DISEÑO DE UNA SOLUCION DE CONTROL DE ACCESO IP A NIVEL NACIONAL PARA LA EMPRESA ABC

JOSE ALEJANDRO LACERA PABON

LEONARDO PAUL AMAYA MENDOZA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

ESPECIALIZACIÓN EN TELECOMUNICACIONES

CARTAGENA DE INDIAS D.T. y C.

2012

DISEÑO DE UNA SOLUCION DE CONTROL DE ACCESO IP A NIVEL NACIONAL PARA LA EMPRESA ABC

JOSE ALEJANDRO LACERA PABON

LEONARDO PAUL AMAYA MENDOZA

Trabajo Integrador presentado como registro de aprobación para la Especialización En Telecomunicaciones

Director

Gonzalo López Vergara

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

ESPECIALIZACIÓN EN TELECOMUNICACIONES

CARTAGENA DE INDIAS D.T. y C.

2012

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena De Indias 15 de Abril, 2012

A Dios, a nuestros familiares y amigos que nos apoyaron durante todo este proyecto.

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

Dios, por ser nuestra guía en todo momento

A nuestros padres por su incondicional apoyo.

Al Ingeniero Gonzalo López Vergara, por liderar nuestro proceso de aprendizaje tanto en lo académico como en lo humano.

Y a la prestigiosa institución Educativa Universidad Tecnología de Bolívar que nos acogió e instruyo tanto en lo humano como lo académico.

TABLA DE CONTENIDO

Pag.

TABLA DE FIGURAS

Pag.

TABLAS

Pag.

RESUMEN

En la actualidad las empresas tienen la necesidad de controlar el acceso a personas ajenas a la organización o dentro de estas controlar el acceso a ciertas áreas como medida para minimizar el riesgo de hurtos, sabotajes o ataques a la infraestructura, las personas o su operación, dentro de los sitios mas comunes y dependiendo del modelo del negocio tenemos oficinas específicas, centrales de seguridad, centros de cómputo, oficina de archivos confidenciales, bodegas, etc.

El medio de identificación de las personas puede ser mediante el uso de tarjetas de proximidad, biometría, teclados alfanuméricos o combinación de estas.

Es necesario realizar un análisis costo beneficio de los diferentes medios de identificación, para escoger cual de estos medios puede proveer un buen nivel de seguridad a un costo razonable.

Teniendo en cuenta la tendencia tecnológica, se ha decidido que el sistema sea basado en IP (Internet Protocol), lenguaje universal y protocolo abierto de comunicaciones, de tal manera que sea escalable permitiendo la integración de diferentes sistemas tanto de seguridad electrónica como convencionales: Control de Acceso, CCTV (Video IP), monitoreo de alarmas y voz sobre IP (VoIP).

Como aspectos claves para la definición y alcance del sistema se deben tener en cuenta la cantidad de usuarios, el flujo de la población, población flotante, distribución geográfica, entre otros, los cuales definirán el éxito en cuanto a la administración de la seguridad en las instalaciones.

INTRODUCCIÓN

La Empresa ABC cuenta con varias sedes distribuidas en el territorio nacional y para su operación debe disponer de un sistema administrable, robusto y escalable con el fin de garantizar la seguridad del personal y la infraestructura misma; para mitigar los riesgos debe disponer de herramientas como sistemas de control de accesos que cumpla con una serie de interrelaciones con otros sistemas y disciplinas y objetivos específicos de la empresa.

El presente documento describe la arquitectura del Sistema de Control de Acceso su estructura y funciones de sus componentes, sus relaciones, principios y guías que rigen su diseño y evolución en el tiempo.

En el marco de crecimiento de La Empresa ABC se requiere afrontar con decisión y agilidad los procesos necesarios de integración empresarial y operativa en los diferentes escenarios de la empresa.

Por este motivo se requiere estructurar la guía para consolidar un sistema de seguridad robusto, eficaz y eficiente con el cual poder ofrecer la capacidad de crecimiento y rentabilidad sostenible que demanda la compañía en su estrategia de superar la evolución del mercado y ser una compañía de elevado atractivo dentro del sector en que se desempeña.

1. EL PROBLEMA DE LA INVESTIGACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

En particular el Sistema de Control de Acceso de la Empresa ABC, requiere de una inversión que permita alinearlo con la política de crecimiento de la compañía. El objetivo principal es que los funcionarios mediante una sola tarjeta puedan acceder, si dispone de los permisos necesarios, a cualquier edificio u oficina de la compañía ubicada en cualquier parte del territorio nacional, para desempeñar sus funciones, manteniendo una cultura de bienvenida y cordialidad, sin desatender la seguridad. Resultaría irónico que una compañía que precisa avanzar más rápidamente, donde la agilidad es un elemento clave para un negocio basado en el avance tecnológico, tenga funcionarios que no puedan avanzar por la puerta cuando se desplazan de una instalación de trabajo a otra dentro de la misma ciudad o país. Para un funcionario que se desplaza entre varios centros, en caso de no realizar dicha inversión, sería necesario dotarle de al menos seis tarjetas de control de accesos de cada instalación o en su defecto realizar duplicidad de la información en cada base de datos de cada instalación.

Debido a lo anterior se requiere disponer de un Sistema de Control de Acceso lo suficientemente versátil de forma que entre otras, desde una única instalación sea posible asignar los permisos de acceso para diferentes funcionarios de cualquier de las instalaciones, en función de las autorizaciones de sus responsables para acceder a un área de trabajo de un edificio. En la actualidad la ejecución de proyectos requiere gestionar los accesos en fin de semana, festivos, proyectos especiales, grupos especiales, permitir el acceso a determinadas áreas por un tiempo limitado o extendido etc. Este tipo de gestión precisa un sistema de gestión sistematizada y centralizada, con una única base de datos de personal y no

diferentes bases de datos por instalaciones, para gestionar el ingreso y salida de personal de forma centralizada e instantánea, que permita validar en campo la foto del empleado almacenado en la base de datos y la persona portadora de la tarjeta, una única tarjeta con un formato corporativo para todas las instalaciones, etc.

En este sentido un Control de Acceso Corporativo centralizado para todas las instalaciones permitirá que los empleados, las instalaciones y los bienes de la compañía sean más seguros y gestionados de forma más eficiente. La eficiencia del Control de Acceso ayuda a la productividad, lo cual es vital para cualquier negocio pero especialmente para una compañía como la Empresa ABC, donde la rapidez en llevar avances tecnológicos al mercado tiene una importancia estratégica.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

- Diseñar una solución de Sistema de Control de Acceso empresarial centralizado para las sedes de la empresa ABC a nivel nacional.

1.2.2 OBJETIVOS ESPECÍFICOS

- Establecer los requisitos funcionales y operativos del Sistema de Control de Acceso.
- Establecer el tipo de tecnología para la identificación del personal.
- Diseñar el sistema de control de acceso en cada sede.

- Diseñar el modelo de interconexión de las 6 sedes en el país, bajo una gestión administrada de forma centralizada.

1.3 JUSTIFICACIÓN

El sistema de control de acceso se diseña para operar en las diferentes instalaciones y topologías de la Empresa ABC, siendo su principal función el aseguramiento y protección de las instalaciones involucradas, así como la vigilancia de las mismas ante diversos tipos de eventos (Atentados terroristas, Hurtos, Sabotajes e Intrusión o eventos fuera de lo normal). Estos eventos deben ser gestionados en tiempo real así como registrados y almacenados para su posterior análisis y seguimiento.

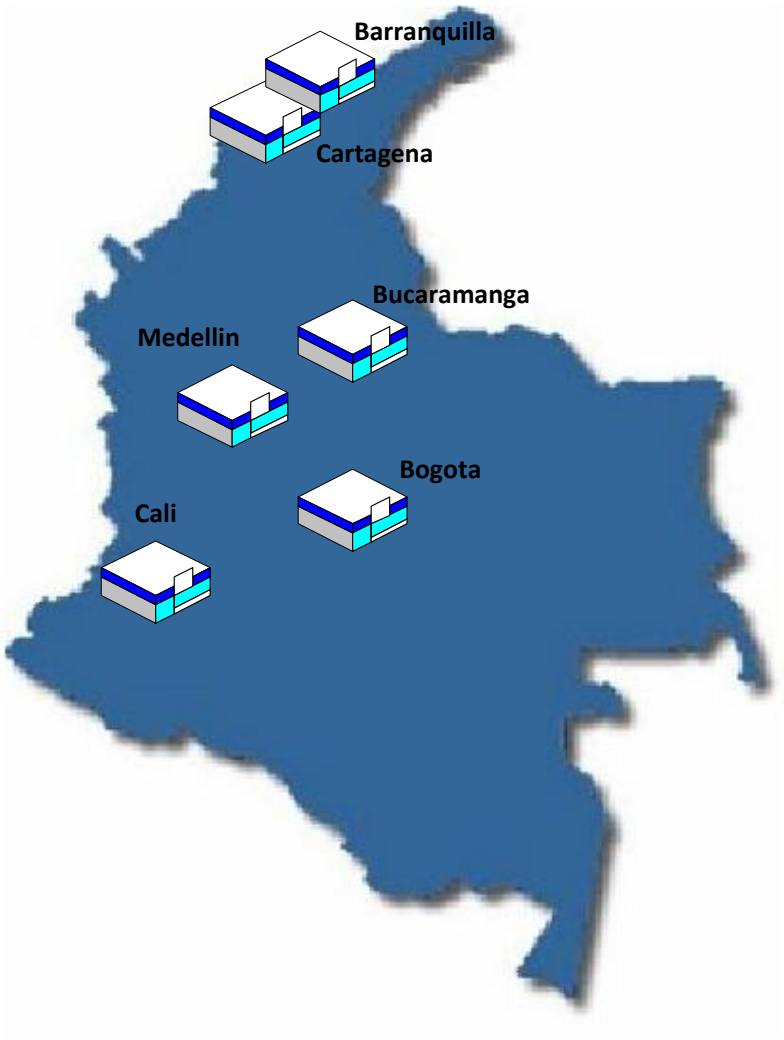
Siendo conscientes del gran impacto social que este sistema causa dentro de la compañía a nivel nacional, debido a la cantidad de usuarios y el tipo y tamaño de cada instalación se decidió instalar una plataforma centralizada con la posibilidad de tener clientes WEB en cada sitio para la administración local y que con un solo sistema de identificación cada usuario pueda desplazarse e ingresar a sus áreas de trabajo sin mayores complicaciones, por lo que se considera altamente favorable al permitir un muy buen nivel de seguridad ofreciendo un sistema amigable para los usuarios finales permitiendo mayor agilidad en los funcionarios lo que finalmente se verá reflejado en agilidad en los procesos.

2. DESCRIPCIÓN DEL PROYECTO

De acuerdo al perfil de la empresa ABC, las seis sedes ubicadas en el territorio nacional están en las siguientes ciudades

- Bogotá
- Medellín
- Cali
- Barranquilla
- Cartagena
- Bucaramanga

Figura 1. Ubicación sedes empresa ABC



De acuerdo a la distribución de la geografía nacional, el tamaño de las instalaciones y la cantidad de personal en cada una, se tienen como sedes principales Bogotá para la zona centro y sur de Colombia y Cartagena para la zona norte.

El Sistema de Control de Acceso contará con dos servidores uno en cada sede principal con sincronización por lo que en caso de salir uno de línea el otro soportará toda la operación a nivel nacional.

En cada una de las sedes se instalará Microcontroladores de acuerdo el número de puertas o accesos a controlar, los cuales controlaran el sistema en sitio; estos estarán conectados a los servidores a través de la red corporativa y con el fin minimizar el riesgo de cortes en el servicio estos Microcontroladores tendrán la capacidad de trabajar en modo Stand Alone por lo que en caso de corte estos serán capaz dar continuidad al servicio y una vez se restablezca la comunicación descargar las transacciones al servidor y realizar las actualizaciones necesarias.

2.1 DESCRIPCION TECNICA Y FUNCIONAL DEL SISTEMA DE CONTROL DE ACCESO

Habiendo realizado el análisis tanto técnico como funcional de diversos Sistemas de Control de Acceso existentes en el mercado, a continuación se describen las características que cumple el sistema escogido:

Debido a que la empresa ABC se encuentra en permanente crecimiento, el sistema debe ser escalable, modular y flexible con el fin de permitir su crecimiento a nuevas instalaciones del territorio nacional.

Para mantener las puertas aseguradas se usaran electroimanes y su apertura será mediante el sistema o desde cliente WEB del sistema y para los casos de emergencia desde pulsador de emergencia en sitio.

Se instalará un contacto magnético en cada puerta y se realizara la programación para informar a la controladora del sistema de control de acceso el estado en que se encuentran las puertas de entrada y salida controladas (Abierta, cerrada, Forzada, etc.).

Este sistema recolectara y direccionará la información a través de las controladoras hacia el servidor del Sistema de Control de Acceso y estos incluyen la interfaz necesaria para la comunicación con el servidor.

Mediante cualquier cliente web desde la red corporativa y con los permisos adecuados es posible asignar los permisos de acceso para diferentes usuarios de varios centros en función de las autorizaciones de sus responsables para acceder a un área de trabajo de una instalación o para diferentes áreas de las diferentes instalaciones controladas con el sistema.

Las características funcionales del software de Control de Acceso que debe cumplir son:

- ✓ Mantener comunicación continua y en tiempo real con la red de equipos en campo del Sistema de Control de Acceso tales como controladoras, lectoras, electroimanes, contactos, etc.
- ✓ Configurar, supervisar y registrar el comportamiento de la red de elementos físicos desde cualquier estación de trabajo:
  - Horarios y perfiles de acceso.
  - Alarmas: cualquier intento de acceso invalido o no autorizado debe disparar una alarma.
  - Transacciones.
- ✓ Interactuar con la red de elementos físicos (equipos en campo) de manera que se puedan controlar remotamente las puertas controladas (bloqueos o aperturas).
- ✓ Visualizar eventos a medida que se producen.

- ✓ Almacenar de forma estructurada y accesible informes de accesos, alarmas y demás información generada por el sistema.
- ✓ Escalabilidad: capacidad de crecimiento bajo la misma plataforma.
- ✓ Segmentación: cada estación de trabajo o servidor regional solo puede acceder a la información de su instalación o región respectivamente o a las zonas que se programen.
- ✓ Posibilidad de que la información almacenada en los servidores regionales se sincronice y almacene posteriormente en un servidor global.
- ✓ Posibilidad de operación autónoma e independiente de los servidores regionales.
- ✓ Funcionamiento autónomo de los controladores, en caso de fallo en las comunicaciones.
- ✓ Generación de reportes a partir de históricos almacenados en la base de datos destinada para ello.
- ✓ La disponibilidad de información deberá contener todas las transacciones realizadas mínimos los últimos 360 días.

Las características técnicas que la aplicación de control de acceso debe incluir, sin limitarse a ello:

- ✓ Arquitectura distribuida multiservidor con sincronización de bases de datos.
- ✓ Arquitectura cliente/servidor

- ✓ Soporte de múltiples tecnologías de identificación de personas.
- ✓ Multiusuario, con comunicaciones en tiempo real.
- ✓ Posibilidad de número de tarjeta: ilimitados
- ✓ Posibilidad de número máximo de lectores: ilimitados
- ✓ Posibilidad de número de entradas supervisadas: ilimitadas
- ✓ Posibilidad de número de salidas: ilimitadas
- ✓ Posibilidad de estaciones de trabajo (clientes) : ilimitados
- ✓ Comunicación TCP/IP
- ✓ Control de eventos
- ✓ Activación/desactivación/habilitación/deshabilitación remota de puertas controladas y/o en base a horarios.
- ✓ Transmisión automática de derechos de acceso a los controladores
- ✓ Definición de horarios de actividad e inactividad de puertas
- ✓ Perfiles de tarjeta-habientes, con horarios y derechos de acceso.
- ✓ Visualización en tiempo real de accesos válidos o no autorizados y alarmas correspondientes.
- ✓ Arquitectura abierta.
- ✓ Registro de fotografías de personal y visitas.
- ✓ Perfiles de operadores.

- ✓ Encriptación de la información proveniente de los controladores.
- ✓ Interfaz gráfica amigable al operador.
- ✓ Posibilidad de llamar automáticamente a la pantalla el video en vivo desde una cámara del sistema de CCTV para visualizar el área bajo alarma.
- ✓ Posibilidad de integración en caso de requerirse con sistemas del negocio existentes:
    - SNMP
    - LDAP
- ✓ La visualización, administración y monitoreo puede realizarse desde cualquier estación dentro de la red de datos corporativa, teniendo en cuenta la segmentación realizada y perfiles de usuario.
- ✓ Ofrecer funcionalidades de rastreo, auditoría y reportes.
- ✓ Posibilidad de sincronización de los servidores regionales con el servidor global en caso de requerirse.
- ✓ Reportes de estado del Hardware y de las comunicaciones.
- ✓ Procesos de backup y restauración de datos.
- ✓ Un histórico de eventos con capacidad mínima de 2.000.000 de eventos.
- ✓ Capacidad ilimitada para definir múltiples periodos de tiempo indicando franjas horarias, días de la semana y calendarios.
- ✓ Capacidad ilimitada para definir múltiples perfiles de acceso, de manera

que cada usuario puede tener asignados diferentes perfiles de acceso en función del lector y la franja horaria correspondiente.

