|---|
| username telecom privilege 15 secret USTA | Crea el usuario en el router para tener gestión en caso de pérdida de conectividad con RADIUS; el privilegio debe ser siempre 15 para tener privilegios de administrador |
| enable secret ProyectoUSTA | Crea password enable |
| service password-encryption | Encripta todas las claves en el router |

Ahora, se procede a realizar la configuración del nuevo modelo AAA a aplicar en el router sobre el protocolo RADIUS como se muestra en la tabla 3.

Tabla 3 Configuración del nuevo modelo AAA Cisco

| Comando | Observaciones |
|---|---|
| aaa new-model | Crea modelo de AAA nuevo |
| aaa authentication login default group radius local | Autentica primero contra RADIUS y si no hay conectividad usa usuario local |
| aaa authorization exec default group radius if-authenticated | Autoriza los privilegios asociados al grupo RADIUS |
| aaa accounting exec default start-stop group radius | Administra la sesión establecida |
| aaa authorization console | Solicita password cuando se ingresa por consola |

| Comando | Observaciones |
|---|---|
| radius-server host XX.XX.XX.XX auth-port 1812 acct-port 1813 key 7 1145B2255097F6079 | Apunta al servidor RADIUS primario |
| radius-server host XX.XX.XX.XX auth-port 1812 acct-port 1813 key 7 11B2255097F6079 | Apunta al servidor RADIUS secundario |

Ya para finalizar se crea un dominio en el router, se establece el protocolo de gestión SSHv2 sobre las líneas VTY. Ver tabla 4.

Tabla 4 Protocolo de gestión SSH v2 Cisco

| **Comando** | **Observaciones** |
|---|---|
| ip domain name proyecto.esp | Crea dominio |
| crypto key generate rsa | Genera la llave rsa para ssh |
| 1024 | bits de la llave de ssh |
| ip ssh version 2 | Establece el timeout de la sesión ssh |
| ip ssh time-out 120 | Habilita la versión sshv2 |
| ip ssh authentication-retries 3 | Establece la cantidad de intentos fallidos |
| line vty 0 4 | Ingresa a las líneas vty |
| transport input ssh | Habilita ssh como el protocolo de ingreso |

Una vez finalizado la configuración y antes de guardar la configuración realizada, abrir otra sesión SSH, donde se verificará la gestión del router a través de ssh con el usuario de RADIUS asignado y, de ser exitosa la gestión se salva la configuración.

### **1.7.6** Configuración plataforma Huawei

Dependiendo de la versión de software Huawei VRP los comandos de configuración varía ligeramente. Las versiones de software Huawei VRP homologadas para la configuración del servicio SSH y RADIUS son las versiones 3.4 y 5.2.

Al igual que para los router Cisco, Se debe asegurar que se tiene conectividad desde el servidor SSH con la IP loopback del CPE a configurar; para tal requerimiento hacer ping desde la consola del servidor SSH hacia la IP loopback del CPE. Luego ingresar al modo de configuración (system-view) del router para aplicar los comandos de configuración. Tener en cuenta la versión VRP del router para de esta manera escoger la sintaxis de los comandos a ingresar.

Como de medida de seguridad se recomienda crear un usuario en el router en caso de perder conectividad con los servidores de RADIUS y poder tener gestión local del equipo

Como se muestra en la tabla 5. Tener en cuenta que las claves que se usan en este documento son de ejemplo para quien consulte el documento y no hacen parte de ninguna red en específico.

Tabla 5 Medida de seguridad en la configuración del protocolo Huawei

| Comando | | Observaciones |
|---|---|---|
| VRP versión 3.4 | VRP versión 5.2 | |
| local-user proyectoUSTA | local-user proyectoUSTA | Crea un usuario local en caso que se pierda conectividad con el servidor RADIUS |
| level 3 | authorization-attribute level 3 | Asigna privilegios nivel administrador |
| password cipher USTA2016 | password cipher USTA2016 | Generar password para el usuario local |
| service-type ssh | service-type ssh | Habilita el ingreso vía ssh |

Ahora, se procede a realizar la configuración del nuevo modelo AAA a aplicar en el router sobre el protocolo RADIUS como se muestra a continuación en la tabla 6.

Tabla 6 Configuración del nuevo modelo AAA Huawei

| Comando | | Observaciones |
|---|---|---|
| VRP versión 3.4 | VRP versión 5.2 | |
| radius scheme telefónica | radius scheme telefonica | Crea el esquema de RADIUS con nombre telefónica |
| server-type huawei | server-type extended | Habilita el servicio basado en extensión RADIUS de HUAWEI |
| authentication primary ip 172.29.23.2 key simple ProyectoUSTA | primary authentication 172.29.23.2 | Autenticación principal RADIUS |
| accounting primary ip 172.29.23.2 key simple ProyectoUSTA | primary accounting XX.XX.XX.XX | Accounting principal RADIUS |
| authentication secondary ip 172.29.23.1 key simple ProyectoUSTA | secondary authentication XX.XX.XX.XX | Autenticación secundaria RADIUS |

| Comando | | Observaciones |
|---|---|---|
| VRP versión 3.4 | VRP versión 5.2 | |
| accounting secondary ip 172.29.23.1 key simple ProyectoUSTA secondary | secondary accounting XX.XX.XX.XX | Accounting secundaria RADIUS |
| | key authentication ProyectoUSTA | llave de autenticación |
| user-name-format without-domain | key accounting ProyectoUSTA | llave de Accounting |
| nas-ip XX.XX.XX.XX | user-name-format without-domain | Formato del usuario sin dominio |
| accounting-on enable | nas-ip XX.XX.XX.XX | Especifica la dirección IP del cliente RADIUS |
| accounting-on enable | | Habilita el envío de paquetes |

Ya para finalizar se crea un dominio en el router, se establece el protocolo de gestión SSHv2 sobre las líneas VTY. Ver tabla 7.

Tabla 7 Protocolo de gestión SSH v2 Huawei

| Comando | | Observaciones |
|---|---|---|
| VRP versión 3.4 | VRP versión 5.2 | |
| domain USTA | domain USTA | Crea el dominio USTA |
| authentication radius-scheme USTA local | authentication default radius-scheme telefonica local | Esquema de Autenticación primerio RADIUS y luego usuario local |
| | authorization default radius-scheme telefonica local | Esquema de Autorización primero RADIUS y luego usuario local |
| accounting radius-scheme USTA | accounting default radius-scheme telefonica | Esquema de accounting |
| domain default enable USTA | domain default enable USTA | Habilita el dominio configurado por defecto |

| Comando | | Observaciones |
|---|---|---|
| VRP versión 3.4 | VRP versión 5.2 | |
| | ssh server enable | Habilita el servidor ssh |
| rsa local-key-pair create | public-key local create rsa | Crear llave rsa |
| 1024 | 1024 | Crear llave de 1024 bits |
| ssh authentication-type default password | | Especifica el password de Autenticación por defecto |
| user-interface vty 0 4 | user-interface vty 0 4 | Ingresar a las lineas vty |
| authentication-mode scheme domain USTA | authentication-mode scheme | Configura el esquema de ingreso al router |
| protocol inbound ssh | protocol inbound ssh | Solo permite ingreso via ssh |

Una vez finalizado la configuración y antes de guardar la configuración realizada, abrir otra sesión SSH, donde se verificará la gestión del router a través de ssh con el usuario de RADIUS asignado y, de ser exitosa la gestión se salva la configuración.