- ✓ Capacidad ilimitada para realizar grupos de usuarios de tarjeta.
- ✓ Capacidad ilimitada para realizar grupos de lectores de Control de Accesos.
- ✓ El sistema permitirá asegurar/desasegurar las zonas con control de acceso, automáticamente o por horarios y remotamente.
- ✓ Dispondrá de un módulo opcional para control y gestión de dispositivos de generación de acreditaciones o categorías de control de accesos (manejo de imágenes, capturadora, impresora de carnets).
- ✓ El sistema permitirá realizar un informe de presentes en las instalaciones para coordinar labores de evacuación en caso de emergencia y otros.
- ✓ El sistema permitirá activar de forma automática la apertura de los accesos de las instalaciones o cualquier otro evento automático que se programe.
- ✓ El sistema permitirá, de forma integrada en la aplicación, la realización de backup de seguridad de los archivos de configuración así como de las bases de datos e histórico de eventos.
- ✓ El sistema registrará de forma completa todos los eventos (alarmas, accesos, denegación de acceso y causa, actuaciones de los operadores, log-on y log-off, modificaciones de la configuración, todos los fallos de comunicación con dispositivos etc.) con indicación de fecha, hora, minutos y segundos. Cada evento se registrará con la fecha

y hora en la que se produce así como con la fecha y hora en la que llega a la central de seguridad, de forma que disponga de información precisa de los eventos almacenados en los controladores durante los periodos de pérdida de comunicaciones con el servidor. El periodo máximo de almacenamiento de eventos será configurable por el Administrador del Sistema. La generación de informes será un proceso que no interrumpirá la atención de alarmas por parte del operador.

- ✓ El sistema permitirá introducir fecha de expiración de tarjeta así como la fecha de activación de la misma.
- ✓ El sistema permitirá parametrizar un lector o conjunto de lectores sin afectar al funcionamiento del resto de lectores del sistema.
- ✓ El sistema permitirá monitorear y registrar los accesos autorizados con indicación de la activación de apertura de puerta y también con indicación de apertura de la misma detectada por el sensor de puerta.
- ✓ Los sensores en estado de alarma se visualizarán en dicho estado hasta que el sensor vuelva al estado de reposo, independientemente de que un operador haya validado la alarma.
- ✓ El sistema debe contar con la opción antipassback.

El sistema de control de acceso definido fue **ONGUARD ACCESS** de la empresa **LENEL** con controladoras inteligentes LNL-2200, módulos de interfaz de lectora LNL-1320 o LNL-1300, módulo de control de entradas LNL-1100, módulo de control de salidas LNL-1200 entre otros.

Figura 2. Controladora LNL-2200

Dentro de las características del software están:

Diseño de Arquitectura Abierta. El diseño de arquitectura abierta del "OnGuard" asegura un soporte universal y enorme flexibilidad para el usuario. Soporta bases de datos estándares de la industria, cámaras y video grabadoras, redes e impresoras de tarjetas compatibles con Microsoft Windows 2000/XP. También soporta los protocolos y topologías estándares de redes, incluyendo al Microsoft TCP/IP.

Capacidad de Manejo Ilimitada. El "OnGuard" ofrece un ilimitado crecimiento dentro de una simple, y sin remiendos, solución integrada de software. Ha sido diseñado para cubrir las necesidades de cualquier tamaño de organización, desde la que requiere un nivel de entrada de dos lectoras, hasta una gran corporación con numerosas sucursales y miles de lectoras localizadas alrededor del mundo. El

"OnGuard" soporta un número ilimitado de lectoras, puntos de alarmas y tarjeta habientes.

Avanzada Segmentación de Base de Datos. El "OnGuard" les permite a los administradores de sistemas particionar la base de datos en múltiples segmentos, para limitar la vista y manipulación de la data. La base de datos puede ser segmentada para permitir a los operadores individuales de sistema de ver y administrar solo aquellas tarjetas habientes, formatos de tarjetas e interfaces de hardware que están dentro de su dominio autorizado. Esta capacidad es ideal para usarla en grandes corporaciones o universidades donde las funciones de algunos departamentos o áreas funcionales desean tener una autonomía y control independiente.

Integración Biometría/Smart Card. El "OnGuard" provee un soporte avanzado de la biometría, incluyendo lectores de huellas dactilares o patrón de mano. Todos los patrones biométricos del tarjeta habiente son almacenadas en la base de datos "OnGuard". Luego los patrones son descargados a los Controladores Inteligentes del Sistema Lenel, o codificados en las tarjetas Smart Cards (por contacto o sin contacto), eliminando de esta forma la necesidad de tener una red y un sistema administrador de patrones separado.

Integración Multimedia. La funcionalidad Multimedia esta extensivamente integrada dentro y utilizada por el "OnGuard". Con gráficos de mapas dinámicos, y a tiempo real, la ventana que muestra los eventos de alarma no tiene la necesidad de refrescarse cuando un nuevo evento de alarma ocurre. Soporta anuncios verbales programables e iconos titilantes de colores para cada alarma que suceda. Instrucciones verbales también están soportadas, así cada alarma o evento tienen un conjunto de instrucciones en texto y voz pre-grabados. También integra la verificación de video al momento de la alarma, permitiéndole al oficial de guardia verificar en vivo la actividad del tarjetahabiente en áreas remotas de seguridad.

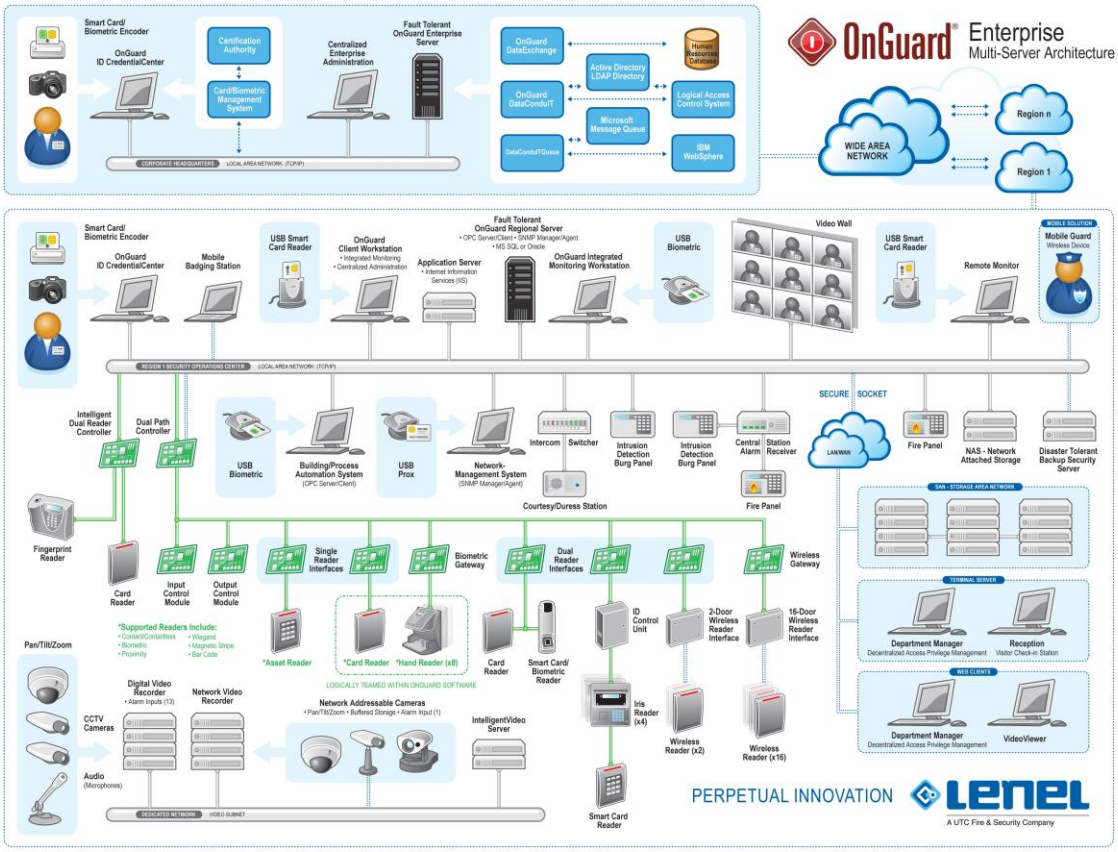
Interfase a Estaciones Centrales de Monitoreo. El "OnGuard" ofrece la integración con estaciones de alarma centralizados de terceros, incluyendo el Radionics 6500/6600, Osbourne-Hoffman OH-2000, AES Intellinet (Radionics 6500 modo de salida), y receptoras Digitize 3500. Todas las alarmas y los eventos que son generadas por un equipo del tipo downstream y se comunica a las receptoras también son reportadas a las estaciones de Monitoreo de alarma del "OnGuard" para ser procesadas. Los eventos recibidos pueden ser configurados para activar procesos de grabación de video del CCTV. También pueden ser almacenados en la cola de auditoria del "OnGuard", y encadenado a otros dispositivos de salida tales como sirenas o luces estroboscópicas.

E-mail y Buscapersonas automatizados. El "OnGuard" se integra con los sistemas de correos electrónicos y buscapersonas (pager) lo que permite que sean enviados textos y mensajes automáticamente cuando ocurre una alarma. Por ejemplo, cuando una puerta se abre forzadamente, una notificación de alarma puede ser enviada al buscapersonas al oficial de seguridad que efectúa la ronda, y un e-mail puede ser enviado al administrador en otro sitio de la ciudad, a tiempo real y sin la intervención del operador.

Recursos de Respaldo, Servidor Tolerante a Fallas. El "OnGuard" soporta a servidores tolerantes a fallas y bases de datos de arquitectura redundante, así permite que el sistema continúe funcionando si la base de datos primaria falla. En el evento de una falla del servidor, el "OnGuard" automáticamente se cambiara al servidor de respaldo. No necesita la intervención de ningún operador.

Listado de Emergencia. El "OnGuard" provee un soporte avanzado del listado de personas. En una situación de emergencia, el "OnGuard" generará un listado de todas las personas que estén en las áreas de peligro, como también de aquellos individuos que están en las áreas seguras. El "OnGuard" continuamente mantiene el listado actualizado a tiempo real.

Figura 3. Esquema Arquitectura empresarial Multiservidor



2.2 DEFINICION DEL SISTEMA DE IDENTIFICACION A UTILIZAR

En la actualidad existen diversos tipos de identificación el cual debe ser definido de acuerdo a los requerimientos del negocio y a las condiciones de su uso, este debe ser automático, de tal forma que no requiera la intervención humana para la validación y que el sistema realice la verificación mediante la comprobación de la información leída por el dispositivo de captura y la información almacenada en el sistema.

Dentro de los sistemas de identificación planteados se evaluaron:

- **Sistemas biométricos**:

  - Dentro de las técnicas biométricas actuales se evaluaron rostro, termografía facial, huella dactilar, geometría de la mano, patrón vascular de la mano, iris o patrones de la retina, voz y firma. A continuación se realiza una breve descripción de cada uno:

    - **Huella dactilar:** La identificación por medio de las huellas digitales constituye una de las formas más representativa de la utilización de la biometría. Una huella digital está formada por una serie de surcos. Las terminaciones o bifurcaciones de los mismos son llamados 'puntos de minucia'. Cada uno de estos puntos tiene una característica y una posición única, que puede ser medida. Comparando esta distribución es posible obtener la identidad de una persona que intenta acceder a un sistema en general, esta tecnología es conocida como AFIS.

Figura 4. Lectora de huella dactilar

http://www.sistautom.com.mx/principal/prod_serv/productos/lectoras/huella.htm

- **Reconocimiento facial:** El reconocimiento facial es la forma como la gente se reconoce entre sí desde hace miles de años. Ahora las computadoras también tienen la habilidad de reconocer rostros. La tecnología de reconocimiento facial, está entre las más recientes tecnologías del ámbito de la biometría. A través de un software un computador conectado a una cámara de video es capaz de capturar la imagen de rostros humanos, y extraer puntos que permiten comparar con un conjunto de imágenes de acuerdo a los patrones faciales almacenados en una base de datos. Esta tecnología se ha popularizado recientemente por la gran cantidad de aplicaciones prácticas que ofrece, sin embargo se considera que existen distintos aspectos de la misma que deben madurar un poco más.

Figura 5. Lectora de reconocimiento facial

http://www.by.com.es/es/reconocimiento-facial.html

- **Geometría de la mano:** Se trata de la medición de las características físicas de manos y dedos desde una perspectiva tridimensional. Estos sistemas son adecuados a bases de muchos usuarios con acceso infrecuente y pueden estar menos predispuestos y disciplinados a ser detectados. La precisión puede ajustarse hasta ser elevada y son técnicas muy flexibles a los escenarios.

Figura 6. Lectora por geometría de mano

http://www.solucionesbiometricas.com/pg_recognition.htm

- **Verificación por Voz:** Potencialmente muy atractivo para las actividades de negocios, pero al momento son muy sensibles a las condiciones de aproximación y externas, por ejemplo la acústica del recinto. Por otra parte la colección de los registros puede ser conflictiva y compleja.

- **Iris o barrido de la Retina:** Una tecnología muy conocida y precisa en la que la delicada retina es barrida por una luz de baja intensidad vía un acoplador óptico, pero requiere que la persona mire dentro de un receptáculo y enfoque su mirada hacia un punto. Esto es un inconveniente si la persona usa anteojos o tiene escrúpulos en contactar el receptáculo.

Figura 7. Lectora por barrido de retina

http://www.tecnocosas.es/lector-de-reconocimiento-de-iris-de-panasonic/

- **Verificación de firma:** La verificación de firma goza de una aceptación que las otras técnicas no tienen. Es suficientemente precisa y su uso es especialmente adecuado a aplicaciones en las que la firma es un identificador aceptado. Curiosamente no se ha desarrollado lo que debiera.

Figura 8. Lectora por verificación de firma

http://es.123rf.com/photo_6541694_su-marca-aqu--deslizar-una-tarjeta-de-recompensas-de-cr-dito-d-bito-a-trav-s-de-un-comerciante-de-te.html

- **Tecnologías sin contacto**
    - **Lectoras de proximidad**: La lectora tiene una antena que continuamente emite un campo electromagnético de frecuencia baja RF. Cuando la tarjeta se acerca al campo, una antena dentro de la tarjeta recoge energía del campo. Esta energía es aprovechada por la tarjeta para alimentar sus circuitos internos y así transmitir su código único a la lectora. Esta verifica la validez de la señal y la manda al controlador para que se tome la acción correspondiente.

Figura 9. Lectora de proximidad

http://www.hidglobal.com/prod_detail.php?prod_id=77

- **Banda magnética**: La información es magnéticamente codificada en la banda. Posteriormente, un lector de banda magnética puede ser usado para leer esta información. Usando la tecnología de máquinas lectoras, la posibilidad de errores humanos se reduce y la velocidad de transacciones de la información es mucho más rápida.

Figura 10. Lectora de banda magnética

http://www.solostocks.com/venta-productos/electronica/general/integrados/lector-grabador-de-tarjetas-de-banda-magnetica-idata-3759437

- **Lectora de código de barra**: El código de barras consiste en una serie de barras negras y espacios en blanco de diferentes anchos que permiten la captura automática de información.

Una vez realizado el análisis costo beneficio de acuerdo a las condiciones de uso, necesidades de la operación, costos de adquisición e implementación, se decidió hacer uso de lectoras y tarjetas de proximidad para controlar el acceso a las instalaciones, con lo que además el personal de seguridad física puede realizar la identificación visual del tarjetahabiente y cotejar en caso de requerirse.

2.3 DISEÑO DEL SISTEMA

Una vez realizado el análisis de población, instalaciones, cantidad de lectoras, puntos a controlar y teniendo en cuenta la red de datos existente se estableció que cada sistema estará conformado de la siguiente forma:

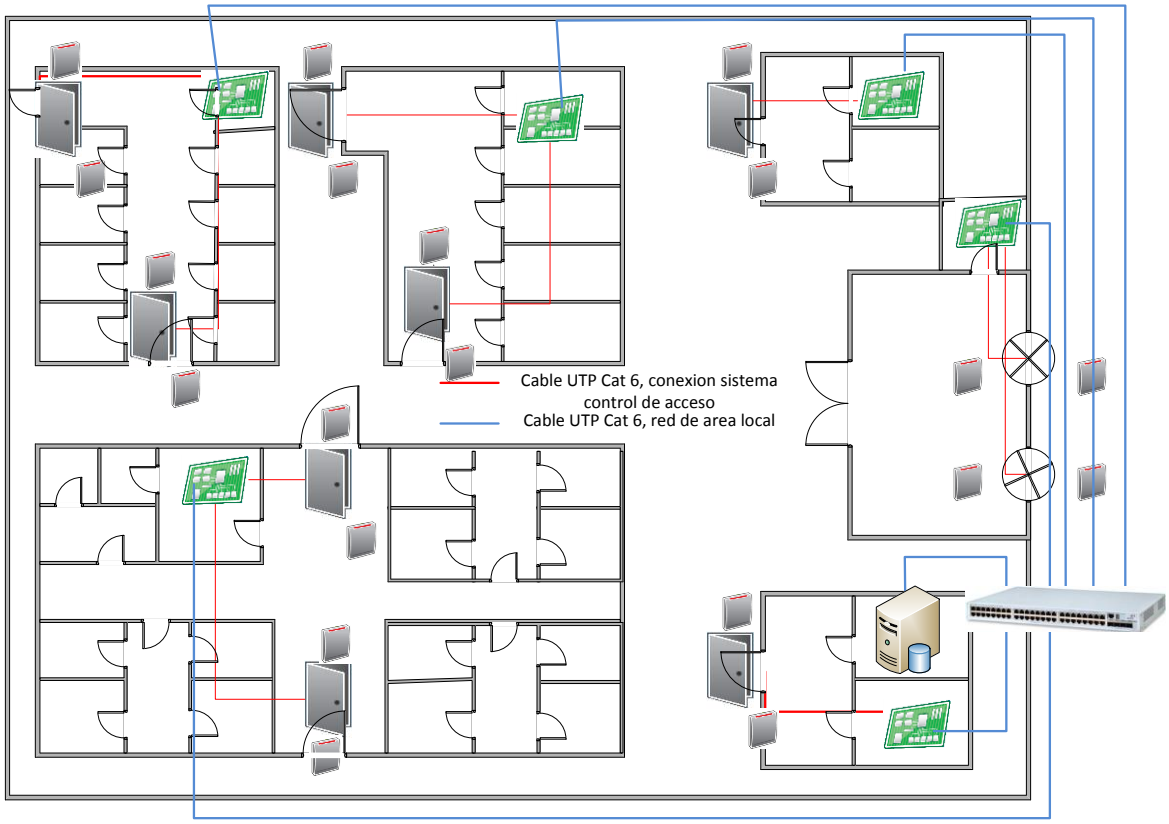
Tabla 1. Resumen equipos SCA con dirección IP

CIUDAD	SERVIDOR	MICROCONTROLADOR
Cartagena	1	11
Bogotá	1	9
Medellín		9
Cali		9
Bucaramanga		9
Barranquilla		9

2.3.1 Diseño Cartagena. Para la sede de Cartagena de acuerdo al análisis realizado se estableció que se requieren 11 controladoras. La ubicación de cada equipo será en los cuartos de equipos o en su defecto donde se encuentran los equipos activos de la red de datos.

Adicionalmente en esta sede está ubicado uno de los dos servidores del sistema de control de acceso.

Figura 11. Área operativa Cartagena



En el edificio administrativo

Figura 12. Área administrativa 5 pisos Cartagena

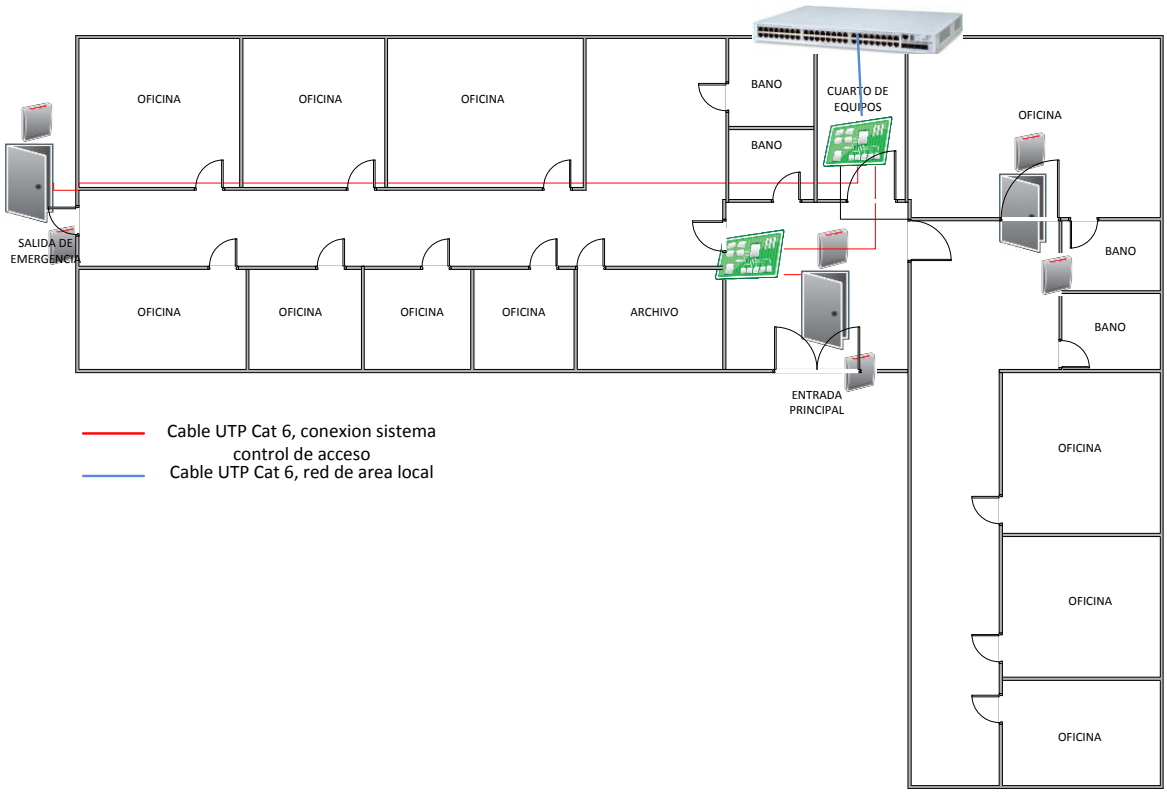


Tabla 2. Diseño sistema control de acceso Cartagena

CARTAGENA												
EQUIPO/UBICACION	Área Operativa						Área administrativa					
	Entrada principal	Oficina 1	Oficina 2	Oficina 3	Oficina 4	Oficina 5	Piso 1	Piso 2	Piso 3	Piso 4	Piso 5	TOTAL
Servidor	0	1	0	0	0	0	0	0	0	0	0	**1**
Controladora LNL 2200	1	1	1	1	1	1	1	1	1	1	1	**11**
Módulo crecimiento LNL 1320	0	0	0	0	0	0	1	1	1	1	1	**5**
Molinete	2	0	0	0	0	0	0	0	0	0	0	**2**
Electroimán	0	1	2	2	2	1	3	3	3	3	3	**23**
Lectora de proximidad	4	2	4	4	4	2	6	6	6	6	6	**50**
Contacto magnético	0	1	2	2	2	1	3	3	3	3	3	**23**
Módulo de entradas	1	1	1	1	1	1	1	1	1	1	1	**11**
Módulo de salidas	1	1	1	1	1	1	1	1	1	1	1	**11**

Tabla 3. Resumen equipos sistema control de acceso Cartagena

	CANTIDAD	ÍTEM	REFERENCIA	MARCA
1	1	Servidor	Dell	Dell
2	11	Controladoras	LNL-2200	Lenel
3	5	Modulo interface crecimiento	LNL 1320	Lenel
4	2	molinetes	Boonedam	Boonedam
5	23	Electroimanes	Zebra	Zebra
6	50	Lectoras de proximidad	RP40	HID
7	23	Contacto magnético	Zebra	Zebra
8	11	Módulo de entradas	LNL-1100	Lenel
9	11	Módulo de salidas	LNL-1200	Lenel

2.3.2 Diseño Bogotá. Para la sede de Bogotá de acuerdo al análisis realizado se estableció que se requieren 9 controladoras. La ubicación de cada equipo será en los cuartos de equipos o en su defecto donde se encuentran los equipos activos de la red de datos.

Adicionalmente en esta sede está ubicado uno de los dos servidores del sistema de control de acceso.

En el primer piso del edificio se ubica una controladora y el otro servidor del sistema, en el resto de los pisos únicamente esta la controladora.

Figura 13. Primer piso edificio Bogotá

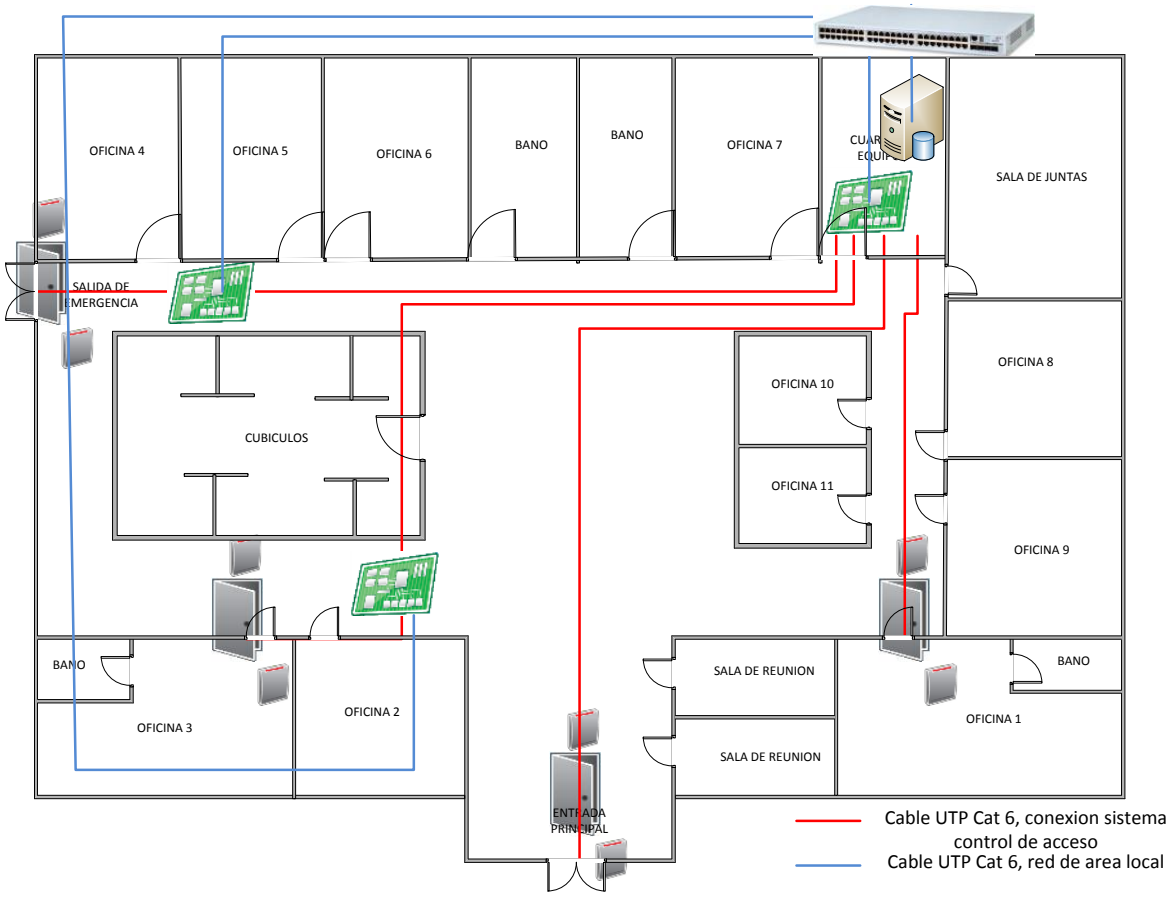


Figura 14. Piso tipo edificio Bogotá

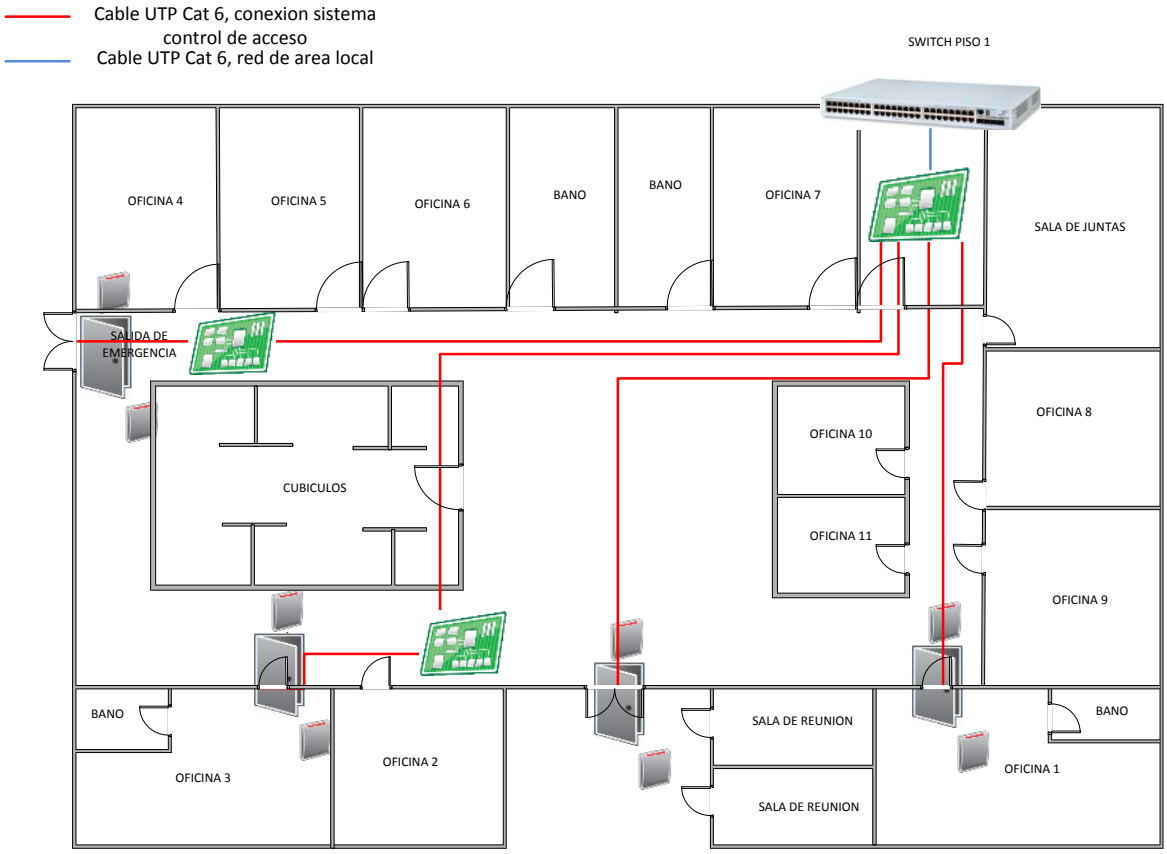


Tabla 4. Diseño sistema control de acceso Bogotá

BOGOTA															
EQUIPO/UBICACION	Piso 1					Piso 2					Piso 3				
	Cuarto de equipos	Entrada principal	Oficina 1	Oficina 3	Salida de emergencia	Cuarto de equipos	Entrada principal	Oficina 1	Oficina 3	Salida de emergencia	Cuarto de equipos	Entrada principal	Oficina 1	Oficina 3	Salida de emergencia
Servidor	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0
Módulo crecimiento LNL 1320	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1
Molinete	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1
Lectora de proximidad	0	2	2	2	2	0	2	2	2	2	0	2	2	2	2
Contacto magnético	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1
Módulo de entradas	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0
Módulo de salidas	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0

BOGOTA															
EQUIPO/UBICACION	Piso 4					Piso 5					Piso 6				
	Cuarto de equipos	Entrada principal	Oficina 1	Oficina 3	Salida de emergencia	Cuarto de equipos	Entrada principal	Oficina 1	Oficina 3	Salida de emergencia	Cuarto de equipos	Entrada principal	Oficina 1	Oficina 3	Salida de emergencia
Servidor	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0
Modulo crecimiento LNL 1320	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1
Molinete	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Electroimán	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1
Lectora de proximidad	0	2	2	2	2	0	2	2	2	2	0	2	2	2	2
Contacto magnético	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1
Módulo de entradas	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0
Módulo de salidas	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0

BOGOTA															
EQUIPO/UBICACION	**Piso 7**					**Piso 8**					**Piso 9**				
	Cuarto de equipos	**Entrada principal**	**Oficina 1**	**Oficina 3**	**Salida de emergencia**	**Cuarto de equipos**	**Entrada principal**	**Oficina 1**	**Oficina 3**	**Salida de emergencia**	**Cuarto de equipos**	**Entrada principal**	**Oficina 1**	**Oficina 3**	**Salida de emergencia**
Servidor	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0
Módulo crecimiento LNL 1300	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1
Molinete	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1
Lectora de proximidad	0	2	2	2	2	0	2	2	2	2	0	2	2	2	2
Contacto magnético	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1
Módulo de entradas	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0
Módulo de salidas	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0

Tabla 5. Resumen equipos sistema control de acceso Bogotá

	CANTIDAD	ÍTEM	REFERENCIA	MARCA
1	1	Servidor	Dell	Dell
2	9	Controladoras	LNL-2200	Lenel
3	18	Modulo interface crecimiento	LNL 1320	Lenel
4	0	molinetes	Boonedam	Boonedam
5	36	Electroimanes	Zebra	Zebra
6	72	Lectoras de proximidad	RP40	HID
7	36	Contacto magnético	Zebra	Zebra
8	9	Módulo de entradas	LNL-1100	Lenel
9	9	Módulo de salidas	LNL-1200	Lenel

2.3.3 **Diseño Medellín.** Para la sede de Medellín de acuerdo al análisis realizado se estableció que se requieren 9 controladoras. La ubicación de cada equipo será en los cuartos de equipos o en su defecto donde se encuentran los equipos activos de la red de datos.