## 1.8 CONTROL DE CAMBIOS

Para el proceso de control de cambios se debe seguir la siguiente secuencia de actividades como se muestra en la ilustración 7:

Ilustración 7 Control de cambios

La aprobación para hacer cualquier cambio en el proyecto debe ser aprobada por el gerente del proyecto y debe quedar un registro en un formato como lo muestra la tabla 8.

Tabla 8 Control de cambios

| Actividad | Versión | Fecha | Responsable | Descripción |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

# 2 GESTIÓN DEL TIEMPO

## 2.1 DEFINICIÓN DE ACTIVIDADES

Para este primer grupo de actividades se tiene contemplada la aprobación de presupuesto para proceder con la adquisición de cada una de los equipos según los tiempos estipulados en la tabla 9 de actividades, para que una vez sea recibido a satisfacción por el Jefe de aseguramiento se proceda con la integración de la nueva plataforma.

Tabla 9 Actividades de renovación tecnológica

| Actividades | Tiempo de ejecución | Responsables (área) |
|---|---|---|
| Elección de Plataforma | 5 días | Aseguramiento |
| Cotización | 11 días | Jefe de gestión y aseguramiento |
| Solicitud de presupuesto | 9 días | Aseguramiento |
| Aprobación de presupuesto | 45 días | Jefe de gestión y aseguramiento |
| Orden de Compra | 25 días | Jefe de gestión y aseguramiento |
| Entrega | 59 días | Jefe de gestión y aseguramiento |
| Recibo a satisfacción equipos | 1 día | Aseguramiento |

En esta parte de las actividades el área de aseguramiento realizará cada una de las labores descritas en la tabla 10 con el fin de garantizar que al iniciar la configuración sobre la red y equipos tanto del cliente como de la empresa no se tenga ningún tipo de retraso o riesgo de que alguna actividad haya quedado sin realizar.

Tabla 10 Actividades de integración nueva plataforma

| Actividades | Tiempo de ejecución | Responsables (área) |
|---|---|---|
| Viabilidad Espacio y Energía | 2 día | Aseguramiento |
| Configuración | 24 días | Aseguramiento |
| Homologación | 60 días | Aseguramiento |
| Instalación | 5 días | Aseguramiento |
| Migración Nueva Plataforma | 5 días | Aseguramiento |
| Pruebas FAILOVER y RESILIENCE | 5 días | Aseguramiento |
| Acta de entrega del servicio | 1 día | Aseguramiento |

En la conectividad de datos, configuración de conectividad y verificación de redundancia. Se hace en conjunto con el área de aseguramiento, calidad y soporte ya que implica trabajar sobre los recursos que provee movistar MAS y pruebas sobre los equipos adquiridos en las primeras actividades desarrolladas. Aquí las pruebas de failOver y

redundancia son de gran importancia ya que son las que nos entregan la aprobación para iniciar la siguiente actividad. Ver tabla 11.

Tabla 11 Actividades de configuración red Telefónica

| Actividades | Tiempo de ejecución | Responsables (área) |
|---|---|---|
| Ingeniería de conectividad Datos e Internet | 72 días | Aseguramiento |
| Levantamiento de Topología | 11 días | Aseguramiento |
| Diseño de la solución | 45 días | Aseguramiento |
| Definir Servidor NTP | 10 días | Aseguramiento |
| Conectividad Servidor NTP | 5 días | Aseguramiento |
| Modificación de políticas ANEXO TÉCNICO | 6 días | Aseguramiento |
| Aprobación Modificación Políticas | 10 días | Aseguramiento |
| Configuración conectividad Internet | 7 días | Soporte técnico |
| VPRN 500003040 | 7 días | Soporte técnico |
| VPRN 500003011 | 7 días | Soporte técnico |
| VPRN 500010020 | 7 días | Soporte técnico |
| Configuración conectividad Datos | 10 días | Aseguramiento |
| Modificación Políticas de Importación | 10 días | Calidad |
| Modificación Políticas de Exportación | 10 días | Calidad |
| Aprovisionamiento Redundancia Conectividad Servidores | 35 días | Aseguramiento |
| Diseño de la solución | 10 días | Aseguramiento |
| Asignación de recursos de red | 10 días | Aseguramiento |
| Aprovisionamiento | 10 días | Aseguramiento |
| Pruebas de FAILOVER y RESILIENCE | 5 días | Aseguramiento |
| Release ANEXO TÉCNICO | 119 días | Aseguramiento |

La socialización y entrega de documentos tanto de configuración como de troubleshooting Se realizará con cada una de las áreas con el fin de dejar claro las modificaciones que se realizaran y como se configuraran los nuevos servicios, para que de esta forma se den los primeros pasos en el inicio de la fase II. Ver tabla 12.

Tabla 12 Actividades de anexo técnico configuración SSH & RADIUS CPE

| Actividades | Tiempo de ejecución | Responsables (área) |
|---|---|---|
| Diagrama de Flujo | 5 días | Aseguramiento |

| Actividades | Tiempo de ejecución | Responsables (área) |
|---|---|---|
| Manual de Configuración | 20 días | Aseguramiento |
| Socialización con las áreas involucradas | 15 días | Aseguramiento |
| Modificación Proceso Implantación | 5 días | Líder de implantación |
| Acta aceptación Implantación | 5 días | Líder de implantación |
| Documentación Anexo Técnico | 1 día | Aseguramiento |

De acuerdo a la base de datos que se tiene de los clientes que ya tienen configurado el servicio de movistar MAS se realiza una cuantificación y se definen los grupos de trabajo para dar inicio a la configuración en cada uno de los routers instalados en la sede de los clientes. Adicionalmente se creará una base de datos sobre los equipos que no pudieron ser configurados ya sea porque no se tiene gestión de los mismos o que por versión no permiten la configuración del protocolo. Ver tabla 13.

Tabla 13 Actividades de configuración de CPE

| Actividades | Tiempo de ejecución | Responsables (área) |
|---|---|---|
| Plan de Migración | 3 días | Aseguramiento |
| Cuantificación servicios por Fase | 3 días | Aseguramiento |
| Definir grupo de trabajo | 1 día | Aseguramiento |
| Programación por Fases | 1 día | Aseguramiento |
| Socialización Anexo Técnico Configuración | 1 día | Aseguramiento |
| Acta Plan de Migración | 1 día | Aseguramiento |
| Fase I | 61 días | Aseguramiento |
| Migración Fase I | 30 días | Aseguramiento |
| Inventario Fase I | 30 días | Aseguramiento |
| Solución servicios no configurados Fase I | 30 días | Aseguramiento |
| Acta migración Fase I | 1 día | Aseguramiento |

## 2.2 CRONOGRAMA GENERAL DEL PROYECTO.

En la tabla 14 se presenta el cronograma, donde se muestra las actividades en general y tiempo total de ejecución de la misma en cada una de las actividades propuestas para el desarrollo completo del proyecto.