Figura 15. Edificio oficinas Medellín primer piso

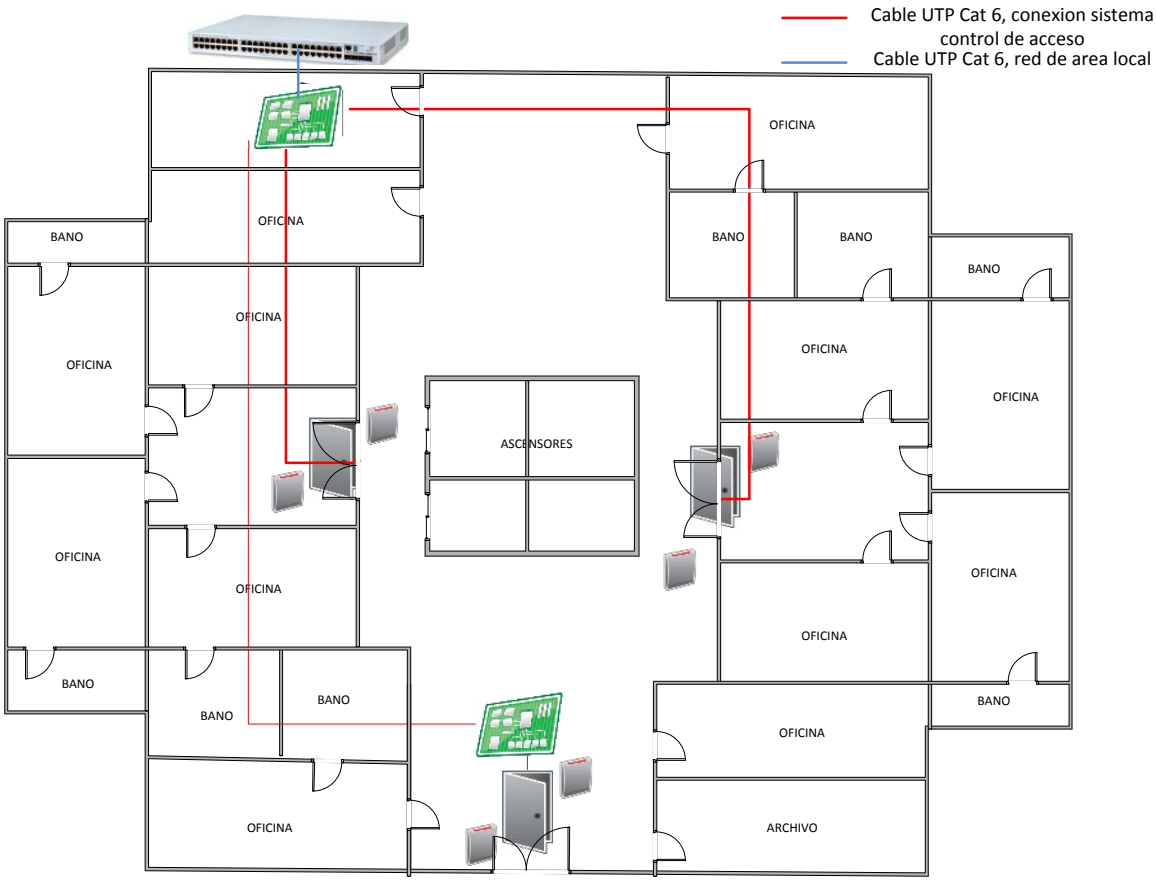


Figura 16. Edificio oficinas Medellín piso 2 al 8

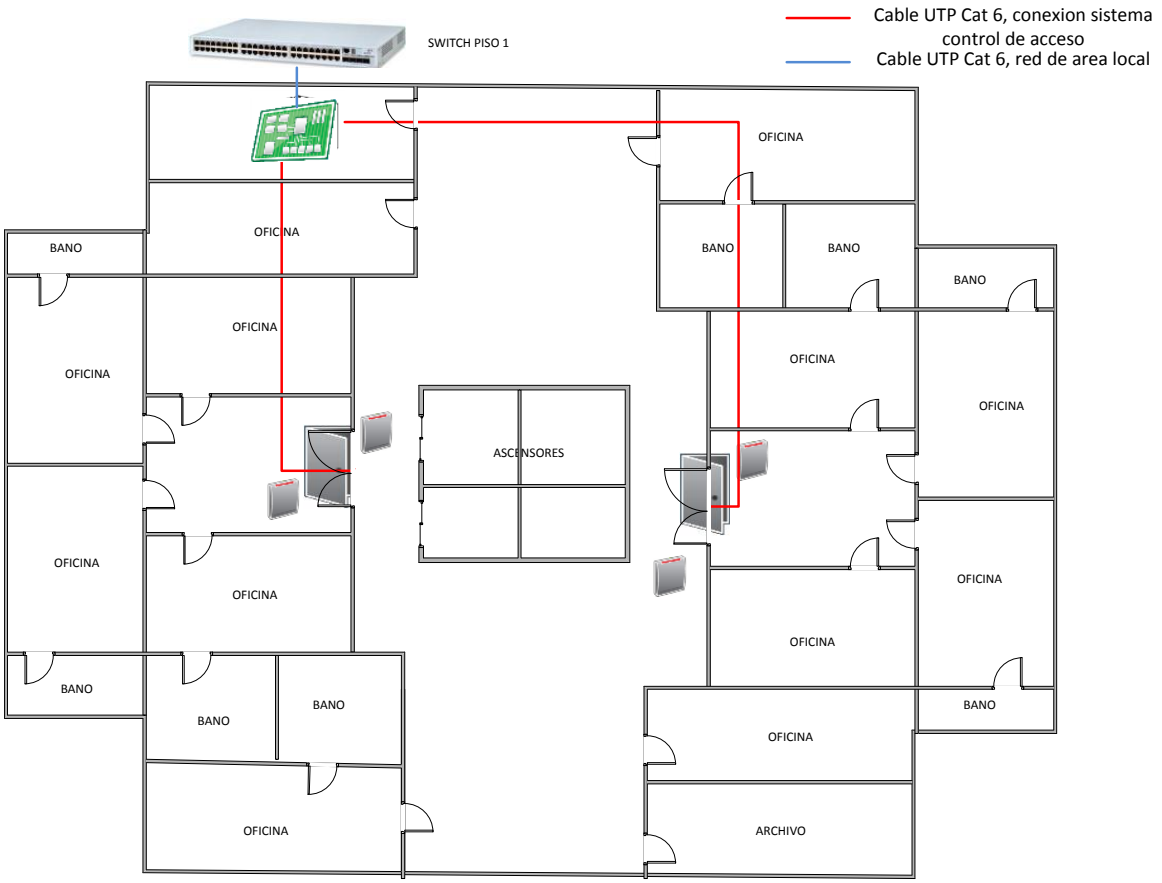


Tabla 6. Diseño sistema control de acceso Medellín

MEDELLIN										
EQUIPO/UBICACIÓN	Piso 1				Piso 2			Piso 3		
	Cuarto de equipos	Entrada principal	Costado oriental	Costado occidental	Cuarto de equipos	Costado oriental	Costado occidental	Cuarto de equipos	Costado oriental	Costado occidental
Servidor	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	0	1	0	0	1	0	0
Módulo crecimiento LNL 1320	0	1	0	0	0	0	0	0	0	0
Molinete	0	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	1	0	1	1	0	1	1
Lectora de proximidad	0	2	2	2	0	2	2	0	2	2
Contacto magnético	0	1	1	1	0	1	1	0	1	1
Módulo de entradas	1	0	0	0	1	0	0	1	0	0
Módulo de salidas	1	0	0	0	1	0	0	1	0	0

MEDELLIN									
EQUIPO/UBICACIÓN	Piso 4			Piso 5			Piso 6		
	Cuarto de equipos	Costado oriental	Costado occidental	Cuarto de equipos	Costado oriental	Costado occidental	Cuarto de equipos	Costado oriental	Costado occidental
Servidor	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	1	0	0	1	0	0
Módulo crecimiento LNL 1320	0	0	0	0	0	0	0	0	0
Molinete	0	0	0	0	0	0	0	0	0

Electroimán	0	1	1	0	1	1	0	1	1
Lectora de proximidad	0	2	2	0	2	2	0	2	2
Contacto magnético	0	1	1	0	1	1	0	1	1
Módulo de entradas	1	0	0	1	0	0	1	0	0
Módulo de salidas	1	0	0	1	0	0	1	0	0

MEDELLIN									
EQUIPO/UBICACIÓN	**Piso 7**			**Piso 8**			**Piso 9**		
	Cuarto de equipos	**Costado oriental**	**Costado occidental**	**Cuarto de equipos**	**Costado oriental**	**Costado occidental**	**Cuarto de equipos**	**Costado oriental**	**Costado occidental**
Servidor	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	1	0	0	1	0	0
Módulo crecimiento LNL 1320	0	0	0	0	0	0	0	0	0
Molinete	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	0	1	1	0	1	1
Lectora de proximidad	0	2	2	0	2	2	0	2	2
Contacto magnético	0	1	1	0	1	1	0	1	1
Módulo de entradas	1	0	0	1	0	0	1	0	0
Módulo de salidas	1	0	0	1	0	0	1	0	0

Tabla 7. Resumen equipos sistema control de acceso Medellín

	CANTIDAD	ÍTEM	REFERENCIA	MARCA
1	0	Servidor	Dell	Dell
2	9	Controladoras	LNL-2200	Lenel
3	1	Modulo interface crecimiento	LNL 1320	Lenel
4	0	molinetes	Boonedam	Boonedam
5	19	Electroimanes	Zebra	Zebra
6	38	Lectoras de proximidad	RP40	HID
7	19	Contacto magnético	Zebra	Zebra
8	9	Módulo de entradas	LNL-1100	Lenel
9	9	Módulo de salidas	LNL-1200	Lenel

2.3.4 **Diseño Cali.** Para la sede de Cali de acuerdo al análisis realizado se estableció que se requieren 9 controladoras. La ubicación de cada equipo será en los cuartos de equipos o en su defecto donde se encuentran los equipos activos de la red de datos.

Figura 17. Edificio oficinas Cali

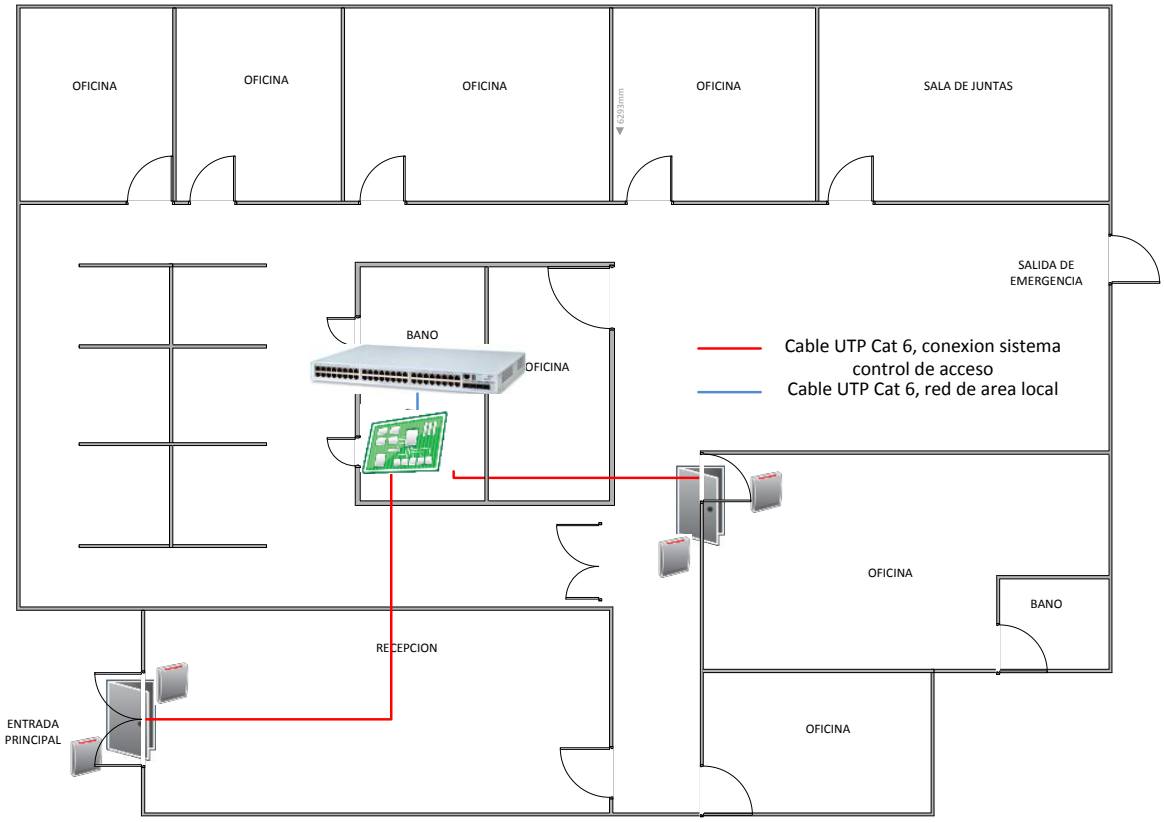


Tabla 8. Diseño sistema control de acceso Cali

CALI												
EQUIPO/UBICACION	Piso 1			Piso 2			Piso 3			Piso 4		
	Cuarto de equipos	Entrada principal	Oficina 1	Cuarto de equipos	Costado oriental	Oficina 1	Cuarto de equipos	Costado oriental	Oficina 1	Cuarto de equipos	Costado oriental	Oficina 1
Servidor	0	0	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	1	0	0	1	0	0	1	0	0
Módulo crecimiento LNL 1300	0	0	0	0	0	0	0	0	0	0	0	0
Molinete	0	0	0	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	0	1	1	0	1	1	0	1	1
Lectora de proximidad	0	2	2	0	2	2	0	2	2	0	2	2
Contacto magnético	0	1	1	0	1	1	0	1	1	0	1	1
Módulo de entradas	1	0	0	1	0	0	1	0	0	1	0	0
Módulo de salidas	1	0	0	1	0	0	1	0	0	1	0	0

CALI															
EQUIPO/UBICACION	Piso 5			Piso 6			Piso 7			Piso 8			Piso 9		
	Cuarto de equipos	Costado oriental	Oficina 1	Cuarto de equipos	Costado oriental	Oficina 1	Cuarto de equipos	Costado oriental	Oficina 1	Cuarto de equipos	Costado oriental	Oficina 1	Cuarto de equipos	Costado oriental	Oficina 1
Servidor	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
Módulo crecimiento LNL 1300	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Molinete	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
Lectora de proximidad	0	2	2	0	2	2	0	2	2	0	2	2	0	2	2
Contacto magnética	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1

Módulo de entradas	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
Módulo de salidas	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0

Tabla 9. Resumen equipos sistema control de acceso Cali

	CANTIDAD	ÍTEM	REFERENCIA	MARCA
1	0	Servidor	Dell	Dell
2	9	Controladoras	LNL-2200	Lenel
3	0	Modulo interface crecimiento	LNL 1300	Lenel
4	0	molinetes	Boonedam	Boonedam
5	18	Electroimanes	Zebra	Zebra
6	36	Lectoras de proximidad	RP40	HID
7	18	Contacto magnético	Zebra	Zebra
8	9	Módulo de entradas	LNL-1100	Lenel
9	9	Módulo de salidas	LNL-1200	Lenel

2.3.5 **Diseño Bucaramanga.** Para la sede de Bucaramanga de acuerdo al análisis realizado se estableció que se requieren 9 controladoras. La ubicación de cada equipo será en los cuartos de equipos o en su defecto donde se encuentran los equipos activos de la red de datos.

Figura 18. Edificio oficinas Bucaramanga

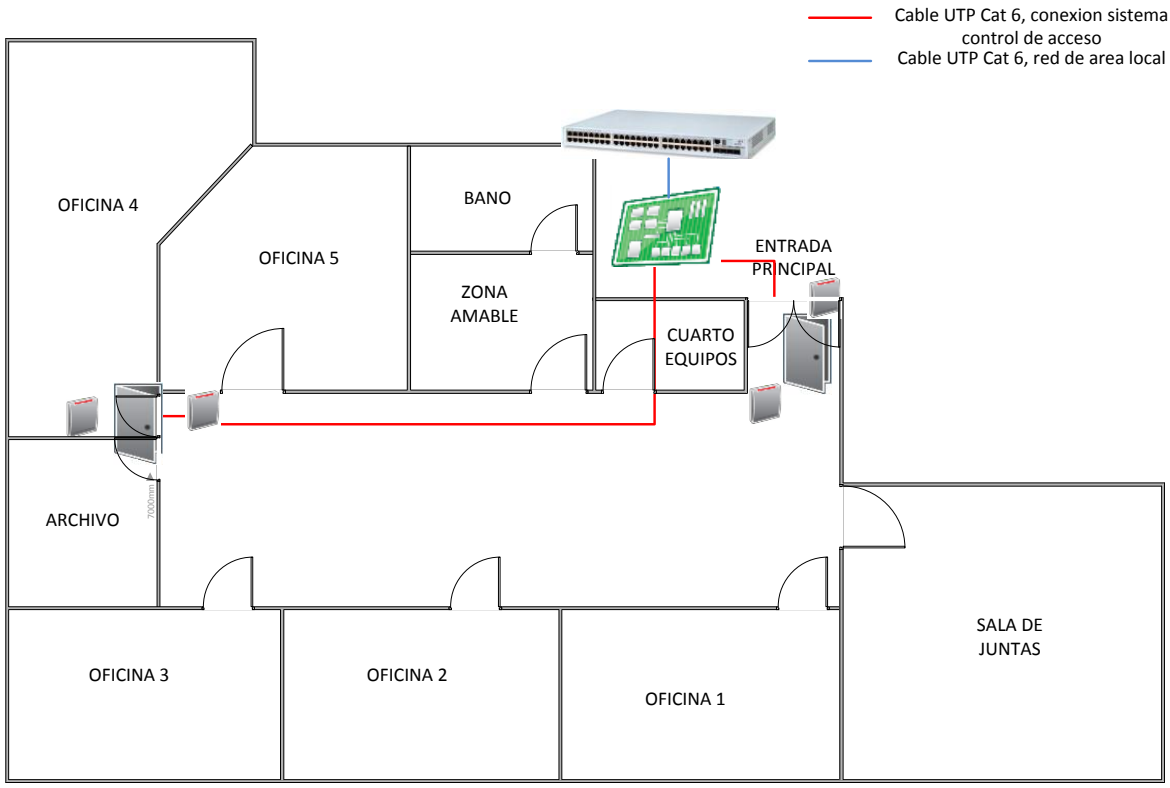


Tabla 10. Diseño sistema control de acceso Bucaramanga

BUCARAMANGA												
EQUIPO/UBICACION	Piso 1			Piso 2			Piso 3			Piso 4		
	Cuarto de equipos	Entrada principal	Oficina 4	Cuarto de equipos	Costado oriental	Oficina 4	Cuarto de equipos	Costado oriental	Oficina 4	Cuarto de equipos	Costado oriental	Oficina 4
Servidor	0	0	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	1	0	0	1	0	0	1	0	0
Módulo crecimiento LNL 1300	0	0	0	0	0	0	0	0	0	0	0	0
Molinete	0	0	0	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	0	1	1	0	1	1	0	1	1
Lectora de proximidad	0	2	2	0	2	2	0	2	2	0	2	2
Contacto magnética	0	1	1	0	1	1	0	1	1	0	1	1
Módulo de entradas	1	0	0	1	0	0	1	0	0	1	0	0
Módulo de salidas	1	0	0	1	0	0	1	0	0	1	0	0

BUCARAMANGA															
EQUIPO/UBICACION	Piso 5			Piso 6			Piso 7			Piso 8			Piso 9		
	Cuarto de equipos	Costado oriental	Oficina 4	Cuarto de equipos	Costado oriental	Oficina 4	Cuarto de equipos	Costado oriental	Oficina 4	Cuarto de equipos	Costado oriental	Oficina 4	Cuarto de equipos	Costado oriental	Oficina 4
Servidor	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
Modulo crecimiento LNL 1300	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Molinete	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
Lectora de proximidad	0	2	2	0	2	2	0	2	2	0	2	2	0	2	2
Contacto magnética	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1

Módulo de entradas	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
Módulo de salidas	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0

Tabla 11. Resumen equipos sistema control de acceso Bucaramanga

	CANTIDAD	ÍTEM	REFERENCIA	MARCA
1	0	Servidor	Dell	Dell
2	9	Controladoras	LNL-2200	Lenel
3	0	Modulo interface crecimiento	LNL 1300	Lenel
4	0	molinetes	Boonedam	Boonedam
5	18	Electroimanes	Zebra	Zebra
6	36	Lectoras de proximidad	RP40	HID
7	18	Contacto magnético	Zebra	Zebra
8	9	Módulo de entradas	LNL-1100	Lenel
9	9	Módulo de salidas	LNL-1200	Lenel

2.3.6 **Diseño Barranquilla.** Para la sede de Barranquilla de acuerdo al análisis realizado se estableció que se requieren 9 controladoras. La ubicación de cada equipo será en los cuartos de equipos o en su defecto donde se encuentran los equipos activos de la red de datos.

Figura 19. Edificio oficinas Barranquilla

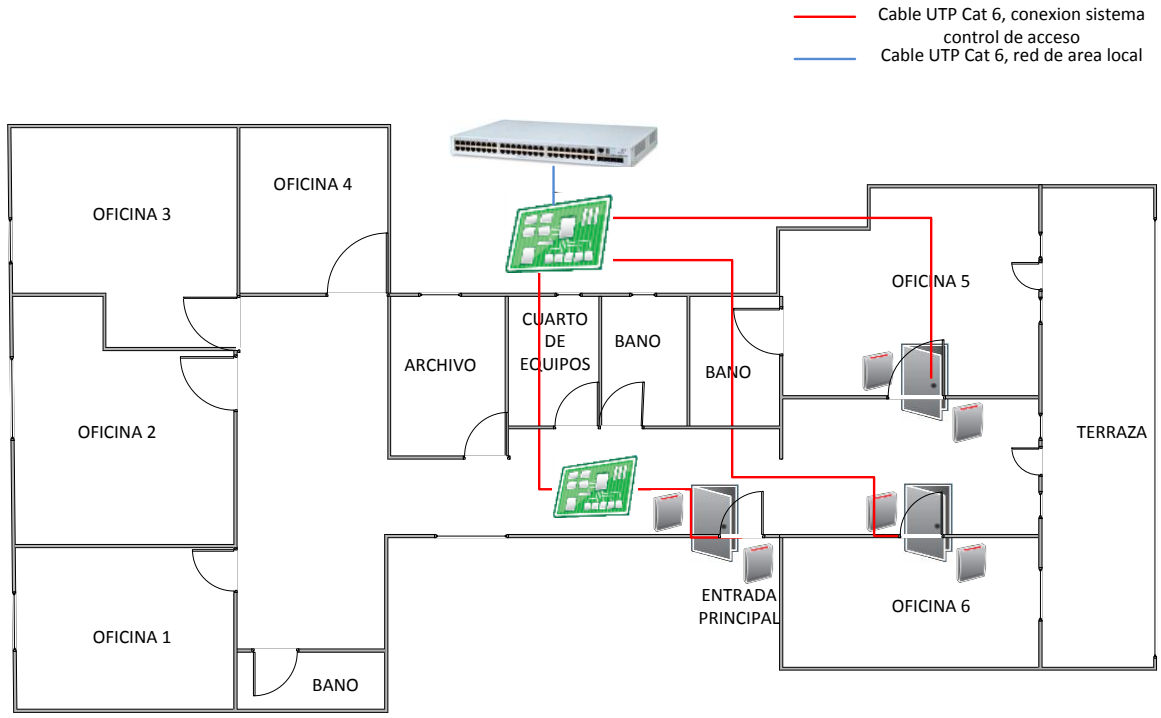


Tabla 12. Diseño sistema control de acceso Barranquilla

BARRANQUILLA												
EQUIPO/UBICACION	Piso 1				Piso 2				Piso 3			
	Cuarto de equipos	Entrada principal	Oficina 5	Oficina 6	Cuarto de equipos	Entrada principal	Oficina 5	Oficina 6	Cuarto de equipos	Entrada principal	Oficina 5	Oficina 6
Servidor	0	0	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	0	1	0	0	0	1	0	0	0
Módulo crecimiento LNL 1300	0	1	0	0	0	1	0	0	0	1	0	0
Molinete	0	0	0	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	1	0	1	1	1	0	1	1	1
Lectora de proximidad	0	2	2	2	0	2	2	2	0	2	2	2
Contacto magnética	0	1	1	1	0	1	1	1	0	1	1	1
Módulo de entradas	1	0	0	0	1	0	0	0	1	0	0	0
Módulo de salidas	1	0	0	0	1	0	0	0	1	0	0	0

BARRANQUILLA												
EQUIPO/UBICACION	Piso 4				Piso 5				Piso 6			
	Cuarto de equipos	Entrada principal	Oficina 5	Oficina 6	Cuarto de equipos	Entrada principal	Oficina 5	Oficina 6	Cuarto de equipos	Entrada principal	Oficina 5	Oficina 6
Servidor	0	0	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	0	1	0	0	0	1	0	0	0
Modulo crecimiento LNL 1300	0	1	0	0	0	1	0	0	0	1	0	0
Molinete	0	0	0	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	1	0	1	1	1	0	1	1	1

Lectora de proximidad	0	2	2	2	0	2	2	2	0	2	2	2
Contacto magnética	0	1	1	1	0	1	1	1	0	1	1	1
Módulo de entradas	1	0	0	0	1	0	0	0	1	0	0	0
Módulo de salidas	1	0	0	0	1	0	0	0	1	0	0	0

BARRANQUILLA												
EQUIPO/UBICACION	**Piso 7**				**Piso 8**				**Piso 9**			
	Cuarto de equipos	**Entrada principal**	**Oficina 5**	**Oficina 6**	**Cuarto de equipos**	**Entrada principal**	**Oficina 5**	**Oficina 6**	**Cuarto de equipos**	**Entrada principal**	**Oficina 5**	**Oficina 6**
Servidor	0	0	0	0	0	0	0	0	0	0	0	0
Controladora LNL 2200	1	0	0	0	1	0	0	0	1	0	0	0
Módulo crecimiento LNL 1300	0	1	0	0	0	1	0	0	0	1	0	0
Molinete	0	0	0	0	0	0	0	0	0	0	0	0
Electroimán	0	1	1	1	0	1	1	1	0	1	1	1
Lectora de proximidad	0	2	2	2	0	2	2	2	0	2	2	2
Contacto magnético	0	1	1	1	0	1	1	1	0	1	1	1
Módulo de entradas	1	0	0	0	1	0	0	0	1	0	0	0
Módulo de salidas	1	0	0	0	1	0	0	0	1	0	0	0

Tabla 13. Resumen equipos sistema control de acceso Barranquilla

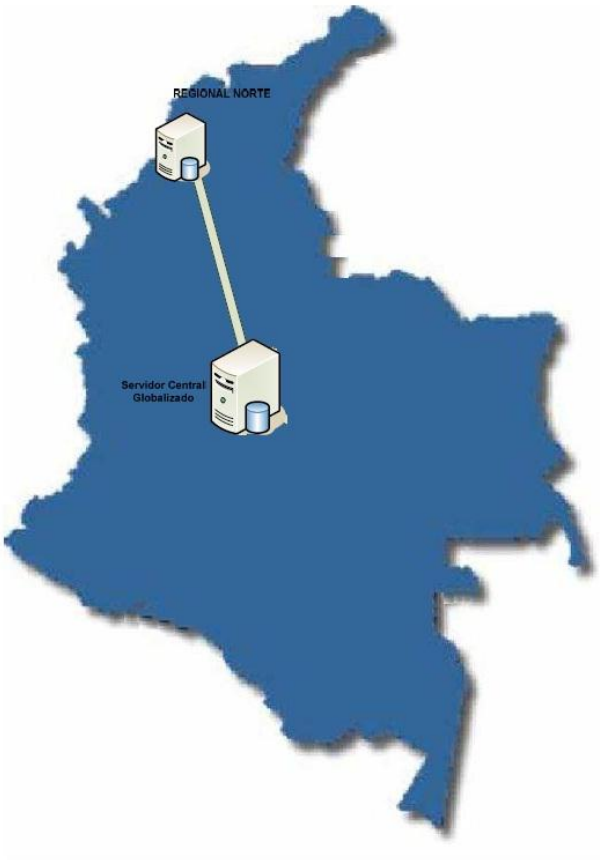
	CANTIDAD	ÍTEM	REFERENCIA	MARCA
1	0	Servidor	Dell	Dell
2	9	Controladoras	LNL-2200	Lenel
3	9	Modulo interface crecimiento	LNL 1300	Lenel
4	0	molinetes	Boonedam	Boonedam
5	27	Electroimanes	Zebra	Zebra
6	54	Lectoras de proximidad	RP40	HID
7	27	Contacto magnético	Zebra	Zebra
8	9	Módulo de entradas	LNL-1100	Lenel
9	9	Módulo de salidas	LNL-1200	Lenel

2.3.7 **Esquema ubicación servidores.** Debido a la criticidad y tamaño de las sedes se estableció que se ubicara un servidor para la regional Norte en la sede de Cartagena el cual atenderá la sede de Cartagena y barranquilla.

El otro servidor y el cual será el servidor central globalizado estará ubicado en la sede de Bogotá y atenderá las sedes de Bogotá, Medellín, Cali, y Bucaramanga.

Estos servidores estarán sincronizados y en caso de falla de cualquiera podrá soportar la operación nacional.

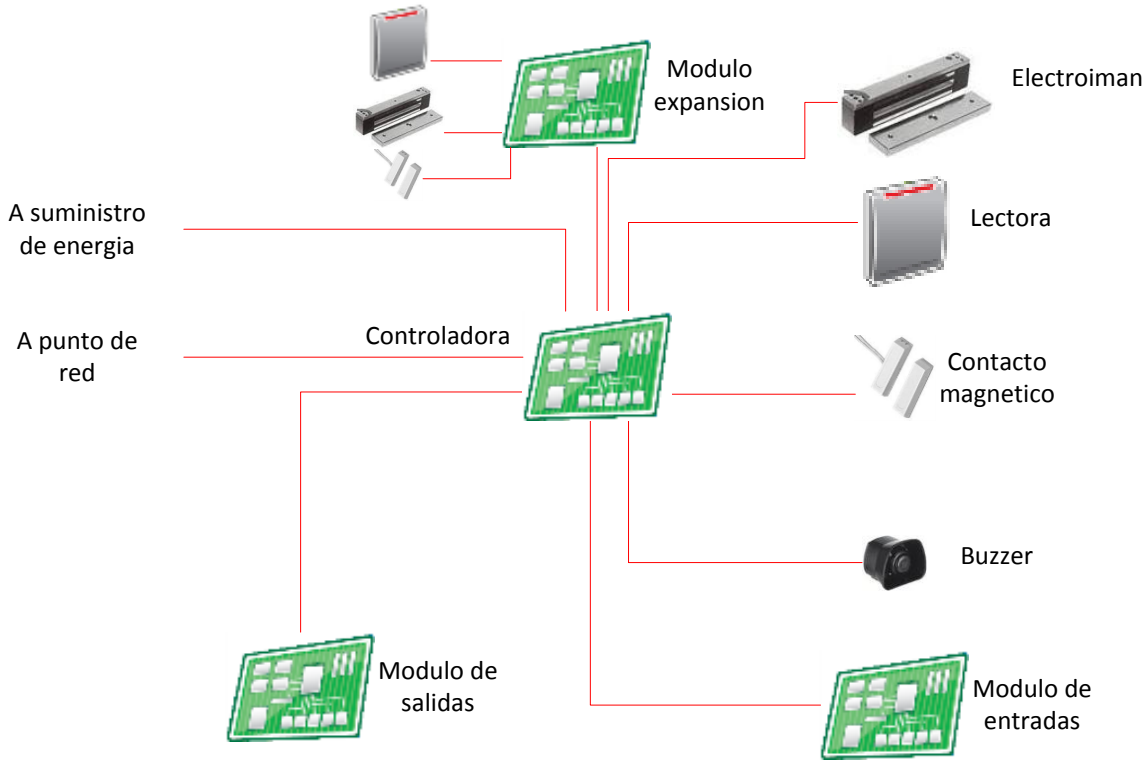
Figura 20. Esquema ubicación servidores



2.3.8 **Esquema típico de conexión de Microcontrolador.** A continuación se describe el esquema típico de conexionado del microcontrolador con el resto de los elementos en campo.