Tabla 14 Cronograma general del proyecto

| Nombre de tarea | Duración |
|---|---|
| Renovación tecnológica | 155 días |
| Integración Nueva Plataforma | 160 días |
| Configuración Red Telefónica | 119 días |
| Anexo Técnico Configuración SSH&RADIUS CPE | 51 días |
| Configuración de CPE | 189 días |

## 2.3 CRONOGRAMA DETALLADO POR FASES

La tabla 15 muestra el cronograma detallado por fases según se mencionó en el punto 1.2 (planificación, implementación y cierre) donde se relaciona cada una de las actividades a realizar y el tipo de labor que se va a ejecutar teniendo en cuenta los días propuestos para cada actividad.

Tabla 15 Cronograma detallado por fases

| Actividades | Duración | Fase |
|---|---|---|
| Renovación tecnológica | 155 días | Planificación |
| Elección de Plataforma | 5 días | Planificación |
| Cotización | 11 días | Planificación |
| Solicitud de presupuesto | 9 días | Planificación |
| Aprobación de presupuesto | 45 días | Planificación |
| Orden de Compra | 25 días | Planificación |
| Entrega | 59 días | Planificación |
| Recibo a satisfacción equipos | 1 día | Cierre |
| Integración Nueva Plataforma | 160 días | Implementación |
| Viabilidad Espacio y Energía | 2 días | Implementación |
| Configuración | 24 días | Implementación |
| Homologación | 60 días | Implementación |
| Instalación | 5 días | Implementación |

| Actividades | Duración | Fase |
|---|---|---|
| Migración Nueva Plataforma | 5 días | Implementación |
| Pruebas FAILOVER y RESILIENCE | 5 días | Implementación |
| Acta de entrega del servicio | 1 día | Cierre |
| Configuración Red Telefónica | 119 días | Implementación |
| Ingeniería de conectividad Datos e Internet | 72 días | Planificación |
| Levantamiento de Topología | 11 días | Planificación |
| Diseño de la solución | 45 días | Planificación |
| Definir Servidor NTP | 10 días | Planificación |
| Conectividad Servidor NTP | 5 días | Implementación |
| Modificación de políticas ANEXO TÉCNICO | 6 días | Implementación |
| Aprobación Modificación Políticas | 10 días | Cierre |
| Configuración conectividad Internet | 7 días | Implementación |
| VPRN 500003040 | 7 días | Implementación |
| VPRN 500003011 | 7 días | Implementación |
| VPRN 500010020 | 7 días | Implementación |
| Configuración conectividad Datos | 10 días | Implementación |
| Modificación Políticas de Importación | 10 días | Implementación |
| Modificación Políticas de Exportación | 10 días | Implementación |
| Aprovisionamiento Redundancia Conectividad Servidores | 35 días | Implementación |
| Diseño de la solución | 10 días | Planificación |
| Asignación de recursos de red | 10 días | Implementación |
| Aprovisionamiento | 10 días | Implementación |
| Pruebas de FAILOVER y RESILIENCE | 5 días | Implementación |
| Release ANEXO TÉCNICO | 119 días | Cierre |
| Anexo Técnico Configuración SSH&RADIUS CPE | 51 días | Implementación |
| Diagrama de Flujo | 5 días | Implementación |
| Manual de Configuración | 20 días | Implementación |
| Socialización con las áreas involucradas | 15 días | Implementación |
| Modificación Proceso Implantación | 5 días | Implementación |
| Acta aceptación Implantación | 5 días | Cierre |
| Documentación Anexo Técnico | 1 día | Cierre |
| Configuración de CPE | 140 días | Implementación |
| Plan de Migración | 3 días | Planificación |
| Cuantificación servicios por Fase | 3 días | Implementación |
| Definir grupo de trabajo | 1 día | Planificación |
| Programación por Fases | 1 día | Planificación |
| Socialización Anexo Técnico Configuración | 1 día | Planificación |

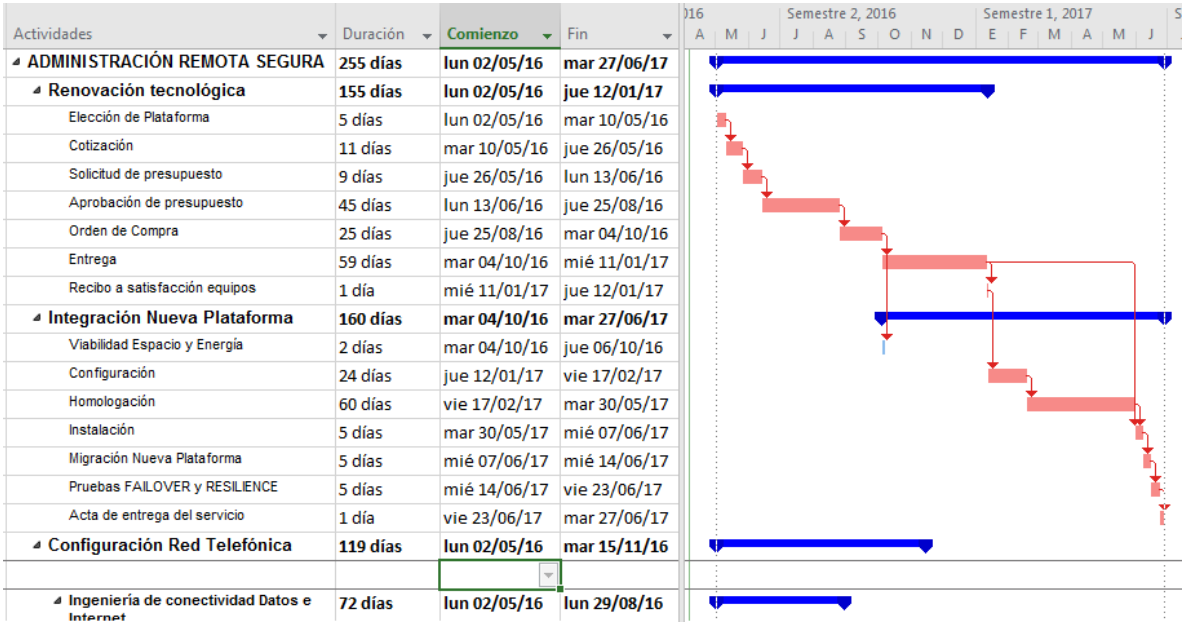
| Actividades | Duración | Fase |
|---|---|---|
| Acta Plan de Migración | 1 día | Cierre |
| Fase I | 61 días | Implementación |
| Migración Fase I | 30 días | Implementación |
| Inventario Fase I | 30 días | Implementación |
| Solución servicios no configurados Fase I | 30 días | Implementación |
| Acta migración Fase I | 1 día | Implementación |

## 2.4 DEFINICIÓN Y ANÁLISIS DE RUTAS CRÍTICAS

La ruta crítica se define como la secuencia de actividades que deben ser completadas según el cronograma planteado en el proyecto de tal manera que se termine de acuerdo a este. Si se presentara algún retraso en uno de estas actividades afecta completamente al proyecto.

En la ilustración 8 se muestra la ruta crítica para este proyecto la cual está señalada en color rojo. Si alguna de estas actividades que están dentro de la ruta crítica sufren un retraso afectaría el cronograma establecido en un comienzo y puede llevar a un sobrecosto en el proyecto y retraso del mismo.