A cada micro se deberán conectar las lectoras, los botones de salida o emergencia, los contactos magnéticos, los electroimanes, buzzer para los casos de alarma auditiva para los casos en que la puerta de emergencia se abra o se deje la puerta mucho tiempo abierta.

Figura 21. Esquema típico de conexionado del micro



2.4 DISEÑO DEL MODELO DE INTERCONEXIÓN

A continuación se realiza la configuración de la red

Tabla 14. Rango direcciones IP equipos sistema control de acceso

Descripción	Red	Rango Utilizar
WAN	CARTAGENA	10.168.79.90
	BOGOTA	10.160.52.168
	MEDELLIN	10.164.48.238
	CALI	10.162.41.118
	BUCARAMANGA	10.166.60.246
	BARRANQUILLA	10.168.31.250

Tabla 15. Tabla subnetting

Descripción	Red	# Bit	Ip Utilizar	Ip SubRed	Ip BroadCast	Rango Utilizar	Mask (I)	Mask (Decimal
LAN	BARRANQUILLA	4	9	10.32.14.0	10.32.14.255	10.32.14.1-254	/24	255.255.255.0
	BOGOTA	4	10	10.32.6.0	10.32.6.255	10.32.6.1-254	/24	255.255.255.0
	BUCARAMANGA	4	9	10.32.12.0	10.32.12.255	10.32.12.1-254	/24	255.255.255.0
	CALI	4	9	10.32.10.0	10.32.10.255	10.32.10.1-254	/24	255.255.255.0
	CARTAGENA	4	12	10.32.4.0	10.32.4.255	10.32.4.1-254	/24	255.255.255.0
	MEDELLIN	4	9	10.32.8.0	10.32.8.255	10.32.8.1-254	/24	255.255.255.0

Tabla 16. Tabla asignación direcciones IP

OFICINA	NOM_EQUIPO	TIPO	IP	MASK	GATEWAY
BARRANQUILLA	BAQ_MICRO_01	MC	10.32.14.20	255.255.255.0	10.32.14.1
BARRANQUILLA	BAQ_MICRO_02	MC	10.32.14.21	255.255.255.0	10.32.14.1
BARRANQUILLA	BAQ_MICRO_03	MC	10.32.14.22	255.255.255.0	10.32.14.1
BARRANQUILLA	BAQ_MICRO_04	MC	10.32.14.23	255.255.255.0	10.32.14.1
BARRANQUILLA	BAQ_MICRO_05	MC	10.32.14.24	255.255.255.0	10.32.14.1
BARRANQUILLA	BAQ_MICRO_06	MC	10.32.14.25	255.255.255.0	10.32.14.1
BARRANQUILLA	BAQ_MICRO_07	MC	10.32.14.26	255.255.255.0	10.32.14.1
BARRANQUILLA	BAQ_MICRO_08	MC	10.32.14.27	255.255.255.0	10.32.14.1
BARRANQUILLA	BAQ_MICRO_09	MC	10.32.14.28	255.255.255.0	10.32.14.1
BOGOTA	BOG_SERVER	SERVER	10.32.6.10	255.255.255.0	10.32.6.1
BOGOTA	BOG_MICRO_01	MC	10.32.6.20	255.255.255.0	10.32.6.1
BOGOTA	BOG_MICRO_02	MC	10.32.6.21	255.255.255.0	10.32.6.1
BOGOTA	BOG_MICRO_03	MC	10.32.6.22	255.255.255.0	10.32.6.1
BOGOTA	BOG_MICRO_04	MC	10.32.6.23	255.255.255.0	10.32.6.1
BOGOTA	BOG_MICRO_05	MC	10.32.6.24	255.255.255.0	10.32.6.1
BOGOTA	BOG_MICRO_06	MC	10.32.6.25	255.255.255.0	10.32.6.1
BOGOTA	BOG_MICRO_07	MC	10.32.6.26	255.255.255.0	10.32.6.1
BOGOTA	BOG_MICRO_08	MC	10.32.6.27	255.255.255.0	10.32.6.1
BOGOTA	BOG_MICRO_09	MC	10.32.6.28	255.255.255.0	10.32.6.1
BUCARAMANGA	BGA_MICRO_01	MC	10.32.12.20	255.255.255.0	10.32.12.1
BUCARAMANGA	BGA_MICRO_02	MC	10.32.12.21	255.255.255.0	10.32.12.1
BUCARAMANGA	BGA_MICRO_03	MC	10.32.12.22	255.255.255.0	10.32.12.1
BUCARAMANGA	BGA_MICRO_04	MC	10.32.12.23	255.255.255.0	10.32.12.1
BUCARAMANGA	BGA_MICRO_05	MC	10.32.12.24	255.255.255.0	10.32.12.1
BUCARAMANGA	BGA_MICRO_06	MC	10.32.12.25	255.255.255.0	10.32.12.1
BUCARAMANGA	BGA_MICRO_07	MC	10.32.12.26	255.255.255.0	10.32.12.1
BUCARAMANGA	BGA_MICRO_08	MC	10.32.12.27	255.255.255.0	10.32.12.1
BUCARAMANGA	BGA_MICRO_09	MC	10.32.12.28	255.255.255.0	10.32.12.1
CALI	CLO_MICRO_01	MC	10.32.10.20	255.255.255.0	10.32.10.1
CALI	CLO_MICRO_02	MC	10.32.10.21	255.255.255.0	10.32.10.1
CALI	CLO_MICRO_03	MC	10.32.10.22	255.255.255.0	10.32.10.1
CALI	CLO_MICRO_04	MC	10.32.10.23	255.255.255.0	10.32.10.1
CALI	CLO_MICRO_05	MC	10.32.10.24	255.255.255.0	10.32.10.1
CALI	CLO_MICRO_06	MC	10.32.10.25	255.255.255.0	10.32.10.1
CALI	CLO_MICRO_07	MC	10.32.10.26	255.255.255.0	10.32.10.1
CALI	CLO_MICRO_08	MC	10.32.10.27	255.255.255.0	10.32.10.1
CALI	CLO_MICRO_09	MC	10.32.10.28	255.255.255.0	10.32.10.1
CARTAGENA	CTG_SERVER	SERVER	10.32.4.10	255.255.255.0	10.32.4.1
CARTAGENA	CTG_MICRO_01	MC	10.32.4.20	255.255.255.0	10.32.4.1
CARTAGENA	CTG_MICRO_02	MC	10.32.4.21	255.255.255.0	10.32.4.1

CARTAGENA	CTG_MICRO_03	MC	10.32.4.22	255.255.255.0	10.32.4.1
CARTAGENA	CTG_MICRO_04	MC	10.32.4.23	255.255.255.0	10.32.4.1
CARTAGENA	CTG_MICRO_05	MC	10.32.4.24	255.255.255.0	10.32.4.1
CARTAGENA	CTG_MICRO_06	MC	10.32.4.25	255.255.255.0	10.32.4.1
CARTAGENA	CTG_MICRO_07	MC	10.32.4.26	255.255.255.0	10.32.4.1
CARTAGENA	CTG_MICRO_08	MC	10.32.4.27	255.255.255.0	10.32.4.1
CARTAGENA	CTG_MICRO_09	MC	10.32.4.28	255.255.255.0	10.32.4.1
CARTAGENA	CTG_MICRO_10	MC	10.32.4.29	255.255.255.0	10.32.4.1
CARTAGENA	CTG_MICRO_11	MC	10.32.4.30	255.255.255.0	10.32.4.1
MEDELLIN	MDE_MICRO_01	MC	10.32.8.20	255.255.255.0	10.32.8.1
MEDELLIN	MDE_MICRO_02	MC	10.32.8.21	255.255.255.0	10.32.8.1
MEDELLIN	MDE_MICRO_03	MC	10.32.8.22	255.255.255.0	10.32.8.1
MEDELLIN	MDE_MICRO_04	MC	10.32.8.23	255.255.255.0	10.32.8.1
MEDELLIN	MDE_MICRO_05	MC	10.32.8.24	255.255.255.0	10.32.8.1
MEDELLIN	MDE_MICRO_06	MC	10.32.8.25	255.255.255.0	10.32.8.1
MEDELLIN	MDE_MICRO_07	MC	10.32.8.26	255.255.255.0	10.32.8.1
MEDELLIN	MDE_MICRO_08	MC	10.32.8.27	255.255.255.0	10.32.8.1
MEDELLIN	MDE_MICRO_09	MC	10.32.8.28	255.255.255.0	10.32.8.1

Tabla 17. Tabla asignación direcciones IP WAN - LAN

OFICINA	TIPO	TIPO	BW	WAN	IP WAN	LAN	SEGMENTO LAN
BARRANQUILLA	Principal	Intranet	1024 K	FastEthernet0/1.531	10.168.31.250	FastEthernet0/1/1, FastEthernet0/1/2	10.32.14.1,10.32.15.1
BOGOTA	Principal	Intranet	1024 K	FastEthernet0/1.275	10.160.52.168	FastEthernet0/0, FastEthernet0/0/0	10.32.6.1,10.32.7.1
BUCARAMANGA	Principal	Intranet	1024 K	FastEthernet0/0.305	10.166.60.246	FastEthernet0/0/1, FastEthernet0/0/0	10.32.12.1,10.32.13.1
CALI	Principal	Intranet	1024 K	FastEthernet0/0	10.162.41.118	FastEthernet0/0/0, FastEthernet0/0/1,	10.32.10.1,10.32.11.1
CARTAGEN	Princi	Intra	1024 K	FastEthernet0	10.168.7	Fa0/0/0,	10.32.4.1,10.3

A MEDELLIN	pal	net		/0.175	9.90	Fa0/0/3	2.5.1
	Princi pal	Intra net	1024 K	FastEthernet0 /1	10.164.4 8.238	FastEthernet 0/0/0, FastEthernet 0/0/1	10.32.8.1,10.3 2.9.1

2.4.1 **Diseño De Interconexión Entre Las Sedes.** Para la interconexión de las 6 sedes se subcontrata con un operador de telecomunicaciones una solución empresarial de transmisión de datos soportados en una red multiservicios IP/MPLS de última generación, segura y privada, a través de la cual se realiza el intercambio de la información de manera práctica y eficiente, permitiendo incrementar en línea, el ancho de banda de acuerdo con las necesidades del negocio. Permitiendo la integración de redes LAN distribuidas geográficamente, conectando la oficina principal (Cartagena) con sus sucursales remotas, en un mismo ambiente seguro y de alta velocidad.

Para esta interconexión el proveedor proporciona la última milla y los equipos activos capa 3 (Routers)

En Cada una de las sedes se crean 2 VLAN: VLAN 1 para el manejo de PC, impresoras y otros equipos de trabajo; y la VLAN 4 de Seguridad donde se manejara el enrutamiento de todo el proyecto de SCA. Estos 2 segmentos se enrutaran a nivel WAN para la calidad de servicio de los datos.

Figura 22. Diseño con direccionamiento IP.

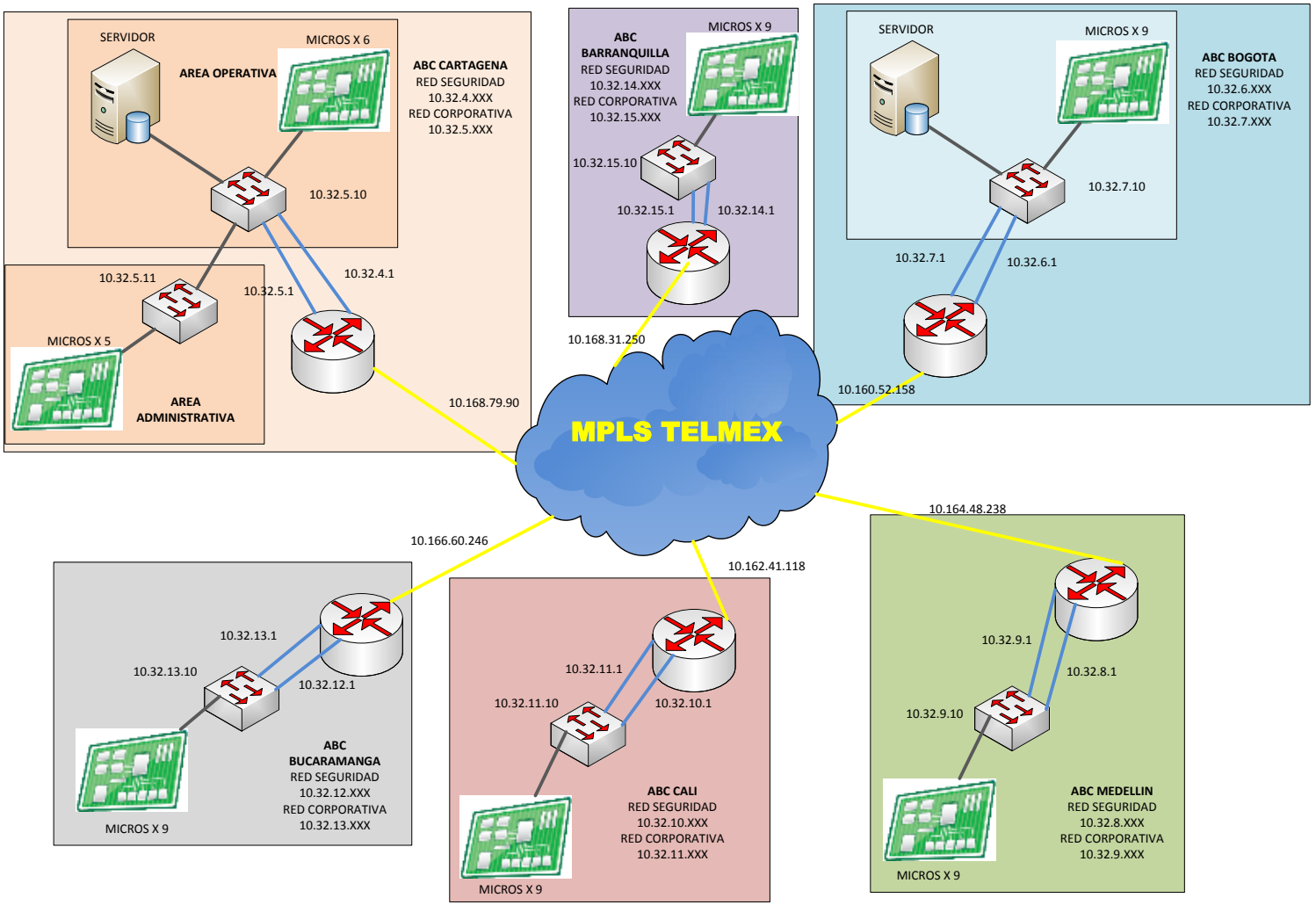


Figura 23. Diseño conectividad entre sedes

Figura 24. Diseño conectividad sede Bogotá

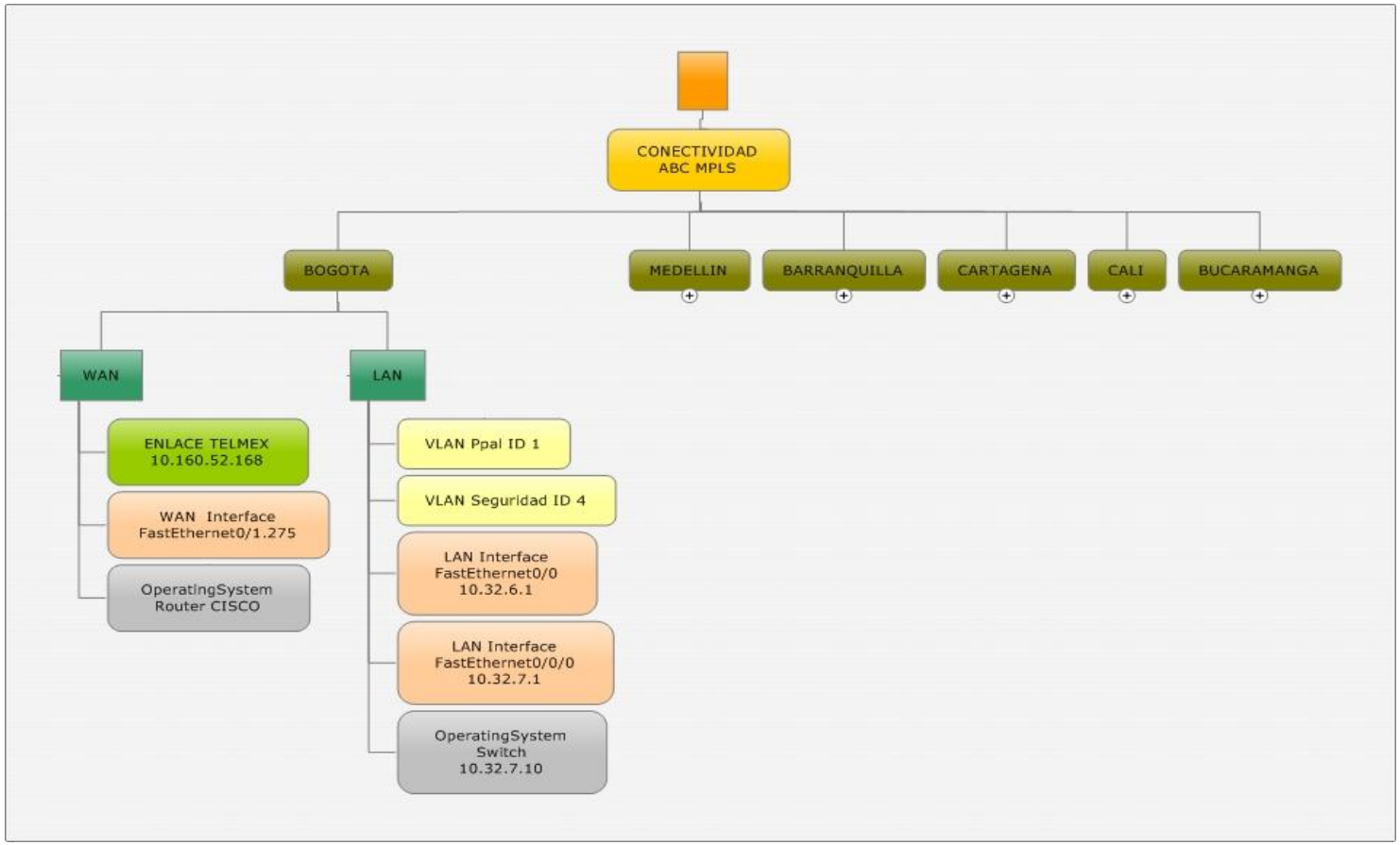


Figura 25. Diseño conectividad sede Medellín

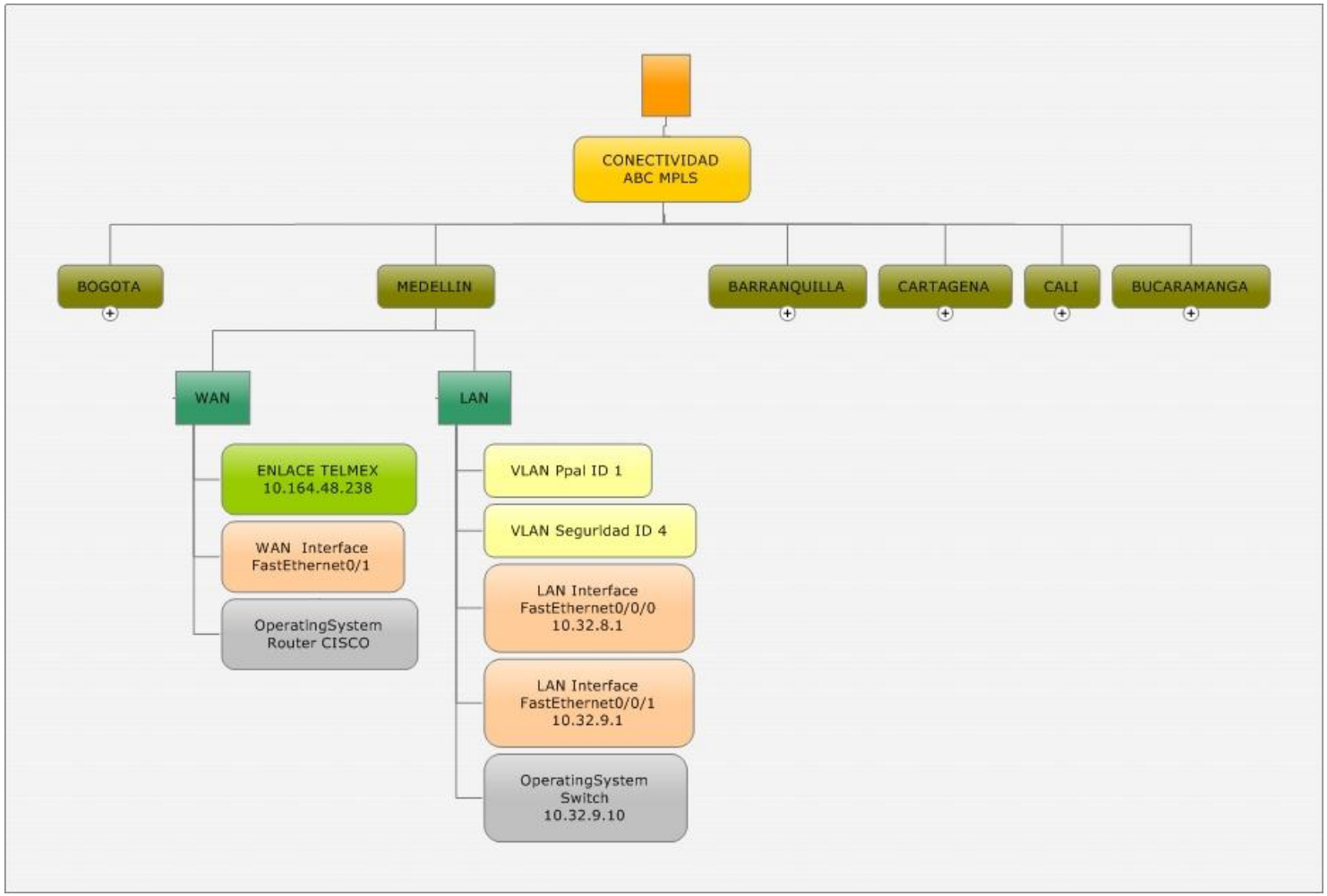


Figura 26. Diseño conectividad sede Barranquilla

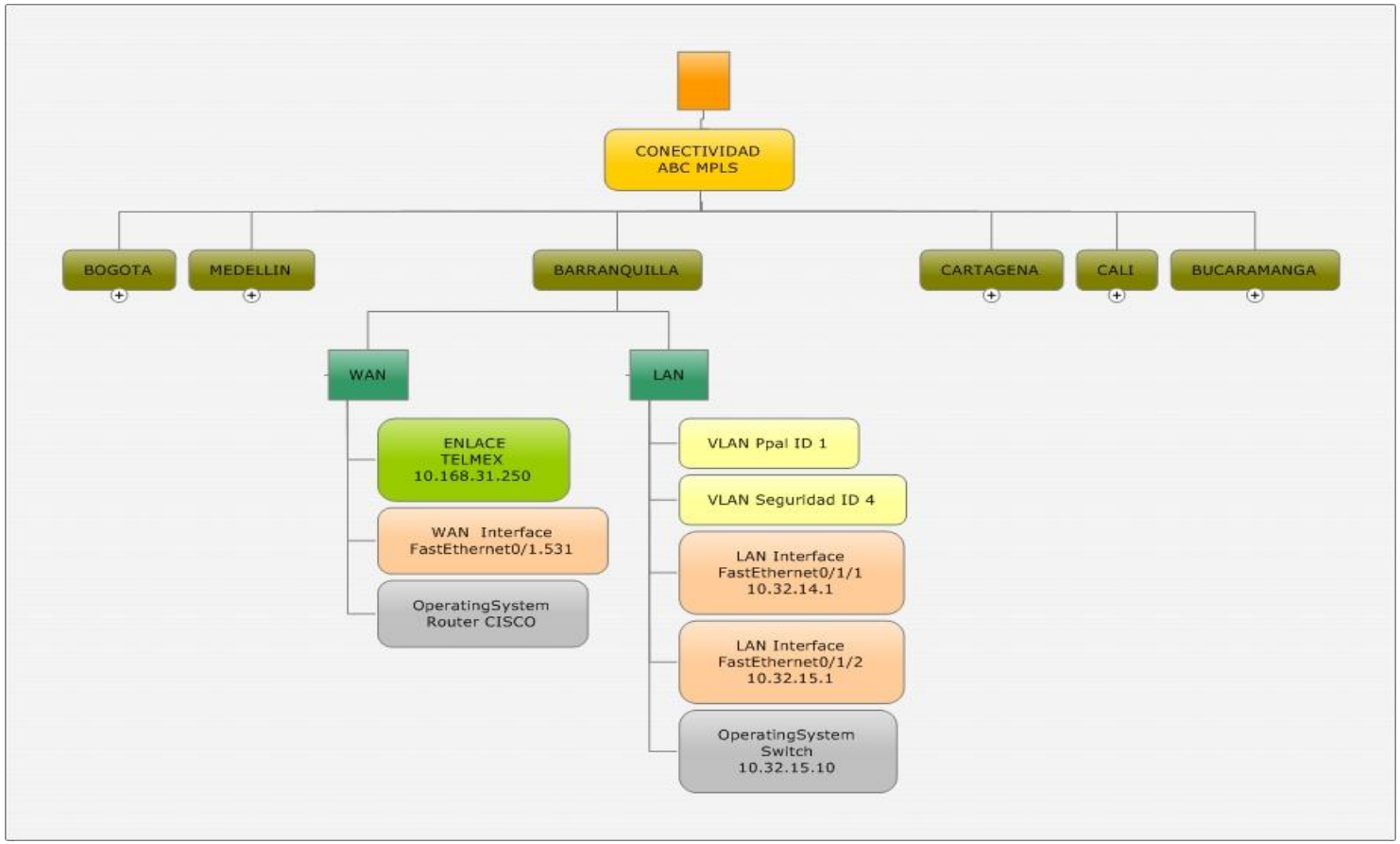


Figura 27. Diseño conectividad sede Cartagena

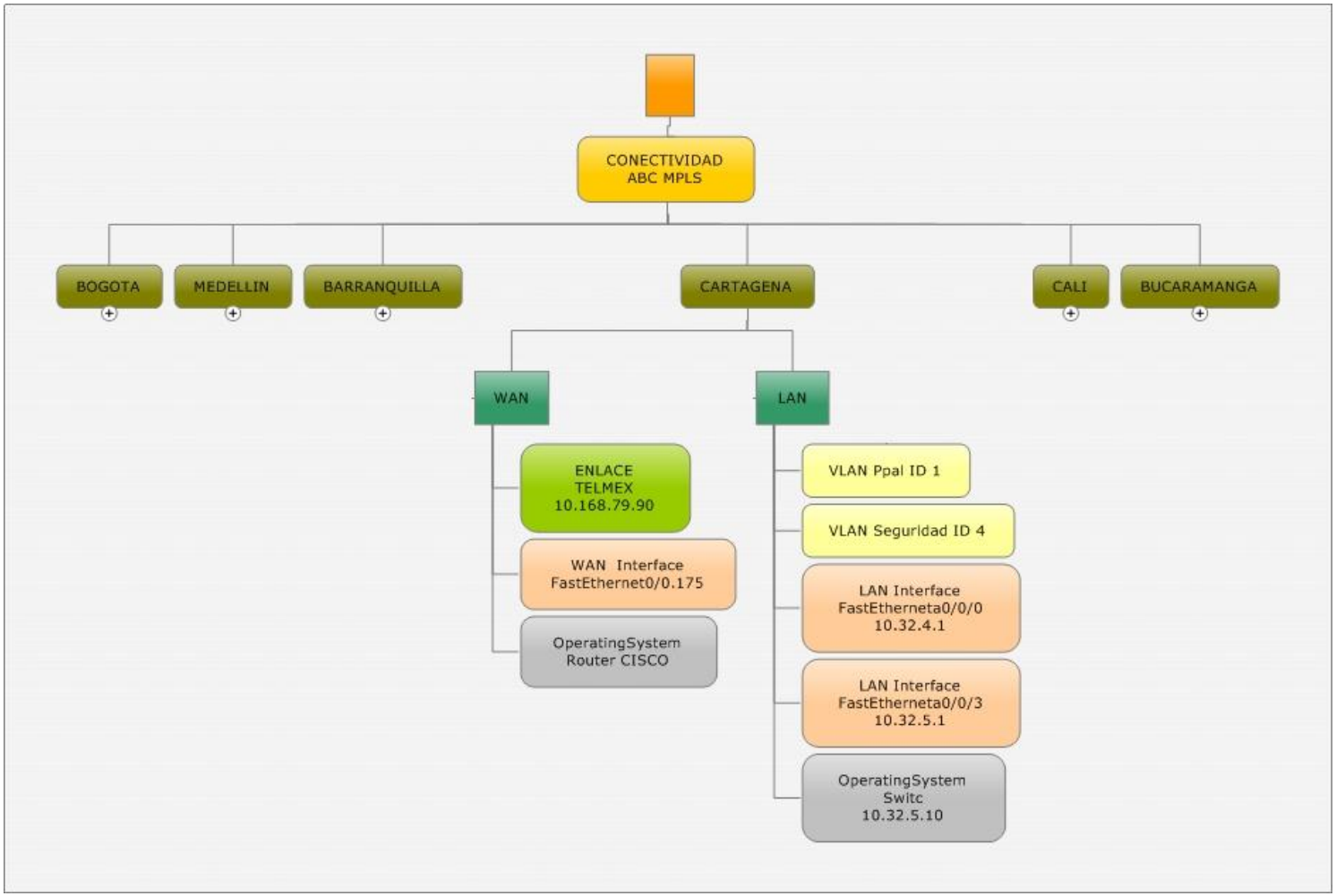


Figura 28. Diseño conectividad sede Cali

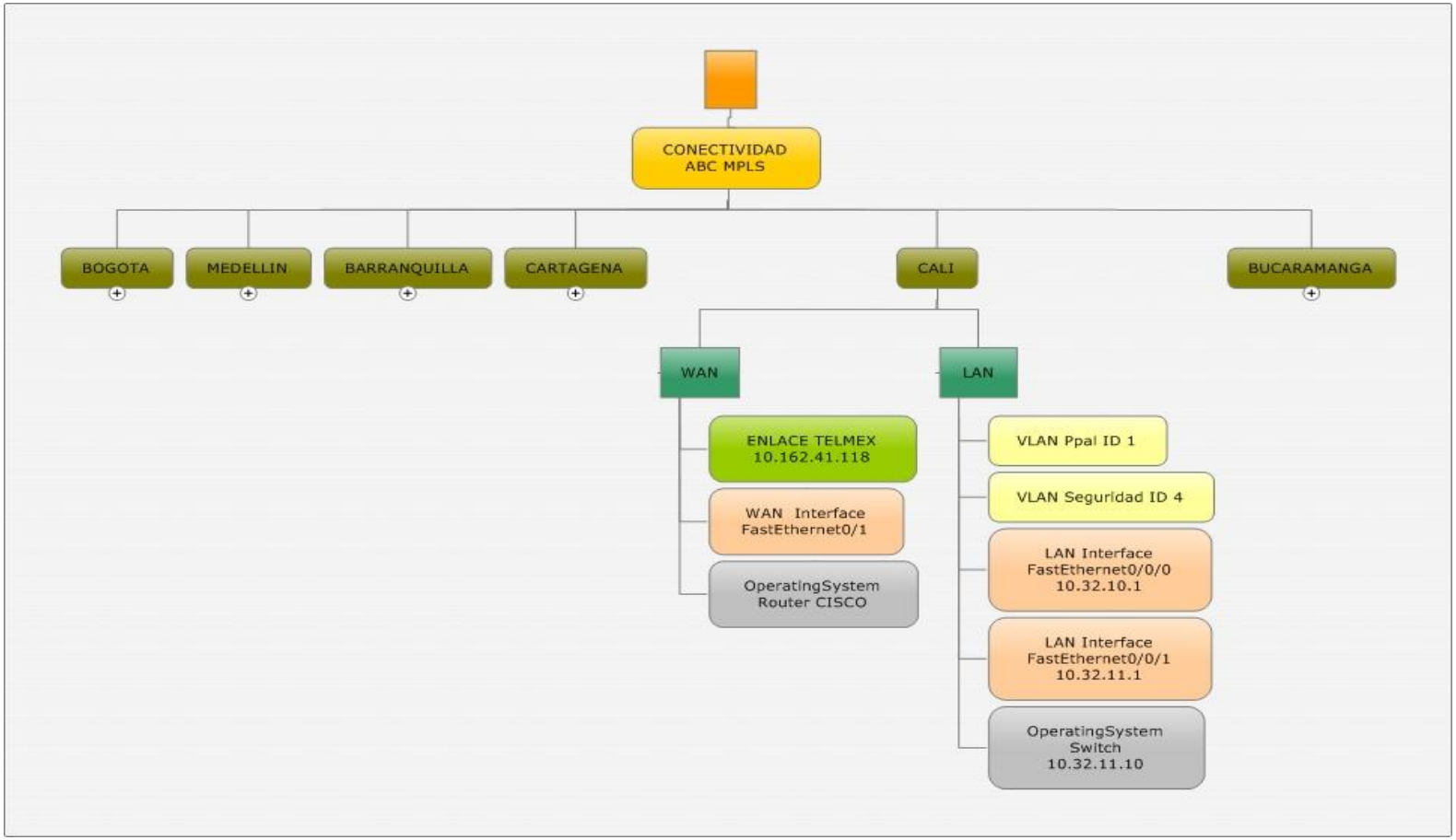
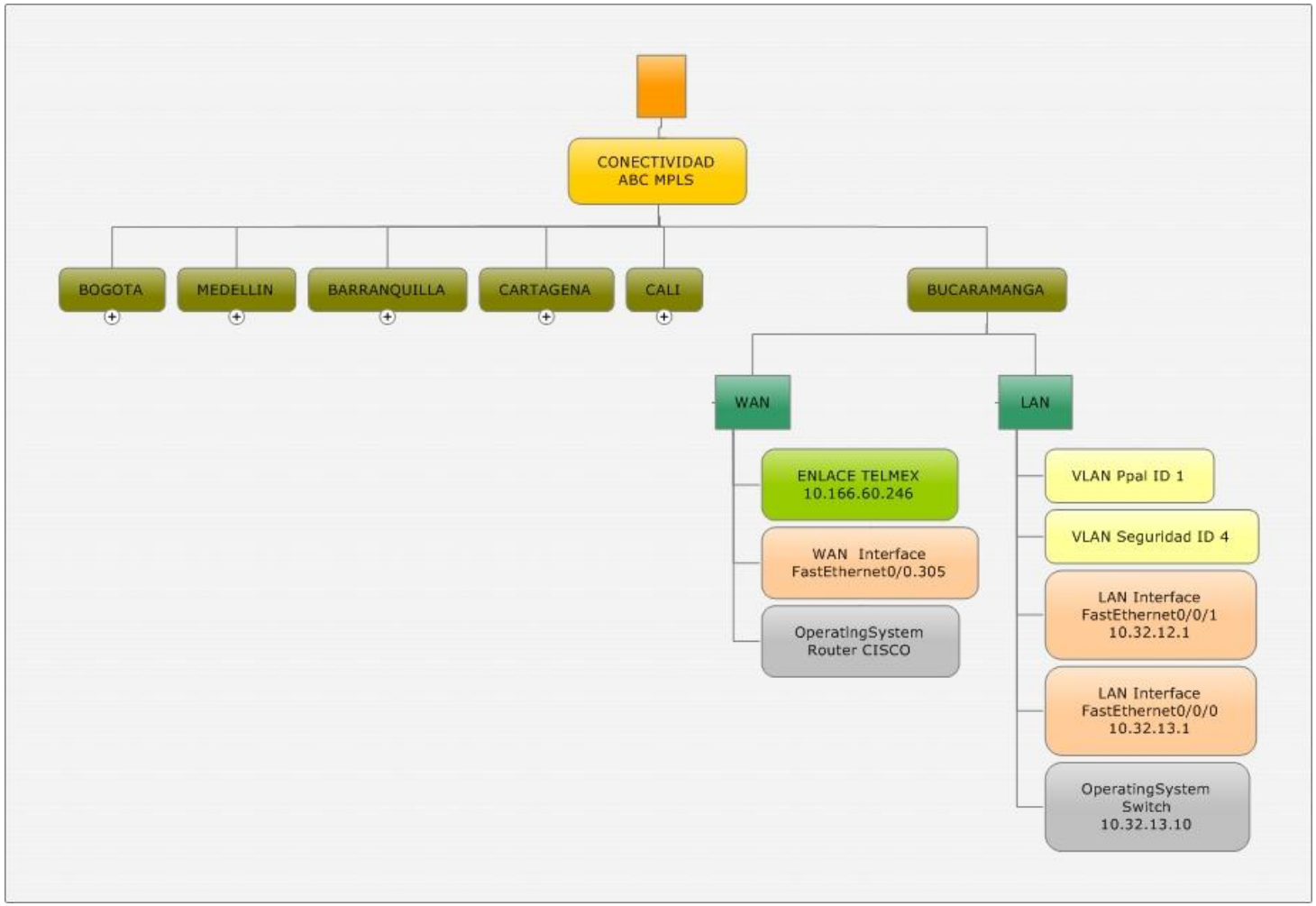


Figura 29. Diseño conectividad sede Bucaramanga



De acuerdo al estudio realizado teniendo en cuenta que el ancho de bando de consumo x equipo es de 20 Kbps. Según la Métrica se calcula No de Equipos x 20Kbps = X. Donde el 50 % de x es el valor mínimo requerido de Ancho de Banda.

Sedes Barranquilla, Medellín, Cali y Bucaramanga.

20 Kbps x 8 = 160 Kbps
160 Kbps / 2 = 80 kbps

Entonces 80 Kbps es el mínimo BA requerido para implementar la solución pero como se espera un crecimiento del 40% entonces 80Kbps * 40 % = 112 Kbps.

Según el requerimiento la solución debe soportar que todas las ciudades puedan tener sus sesiones simultaneas con el servidor principal y el de Backup en caso de una falla se subcontrata un Ancho de Banda de 1024 Kbps Dedicado en cada sede Tipo Cliente y para la Principal Cartagena y la de Backup Bogotá se subcontrata 2Mbps Dedicado para cada sede.

Para el Ancho de Banda subcontratado para esta solución de negocio se incluye el consumo de la red de PC de las sedes por esta razón los canales contratados exceden los cálculos obtenidos para la solución SCA.

Adicionalmente se contrata un canal dedicado de Internet de 2 Mbps con el proveedor UNE en la Ciudad de Cartagena para que el administrador del sistema pueda acceder al sistema a través de Internet, obteniendo así agilidad en los procesos de comunicación y posibilitando el envío de mensajes de control y administración por correo electrónico, envió de archivos, información en línea etc.

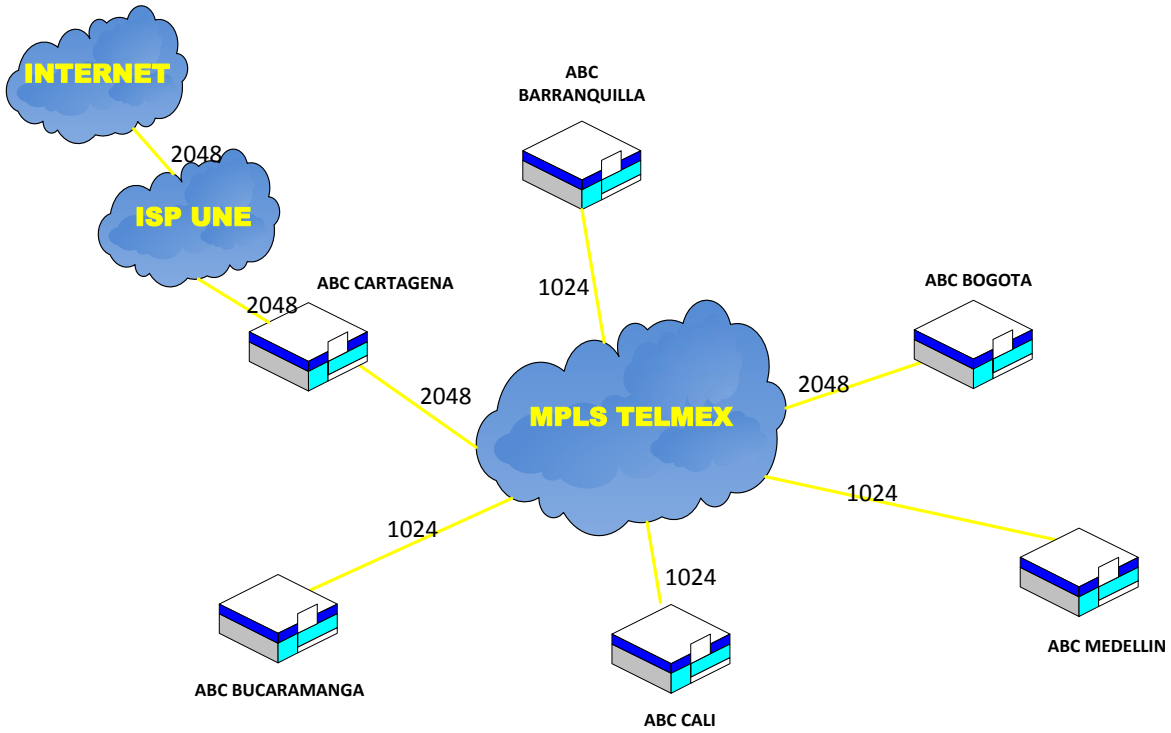
2.4.2 **Protocolo de Enrutamiento.** En la red de Telmex MPLS se maneja el protocolo de enrutamiento dinámico BGP (Border Gateway Protocol). Este protocolo es utilizado para facilitar la comunicación entre diferentes sistemas autónomos. Un sistema autónomo es una red o un grupo de redes que comparten una misma administración técnica y políticas comunes de routing.

Se comparten las diferentes tablas de enrutamiento, y el BGP decide por cual ruta se aprende un destino más fácilmente y rápido, esto se consigna en una forwarding table.

Procedimiento que utiliza BGP para conexión IP

1. Adquisición de Vecino: enrutadores que se encuentran en la misma subred, envía mensajes OPEN, el que recibe e mensaje envía un keepalive y de esta manera queda registrado en la tabla de enrutamiento
2. Detección de un vecino alcanzable: después de identificar un vecino, se mantiene la conexión por medio de keepalive
3. Detección de una red alcanzable: permite conocer que rutas puede alcanzar, envía paquetes UPDATE.

Figura 30. Esquema servicio Internet UNE-ABC



2.5 ANALISIS ECONOMICO DE LA SOLUCION

Implementación de puntos nuevos voz datos y ups para oficinas

	CANT.	VLR UNITARIO	TOTAL UNITARIO	
Suministro e instalación 1 metro de cable utp cat. 6				
Materiales				
Cable UTP	18000	$ 1.500	$ 27.000.000	
Amarre Plástico	400	$ 70	$ 28.000	
Mano de Obra y herramienta				
Mano de obra				
Incluye: tendido de cable UTP por bandeja o tubería	18000	$ 1.100	$ 19.800.000	
Herramienta/DIA	30	$ 300.000	$ 9.000.000	
Valor Total				**$ 55.828.000**
Suministro e instalación de punto de red o voz				
Materiales				
Jack plano Categoría 6	160	$ 14.700	$ 2.352.000	
Face Plate Sencillo	80	$ 9.000	$ 720.000	
Patch Cord 3 pies Cat 6	160	$ 19.000	$ 3.040.000	
Caja o troquel para salida	80	$ 10.000	$ 800.000	
Marquilla para punto	160	$ 2.000	$ 320.000	
Chaso plástico o tornillo perforante	160	$ 200	$ 32.000	
Mano de Obra y herramienta				
Mano de obra				
Incluye: Instalación de caja o troquel para salida, conexión en Jack y patch panel en rack de comunicaciones	80	$ 10.000	$ 800.000	
Herramienta	80	$ 5.000	$ 400.000	
Valor Total				**$ 8.464.000**
Suministro e instalación cto monofásico cable 12				