Ilustración 8 Ruta crítica




Diseño hecho en Microsoft Project

## **2.5** METODOLOGÍA PARA EL CONTROL DEL CRONOGRAMA

Para controlar y hacer seguimiento al proyecto se definirán reuniones semanales en donde se entregarán informes de las actividades y el porcentaje de cumplimiento de las mismas.

De acuerdo a los avances entregados de las actividades el gerente de proyecto debe tomar la decisión de hacer cambios en el cronograma o establecer planes de acción para cumplir con las fechas establecidas para finalizar cada actividad.

# 3 GESTIÓN DE COSTOS

## 3.1 PRESUPUESTO GENERAL ESTIMADO

El presupuesto general del proyecto se calcula de la suma de los valores de los equipos y demás elementos requeridos para la conectividad en la red de Telefónica. No se tendrá en cuenta los costos operativos ya que no se hará ninguna contratación adicional de alguna persona para el desarrollo del proyecto.

Debemos tener en cuenta que las personas que desarrollan las actividades del proyecto tienen un contrato indefinido, pero no estarán exclusivamente dedicadas al proyecto planteado y continúan devengando el mismo sueldo participen o no en alguna actividad.

Debido a las diferentes variaciones del dólar en Colombia el presupuesto se estima en COP$ 160.000.000.

## 3.2 DESGLOSE DE COSTOS DEL PROYECTO (PAGOS, MENSUALIDADES, COMPRAS, ETC.)

En la tabla se muestra el detalle de los equipos que se van a comprar, también se incluyen las licencias que debe los equipos y el soporte que se debe solicitar al proveedor para el servicio principal y backup.

En la primera compra el equipo Cisco Secure Access Control System se adquiere con la licencia y el soporte por 12 meses. Para los siguientes dos años se compran únicamente el soporte.

Tabla 16 Desglose de costos del proyecto

| ID | 2016 | 2017 | 2018 | TOTAL |
|---|---|---|---|---|
| CAPEX | (2) Cisco Secure Access Control System<br>Licencia: SNS-3415K9<br>(2) Licencia Large Deployment: CSACS-5-LRG-LIC x 12 meses | (2) Soporte SMARTNET 8X5XNBD Large Secure Server x 12 meses<br>USD 3.543 | (2) Soporte SMARTNET 8X5XNBD Large Secure Server x 12 meses<br>USD 3.543 | USD 41.108,88 |

| ID | 2016 | 2017 | 2018 | TOTAL |
|---|---|---|---|---|
| | (2) Soporte SMARTNET 8X5XNBD Large Secure Server x 12 meses<br><br>USD$ 34022,88 | | | |
| | (2) Servidores SSH<br><br>USD$ 6.086 | UCS SUPP PSS 24X7X4 UCS C220 M3 SFF w/o<br><br>USD 2.412 | UCS SUPP PSS 24X7X4 UCS C220 M3 SFF w/o<br><br>USD 2.412 | USD 10.910 |
| TOTAL<br>** TRM 3.000 | USD$ 40.108,88<br>COP$ = 120.326.640 | USD$ 5.955<br>COP$ 17.865.000 | USD$ 5.955<br>COP$ 17.865.000 | USD$ 52.018,88<br>COP$ 156.056.640 |

## 3.3 CONTROL DE COSTOS.

En la tabla 17 se muestra un registro del costo acumulado cada año con el fin de llevar un registro de los costos del proyecto. En la figura 9 se puede ver gráficamente como es el comportamiento del costo acumulado en los tres primeros años de funcionamiento del proyecto.

Tabla 17 Costo acumulado

| Año | Costo acumulado |
|---|---|
| 2015 | $ 0 |
| 2016 | $ 120.326.640 |
| 2017 | $ 138.191.640 |
| 2018 | $ 156.056.640 |

Ilustración 9 Costo acumulado


Para tener un control sobre los cambios que pueda tener el proyecto respecto a los costos, se tendrá un control registrando los datos para comparar las variaciones y deducir si hay sobrecostos o disminución en el costo planeado inicialmente. En la tabla 18 se muestra como se hace el registro.

- AC = Costo Actual. Es el costo real del trabajo realizado en el momento del análisis.

- PV = Valor Planificado. Representa el costo del presupuesto para todas las tareas que fueron planeadas empezar y terminar en el momento del análisis.

- EV = Valor Ganado. Representa la suma de todo el costo del presupuesto del trabajo realizado en el momento del análisis.

Tabla 18 Técnica del valor ganado

| Año | Valor planeado (PV) | Costo actual (AC) | Valor ganado (EV) |
|---|---|---|---|
| 2015 | $ 0 | $ 0 | $ 0 |
| 2016 | | | |
| 2017 | | | |
| 2018 | | | |

# 4 GESTIÓN DE CALIDAD DEL PROYECTO

## 4.1 PLANIFICACIÓN DE LA CALIDAD

Ya que el alcance del proyecto en la primera fase está limitado a los servicios monitoreados por Movistar Más, se dará inicio con un plan de información y capacitación de la siguiente manera:

### 4.1.1 Servicios con movistar MAS ya instalados

De acuerdo a la base de datos suministrada por la herramienta movistar MAS se procederá a distribuir en el área de soporte técnico para cada coordinador de área una lista de los canales a los cuales se les realizará la configuración la respectiva configuración del protocolo. Cada ingeniero que realice el trabajo de configuración deberá documentar sobre la misma lista entregada si el proceso se realizó de forma correcta, sobre que marca de router, y versión del equipo. De la misma forma se documentará si no se logró realizar la configuración con una pequeña descripción del inconveniente presentado.

Dado el caso de que la configuración no se pueda realizar por que no se tiene gestión de los equipos por problemas en la contraseña de ingreso, se procederá a generar un incidente desde el área de soporte técnico, con el fin de enviar personal técnico a la sede del cliente, donde se realizará la respectiva recuperación de contraseña y adicionalmente y de forma inmediata la configuración del protocolo.

### 4.1.2 Órdenes de trabajo ejecutadas como altas y modificaciones para los ingenieros de implantación

Para este caso se informará y capacitará al grupo de implantación para que cada una de las órdenes de trabajo que sean ejecutadas como tipo alta y modificación para todo canal de datos (ya sea VPN-IP, internet dedicado o LITE y troncal SIP) le sea configurado el protocolo de seguridad.

### 4.1.3 Órdenes de trabajo revisadas como altas y modificaciones para los ingenieros de calidad

Cada uno de los ingenieros será informado y capacitado y adicionalmente garantizaran que, por parte del área de implantación para cada uno de los servicios de datos, estos contengan la respectiva y correcta de la configuración del protocolo de seguridad.

## 4.2 ASEGURAMIENTO DE LA CALIDAD

Para garantizar la completa seguridad de la información de cada equipo gestionado por Telefónica basado en la configuración del protocolo se realizará así:

## 4.3 Servicios con movistar MAS ya instalados

En el área de soporte, es responsabilidad de los coordinadores de área validar que las listas entregadas hayan sido diligenciadas correctamente por cada uno de los ingenieros que realizaron la configuración. Adicionalmente el coordinador deberá reportar al área de aseguramiento los equipos de los cuales no se tuvo gestión para que de esta manera se realice una lista y se programen las visitas técnicas para el restablecimiento de contraseña y se proceda con la configuración del protocolo de seguridad.

La información será entregada por parte del coordinador o líder en la tabla 19 que se muestra a continuación con el fin de asegurar la completa información.

Tabla 19 Seguimiento a movistar MAS

| Ingeniero | Loopback de Gestión y Monitoreo | RADIUS (si/no) | Tipo de Router | Modelo | Observaciones |
|---|---|---|---|---|---|
| | | | | | |

### 4.3.1 Órdenes de trabajo revisadas como altas y modificaciones para los ingenieros de calidad

La metodología aplicar por parte del área de calidad será que, cuando al revisar una orden de trabajo referente a un servicio de datos y que no contenga la configuración del protocolo de seguridad, se procederá a generar una tarea a nombre del ingeniero de implantación sobre la orden de trabajo, quien tendrá que realizar la respectiva verificación y configuración de la misma. Esta será la manera de controlar la correcta ejecución del protocolo en cada uno de los routers que se encuentran en la sede del cliente.

La tarea que se generará tendrá la siguiente forma sobre la orden de trabajo. Ver tabla 20.

Tabla 20 Seguimiento a configuración

| Número de OT | Cliente | Observaciones | Responsable Revisión implantación | N° Tarea de Calidad | Tipo de servicio |
|---|---|---|---|---|---|
| | | | | | |

## 4.4 CONTROL DE CALIDAD

El control de calidad estará a cargo del área de calidad quien tendrá la labor de revisar cada una de las tareas generadas hacia el área de implantación, ingresando al router y verificando que la configuración se haya realizado correctamente. Una vez hecha la validación de procederá a cambiar el estado de la tarea a cerrada y respuesta positiva.

De no estar correctamente realizada la configuración del protocolo, se mantendrá la tarea aún abierta y su estado en desarrollo.
La tabla que se utilizará para mantener una base de datos actualizada será la siguiente (Ver tabla 21).

Tabla 21 Control de calidad

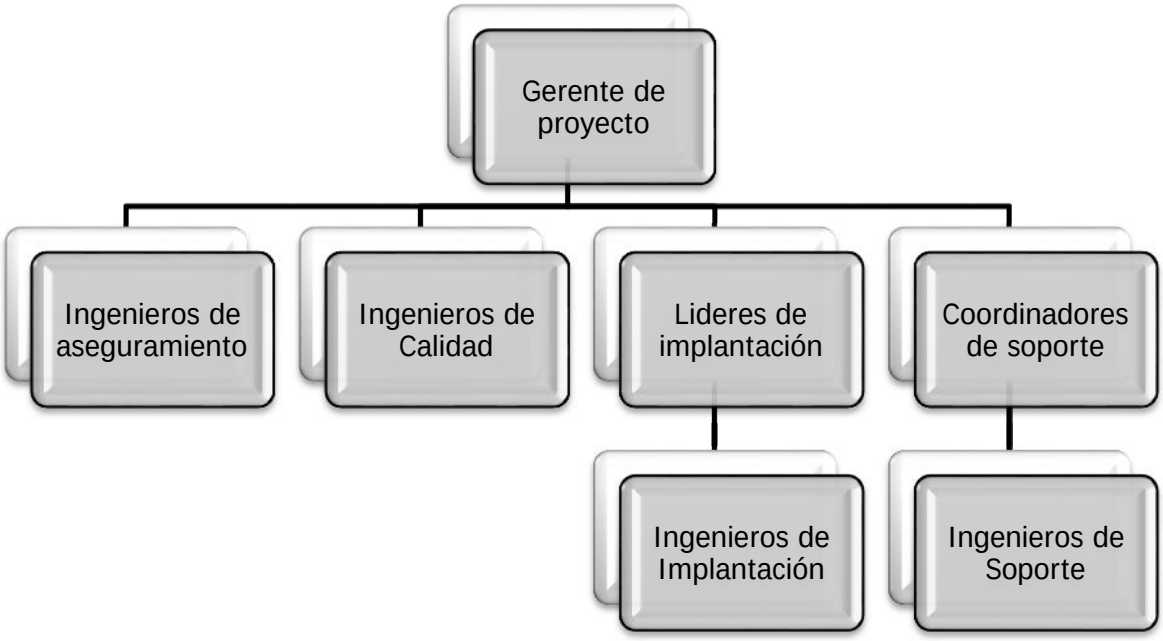
| Número de OT | Cliente | Observaciones | Responsable Revisión implantación | Tarea de Calidad | Tipo de servicio | Respuesta | Estado |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

# 5 GESTIÓN DEL RECURSOS HUMANO

## 5.1 ORGANIGRAMA INTERNO DEL PROYECTO

Para el proyecto se tiene asignado un marco jerárquico que se muestra a continuación ( Ver ilustración 10), el cual permitirá culminar el proyecto de forma positiva. Cada grupo tiene labores asignadas de acuerdo a las habilidades y perfil requerido. De ser necesario algún tipo de solicitud o requerimiento de parte de alguno de los grupos funcionales, pueden ser remitidos al siguiente nivel quien atenderá de manera oportuna la solicitud. De no poderse atender la solicitud o requerimiento este será escaldo al siguiente nivel y así sucesivamente hasta entregar la correspondiente solución.

Ilustración 10 Organigrama interno




## 5.2 ORGANIGRAMA EXTERNO DEL PROYECTO (CLIENTE-PROVEEDORES)

Ya que la gestión de los equipos la hace directamente Telefónica, para el cliente esta configuración que se realiza es totalmente transparente, lo cual implica que cada uno de los clientes en ningún momento verá afectado su servicio o tendrá que reportar algún tipo de falla al respecto sobre esta configuración.

Para el cliente es un valor agregado sobre el servicio que no incrementará de alguna forma los costos de su servicio, si no que le brindará una mayor seguridad sobre el canal que contrató, ya que se podrá tener más control y administración de los ingenieros que ingresan a la información de estos routers y validar que tipo de cambios se realizaron y cuantas veces se realizó un ingreso, identificando adicionalmente la persona que ingreso.

## 5.3 MATRIZ DE RESPONSABILIDADES

A cada uno de los grupos funcionales se les estableció una responsabilidad específica de acuerdo a los perfiles del cargo que se tiene. Esto con el fin de garantizar que cada una de las tareas asignadas se desarrolle sin ningún tipo de complicación.
También de esta manera es mucho más fácil validar fallas o inconvenientes que se presenten en cada una de las áreas que tienen asociada una responsabilidad específica ya que el problema se puede atacar de una forma más directa y rápida.

A continuación, se presenta la tabla 22 con la cantidad de personas que se encuentran en el grupo establecido por cargo, asociado con su responsabilidad en el desarrollo del proyecto.

Tabla 22 Matriz de responsabilidades

| Cantidad | Cargo | Responsabilidades |
|---|---|---|
| 1 | Jefe de gestión y Aseguramiento | Garantizar que el diseño e implementación del proyecto se lleve a cabo en su totalidad, con el fin de que asegurar la información sobre los equipos gestionados por la empresa |
| 2 | Ingeniero de Aseguramiento | Asegurar que la ejecución del proyecto se realice en su totalidad, validando técnicamente y administrativamente cada una de las actividades a desarrollar |
| 3 | Ingenieros de Calidad | Garantizar mediante las verificaciones sobre las órdenes de trabajo ejecutadas en el área de implantación contengan la configuración del protocolo de seguridad |
| 4 | Líderes de Implantación | Dirigir e informar al grupo de ingenieros de implantación en la configuración del protocolo de seguridad en cada orden de trabajo ejecutada |
| 20 | Ingenieros de Implantación | Realizar la configuración del protocolo de seguridad sobre cada una de las órdenes de trabajo ejecutadas que vengan como altas o modificaciones |

| Cantidad | Cargo | Responsabilidades |
|---|---|---|
| 3 | Coordinadores Soporte Técnico | Coordinar y realizar la correcta verificación en la configuración del protocolo con los ingenieros de soporte que tienen a su cargo |
| 30 | Ingenieros de Soporte Técnico | Realizar la configuración del protocolo de seguridad sobre los servicios que ya tienen configurado movistar MAS. |

## **5.4** GESTIÓN DEL EQUIPO DEL PROYECTO

En la siguiente matriz (ver tabla 23) se relaciona las actividades a realizar con cada uno de los grupos de trabajo establecidos, logrando con esto asegurar que los componentes del alcance este asignado y que ninguna labor quede pendiente por ejecutar.

Tabla 23 Matriz RACI

| Actividad / Recurso | Jefatura | Aseguramiento | Calidad | Líder Implantación | Ingeniero Implantación | Coordinador soporte | Ingeniero de Soporte |
|---|---|---|---|---|---|---|---|
| **Cotización y compra de equipos** | R | A | | | | | |
| **Instalación de equipos** | I | R | | | | | |
| **Configuración sobre órdenes de trabajo** | I | C | | A | R | | |
| **Configuración en canales con movistar MAS ya instalados** | | | C | | | A | R |
| **Verificación sobre órdenes de trabajo** | | A | R | | | | |

# 6 GESTIÓN DE COMUNICACIONES

## 6.1 PLANIFICACIÓN DE LAS COMUNICACIONES

En la tabla 24 se muestra según el interesado que reporte se entrega y la frecuencia con la que se debe hacer.

Tabla 24 Planeación de las comunicaciones

| Interesados | Nombre del documento | Formato del documento | Frecuencia |
|---|---|---|---|
| Gerencia | Reporte de estado | Copia impresa | Primer día del mes |
| Jefe Aseguramiento | Reporte de estado | Copia impresa | Primer día del mes |
| Jefe Calidad | Reporte de ejecución de órdenes de trabajo | E-mail | Primer día del mes |
| Líder Implantación | Reporte de ejecución de órdenes de trabajo | E-mail | Primer día del mes |
| Coordinador Soporte | Reporte de consolidado de servicios con movistar MAS | E-mail | Al inicio del proyecto (solo una vez) |

## 6.2 DISTRIBUCIÓN DE LA INFORMACIÓN

La distribución de la información relevante se pondrá a disposición de los interesados de acuerdo al plan establecido, las cuales se harán llegar en transcurso del ciclo de vida del proyecto. Para que sea de forma eficaz la distribución de información, se dispone de una tabla (ver tabla 25), que de acuerdo a la información que se requiera enviar o solicitar se elija el medio más conveniente para hacerla llegar y así darle tramite mucho más rápido y adecuado.

Tabla 25 Distribución de la información

| Tipo de requerimiento | Copia impresa | Llamada telefónica | Mensaje de voz | Email | Reunión | Sitio Web |
|---|---|---|---|---|---|---|
| Trasmitir un documento de referencia | 1 | 3 | 3 | 3 | 3 | 1 |
| Suministrar registros permanentes | 1 | 3 | 3 | 1 | 3 | 1 |
| Mantener la confidencialidad | 2 | 1 | 2 | 3 | 1 | 3 |
| Transmitir información simple | 3 | 2 | 1 | 1 | 2 | 3 |
| Hacer preguntas informales | 3 | 2 | 1 | 1 | 3 | 3 |
| Hacer preguntas simples | 3 | 3 | 1 | 1 | 3 | 3 |
| Dar instrucciones complejas | 3 | 3 | 3 | 2 | 1 | 2 |
| Dirigir mucha gente | 2 | 3 | 3 | 2 | 3 | 1 |
| Resolver malentendidos | 3 | 1 | 3 | 3 | 2 | 3 |
| Compromiso de evaluación | 3 | 2 | 3 | 3 | 1 | 3 |
| Valor 1 = Excelente. Valor 2 = Adecuado. Valor 3 = Inapropiado | | | | | | |

## 6.3 INFORMES DE RENDIMIENTO

Para tener una clara y ordenada gestión de los informes de rendimiento se pretende realizar una reunión semanal donde se presenten los pormenores y avances que se han conseguido hasta el momento. La socialización es de gran importancia ya que permite realizar de forma personal recomendaciones o ajustes directamente con las áreas y los compromisos que se generan van a quedar más claros y se darán de forma más precisa.

Por otro lado, se generará un informa de cada reunión, el cual deberá ser entregado a los 8 días con el fin de comparar resultados obtenidos con respecto a la semana anterior, donde se incluirá el nombre del proyecto, los integrantes, el cumplimiento del plan

propuesta en la semana y dentro de este, se detallarán los entregables en que área o grupo de trabajo se desarrolló, el ingeniero responsable y por último el alcance que se tiene de dicha actividad. Finalmente, ira firmada por el jefe de gestión y aseguramiento, con lo cual se da por revisado el informe de rendimiento. Ver tabla 26.

Tabla 26 Informe de rendimiento

| INFORME DE RENDIMIENTO SEMANAL | | | |
|---|---|---|---|
| PROYECTO | | | |
| | | | |
| FECHA DE INFORME | | | |
| | | | |
| INTEGRANTES | | | |
| | | | |
| CUMPLIMIENTO DE ACTIVIDADES SEMANALES | | | |
| Entregables | Área que realiza la actividad | Ingeniero Responsable | Avance (%) |
| | | | |

## 6.4 GESTIÓN DE LOS INTERESADOS

En la tabla 27 se presenta a las partes interesadas en el desarrollo del proyecto, de esta manera se tendrá en cuenta a cada una de ellas para lograr estrategias de gestión adecuadas logrando la participación eficaz de cada una de las áreas a lo largo del ciclo de vida del proyecto.

Tabla 27 Gestión de los interesados

| Área interesada | Poder (1-5) | Interés (1-5) | Influencia |
|---|---|---|---|
| Jefatura | 5 | 5 | Garantizar que el diseño e implementación del proyecto se lleve a cabo en su totalidad |
| Aseguramiento | 4 | 5 | Asegurar que la ejecución del proyecto se realice en su totalidad |

| Área interesada | Poder (1-5) | Interés (1-5) | Influencia |
|---|---|---|---|
| Calidad | 3 | 5 | Garantizar mediante las verificaciones sobre las órdenes de trabajo ejecutadas en el área de implantación contengan la configuración del protocolo de seguridad |
| Líderes Implantación | 3 | 4 | Dirigir e informar al grupo de ingenieros de implantación en la configuración del protocolo de seguridad en cada orden de trabajo ejecutada |
| Ingenieros de implantación | 1 | 4 | Realizar la configuración del protocolo de seguridad sobre cada una de las órdenes de trabajo ejecutadas que vengan como altas o modificaciones |
| Coordinadores Soporte | 3 | 5 | Coordinar y realizar la correcta verificación en la configuración del protocolo con los ingenieros de soporte que tienen a su cargo |
| Ingenieros de soporte | 1 | 4 | Realizar la configuración del protocolo de seguridad sobre los servicios que ya tienen configurado movistar MAS. |

# 7 GESTIÓN DE RIESGOS

## 7.1 PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS DEL PROYECTO

El plan de seguimiento y control de riesgos se muestra a continuación (ver ilustración 11) de forma esquemática, lo cual nos permitirá tener mayor seguridad en la ejecución del proyecto en cuanto al cumplimiento de los tiempos establecidos en cada fase del proyecto.

Cabe aclarar que pueden aparecer nuevos riesgos en el desarrollo del proyecto, más sin embargo se les realizará el respectivo seguimiento y análisis que se requiera, para lo cual serán incluidos en esta planificación. También no se descarta que el análisis efectuado para un riesgo en particular se vea alterado a medida que avanza el proyecto.

Ilustración 11 Planificación de la gestión de riesgos


## 7.2 IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

Ya identificados los riesgos se presenta un análisis cualitativo dentro de una matriz de riesgo para que de esta manera nos permita elaborar un plan de contingencia para cada uno de los riesgos asociados respecto a la probabilidad e impacto que presente dentro del proyecto.

Se le realizó una validación de los riesgos asociados al proyecto los cuales se presentan en la tabla 28 basados en la EDT, así de esta forma acércanos lo más posible a cualquier inconveniente que pueda presentarse

Tabla 28 Identificación de riesgos

| N° | Análisis y evaluación del riesgo |
|---|---|
| 1 | Económico |
| 2 | Levantamiento de topología |
| 3 | Diseño de la solución |
| 4 | Recurso humano |
| 5 | Estimación de costos |
| 6 | Tiempo de entrega |
| 7 | Instalación de equipos |
| 8 | Configuración de los equipos |
| 9 | Asignación de los recursos |
| 10 | Asignación de los recursos de red |

Teniendo en cuenta la numeración asignada en la tabla anterior se posiciona en la matriz de riesgos creada con el fin de tener una medida cualitativa del riesgo como se muestra a continuación (ilustración 12).

Ilustración 12 Matriz cualitativa de riesgos

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | Muy probable | | | | | |
| 4 | Probable | | 9,10 | 8 | | |
| 3 | Poco probable | 1 | 2,3,4 | 6 | | |
| 2 | Improbable | | 5 | 7 | | |
| 1 | Remoto | | | | | |
| | | Muy bajo | Bajo | Medio | Alto | Muy alto |
| | | 1 | 2 | 3 | 4 | 5 |

## 7.3 PLANIFICACIÓN DE LA RESPUESTA A LOS RIESGOS

En respuesta al riesgo asociado se generan los siguientes planes a ejecutar con el fin de que estas acciones permitan disminuir en gran parte las amenazas a los objetivos del proyecto. Ver tabla 29.

Tabla 29 Análisis de riesgo

| Riesgo | Plan a ejecutar |
|---|---|
| Monitorización | Se tienen planes de actuación detectivos los cuales se verificarán y revisarán en cada reunión donde se informa el avance del proyecto |
| Investigación | Se tienen planes de actuación preventivos que permitirán el desarrollo del proyecto sin interrupciones:<br>• Control de tiempos entrega mediante revisiones periódicas.<br>• Comunicación constante con cada jefe de área para asegurar el número de equipos configurados y cantidad de ingenieros efectuando las configuraciones |
| Mitigación | Se tienen planes de actuación correctivos que ayudaran a ajustar el proyecto a lo planificado usando otras herramientas que cumplen el mismo objetivo, pero con otro tipo de recursos:<br>• Cambio de equipos.<br>• Actualización de versiones en los routers |

## 7.4 SEGUIMIENTO Y CONTROL DE RIESGOS

Para tener una constante información de los riesgos asociados y que los tratamientos en donde realmente surgen un efecto positivo se tendrá un registro como se muestra en la tabla 30 tipo DOFA (Debilidades, Fortalezas, Amenazas y Oportunidades) que nos permitirá reflexionar no solo lo negativo sino también lo positivo. De esta manera hacer un seguimiento completo a lo largo de todo el proyecto.

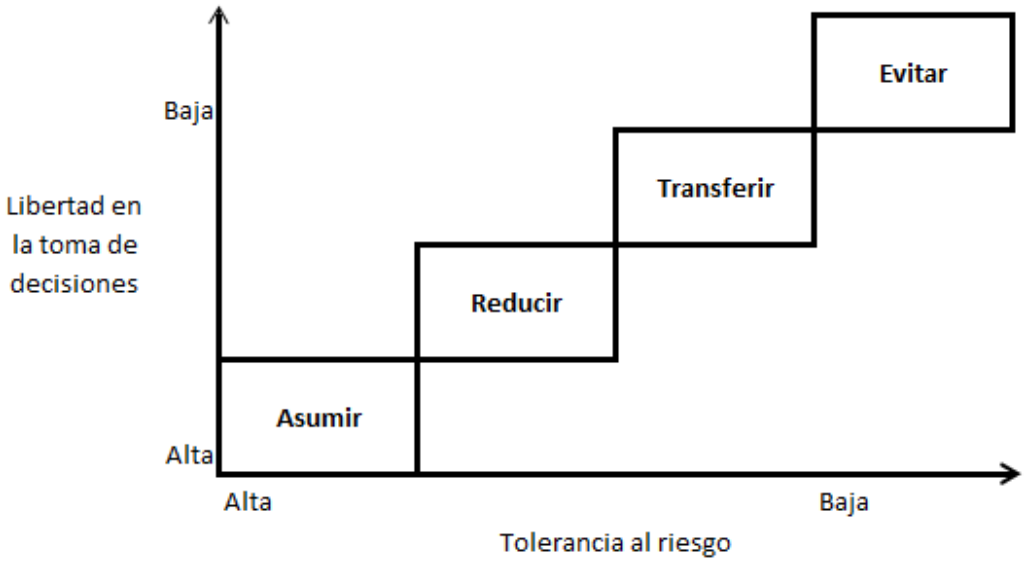
Tabla 30 Seguimiento y control de riesgos

| Identificador de riesgo | Descripción del riesgo | Valor de la probabilidad (A-M-B) | Valor del impacto (A-M-B) | Valor del riesgo | Responsabilidad | Plan y tiempo de respuesta |
|---|---|---|---|---|---|---|
| | | | | | | |

Para el tratamiento de los riesgos asociados al proyecto y de acuerdo al seguimiento realizado, y teniendo en cuenta de que en el transcurso del desarrollo y ejecución pueden surgir otros inconvenientes que no se tuvieron en cuenta, la estrategia a seguir se basará en la libertad para decidir del gerente del proyecto y de la tolerancia al riesgo del proyecto.

De acuerdo a lo anterior la estrategia a seguir según la situación que se presente de muestra en la siguiente ilustración 13.

Ilustración 13 Estrategia para el tratamiento de los riesgos



# 8 GESTIÓN DE ADQUISICIONES

## 8.1 PLANIFICACIÓN DE COMPRAS Y ADQUISICIONES

Como se viene haciendo en la compañía para toda solicitud de equipos, materiales o servicios, de bebe generar una viabilidad para identificar si existen los recursos que se necesitan además de la aprobación del presupuesto para llevar a cabo el proyecto.

### 8.1.1 Solicitud de servicios especiales (arrendamiento de áreas y energía)

Para solicitar un espacio en el nodo donde se va a instalar el servicio se debe diligenciar un formato como muestra la tabla 31 donde se especifica los equipos a instalar, las dimensiones y los datos geográficos de instalación.

Tabla 31 Solicitud de espacios físicos.

| Espacios | | | | | | | | PARA DILIGENCIAR POR VICEPRESIDENCIA INFRAESTRUCTURA | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Dimensiones | | | | SITIO ESPECIFICO | | VIABILIDAD | | |
| QUE EQUIPO | PESO | ALTO | ANCHO | LARGO | RACK | Ciudad | Dirección | UBICACIÓN FISICA PUNTO PARA SUMINISTRO DE ESPACIO | VIABLE (SI / NO) | OBSERVACIONES |
| | | | | | | | | | | |
| | | | | | | | | | | |

Igualmente se debe hacer una solicitud de energía para la conexión de los equipos y energizarlos dentro del nodo donde fue asignado el espacio físico. Se debe llenar un formato similar al que se muestra en la tabla 32.

Tabla 32 Solicitud de energía

| Energía | | | | | | | PARA DILIGENCIAR POR VICEPRESIDENCIA INFRAESTRUCTURA | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | SITIO ESPECIFICO | | VIABILIDAD | | |
| TIPO DE ENERGÍA (AC o DC) | LÍNEA | TIPO DE RESPALDO (Baterias, UPS, etc) | Potencia (A o W) | Voltaje (V) | Ciudad | Dirección | UBICACIÓN FISICA PUNTO PARA SUMINISTRO DE ENERGIA | VIABLE (SI / NO) | OBSERVACIONES |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

### **8.1.2** Solicitud de presupuesto

Para hacer la solicitud de viabilidad de presupuesto se debe diligenciar un formato el cual se puede observar en el anexo 1. En este formato se listan los materiales y equipos necesarios para el desarrollo del proyecto con sus respectivos valores.

## **8.2** PLANIFICACIÓN DE CONTRATOS

De acuerdo a la finalidad del proyecto y a la integración que se requiere con otros equipos y aplicaciones de la empresa se definió que la marca de los equipos debe ser Cisco por lo que no se harán cotizaciones con otros proveedores.
Con la compañía Cisco se hará un contrato para la compra de los equipos y la puesta en marcha de los mismos. Además, se hará un acuerdo para para la compra de las licencias y el soporte anual de los equipos Cisco durante tres años.

## **8.3** SOLICITAR RESPUESTAS A VENDEDORES

Después de hacer la cotización con los proveedores de los equipos Cisco el vendedor debe enviar una respuesta formal en donde especifique que cuenta con los equipos solicitados y con las especificaciones técnicas.

También se debe especificar si cuentan con el servicio de soporte para los equipos y garantía que tienen por instalación y soporte de los equipos.

Junto con los documentos debe venir anexo el formato que se muestra en la tabla 33 donde se escriben los equipos, referencias y su costo.

Tabla 33 Formato de respuesta a vendedores

| | | | | |
|---|---|---|---|---|
| Empresa: | | | | |
| NIT: | | | | |
| | | | | |
| Material | Referencia | Cantidad | Valor unitario | Valor total |
| Equipo 1 | | | | |
| Equipo 2 | | | | |
| Equipo 3 | | | | |
| | | | Total | |

## 8.4 ADMINISTRACIÓN DE CONTRATOS

Los contratos que se establezcan para la adquisición de equipos, licencias y soporte de los mismos estarán bajo la administración del gerente del proyecto y con el apoyo del ingeniero de aseguramiento asignado. Si se requiere algún cambio o ampliación del tiempo del contrato se debe solicitar al gerente del proyecto con los respectivos formatos de viabilidad que se establecieron en el punto 8.1.

Los equipos deberán ser entregados por el proveedor en la bodega de la empresa con el visto bueno del gerente de proyectos quien validará que las referencias solicitadas sean las que se entregan y las licencias estén actualizadas.

Si se llegará a presentar algún retraso en la entrega de los equipos en la fecha estipulada se debe informar la gerente de proyectos y al área de compras.

## **8.5** CIERRE DE CONTRATOS

El contrato con Cisco tiene vigencia de tres años según tiempo en el cual el proveedor cumplirá con los tiempos de garantía de instalación, funcionamiento y soporte de los equipos. Después de terminado el contrato se hace una viabilidad para adquirir nuevas licencias y ampliar a uno o más años el soporte sobre los equipos Cisco.

# ANEXOS

## Anexo 1: Formato para solicitud de presupuesto.

| ESTUDIO DE VIABILIDAD | | |
|---|---|---|
| CLIENTE / RAZON SOCIAL / PROYECTO | | |
| REQUERIMIENTO | | |
| DIRECCION | ¿VISITADO? (si / no) | |
| | Fecha visita | |
| PERSONA DE CONTACTO / CARGO | ESTADO PREDIO | |
| | Fecha Terminacion | |

**PRESUPUESTO - DETALLE DE OBRA CIVIL**

| No. | Item | Descripcion | Unidad | Cantidad | Valor Unitario | Valor Total |
|---|---|---|---|---|---|---|
| 1 | | | | | | $ |
| 2 | | | | | | $ |
| 3 | | | | | | $ |
| 4 | | | | | | $ |
| | | | | | Subtotal | $ |
| | | | | | Reajuste 10% | $ |
| | | | | | TOTAL | $ |

| CRONOGRAMA DE ACTIVIDADES | | |
|---|---|---|
| Item | Descripcion | Dias Hab |
| 1 | Replanteo | |
| 2 (Actividades en paralelo) | Permiso IDU o equivalente | |
| | Permiso Secretaria de Transito o equivalente | |
| | Licencia especial | |
| 3 | Ejecucion | |
| 4 | Protocolo de puebas | |
| 5 | Actualizacion SAT - Smas de Información | |
| | TOTAL | |

| PLANTA INTERNA | |
|---|---|
| CENTRAL | |
| DISTRITO / DISTRIBUIDOR | |
| LENS DISPONIBLES | |
| **RED SECUNDARIA** | |
| ARMARIO | |
| CAJA(S) | |
| TIPO CAJA | |
| HABILITAR / REUBICAR | |

| DESCRIPCION DE ACTIVIDADES |
|---|
| |
| **OBSERVACIONES ADICIONALES** |
| |

| Elaborado por | | Fecha elaboración | |
|---|---|---|---|

# GLOSARIO DE TERMINOS

AAA: Authentication, Authorization y Accounting (Autenticación, Autorización y Contabilización)

RADIUS: Remote Authentication Dial-In User Server

NAS: Network Access Server

CPE: Enrutadores de proveedor en el cliente

Movistar MAS: Herramienta de monitoreo usada en Telefónica

VPRN: Virtual private routing network

BGP: Border Gateway Protocol

FailOver: Tolerancia a fallas o conmutación por error

SSH: Secure SHell

P.E: Enrutadores de proeveedor

AC: Costo Actual

PV: Valor Planificado.

EV: Valor Ganado.

EDT: Esquema de desglose de trabajo

MPLS: Multi Protocol Label Switching

LOOPBACK: Interfaz de red virtual