Materiales				
Cable No. 12 AWG	12000	$ 1.000	$ 12.000.000	
Amarre plástico 20cm	400	$ 70	$ 28.000	

Mano de Obra y herramienta							
Mano de obra							
Incluye: tendido de circuito monofásico en cable No 12 por bandeja o tubería	12000	$	1.500	$	18.000.000		
Herramienta/DIA	30	$	300.000	$	9.000.000		
Valor Total						**$**	**39.028.000**
Suministro e instalación punto eléctrico UPS							
Materiales							
Toma monofásica con tierra aislada de 15A	80	$	13.000	$	1.040.000		
Tapa naranja para toma monofásica	80	$	1.000	$	80.000		
Caja o troquel para salida	80	$	10.000	$	800.000		
Chaso plástico o tornillo perforante	1500	$	200	$	300.000		
Mano de Obra y herramienta							
Mano de obra							
Incluye: instalación de caja o troquel ,salida, conexión , verificación, marcación y pruebas de funcionamiento	80	$	21.000	$	1.680.000		
Herramienta	30	$	300.000	$	9.000.000		
Valor Total						**$**	**12.900.000**
TOTAL						**$**	**116.220.000**
AIU	**16%**					**$**	**18.595.200**
TOTAL PUNTOS						**$**	**134.815.200**

SERVIDORES

PowerEdge R610 — COP$ 13.150.365

Número de catálogo / Descripción
Procesador Primario:
Intel® Xeon® E5630 2.53Ghz, 12M Cache, Turbo, HT, 1066MHz Max Mem
Procesador Adicional:
Single Processor Only
Sistema Operativo:
Windows Server 2008 R2 SP1, Standard Edition, Includes 5 CALS
Memoria:

4GB Memory (2x2GB), 1333MHz Single Ranked LV RDIMMs for 1 Proc, Advanced ECC
Configuración Disco Duro:
RAID 0 for PERC 6/i or SAS 6/iR Controllers
Controlador primario:
PERC 6/i SAS RAID Controller, 2x4 Connectors, Internal, PCIe, 256MB Cache
Selección múltiple de Disco Duro:
500GB 7.2K RPM SATA 3Gbps 2.5-in HotPlug Hard Drive
PowerEdge R610:
Chassis for Up to Six 2.5-Inch Hard Drives
Envío:
PowerEdge R610 Shipping
Teclado, Mouse y otros Dispositivos relacionados:
Keyboard, Optical Mouse, USB, Black, Latin America, with 17 LCD Monitor
Mejoras de Características Opcionales para Puertos NIC Integrados.:
Embedded NICs are TOE Ready with iSCSI Offload Enabled
Discos Duro:
HD Multi-Select
Adaptador de Red:
2x Broadcom 5709 Dual Port 1GbE NIC w/TOE iSCSI, PCIe-4
Configuración de BIOS:
Power Saving BIOS Setting
Administración Integrada:
iDRAC6 Enterprise
Documentación del sistema y Manuales:
Electronic System Documentation and OpenManage DVD Kit
Fuente de Poder :
High Output Power Supply, Redundant, 717W
Disco Óptico Interno:
DVD+/-RW, SATA, Internal
Bezel:
Bezel
Configuración de Chassis :
Sliding Ready Rails With Cable Management Arm
Remote Advisory & Onsite Services:
No Installation Assessment
Client Access Licenses:
5-pack of Windows® Server 2008 Device CALs (Standard or Enterprise)
Cables de alimentación :
NEMA 5-15P to C14 Wall Plug, 125 Volt, 15 AMP, 10 Feet (3m), Power Cord

Cables de alimentación :
C13 to C14, PDU Style, 12 AMP, 13 Feet (4m), Power Cord
Proactive Maintenance Package:
Mantenimiento Proactivo, 1 evento por año, asistencia remota, 1 año.
Uninterruptible Power Supplies and Accessories:
UPS de Dell, rack, 1920 W, 2 U, 120 V, con cable de entrada 5-20P a C19 de 3 m
Garantía y Servicio de Soporte:
3 Años de ProSupport, con servicio telefónico 24/7 y con respuesta al día siguiente laborable de un técnico en sitio

SWITCH Y ACCESORIOS

Cant	Modelo	Descripción	Vlr Unitario COP$	Total sin IVA COP$	IVA COP$	Total con IVA COP$
7	WS-C2960S-24TS-L	24PORT 10/100/1000 ENET 4PORT FLEXSTACK STACKING SUP LAN BASE	3.045.000	21.315.000	3.410.400	24.725.400
2	GLC-SX-MM	GE SFP.LC Connector SX transceiver	508.200	1.016.400	162.624	1.179.024
2	C/A LC-LC	PatchCord LC-SC	31500	63.000	10.080	73.080
		TOTAL				**$ 25.977.504**

ENLACES MPLS

SERVICIO	BW	Instalación	Router	Mensualidad	Tiempo De Instalación
Enlace MPLS CARTAGENA	2048 K	$ 880.000	$ 186.399	$ 2.821.375	30
Enlace MPLS BARRANQUILLA - CARTAGENA	1024 K	$ 880.000	$ 186.399	$ 534.000	30
Enlace MPLS BOGOTA - CARTAGENA	2048 K	$ 880.000	$ 186.399	$ 2.821.375	30
Enlace MPLS BUCARAMANGA - CARTAGENA	1024 K	$ 880.000	$ 186.399	$ 534.000	30

Enlace MPLS CALI - CARTAGENA	1024 K	$ 880.000	$ 186.399	$ 534.000	30
Enlace MPLS MEDELLIN - CARTAGENA	1024 K	$ 880.000	$ 186.399	$ 534.000	30
Enlace MPLS INTERNET	2048 K	$ 880.000		$ 1.700.000	30
				$ 9.478.750	

EQUIPOS Y ACCESORIOS SISTEMA CONTROL DE ACCESO

	CANTIDAD	BOG	CTG	CALI	MED	BQUILLA	BMANGA	ÍTEM	REFERENCIA	MARCA	VR UNIT	VR TOTAL
1	2	1	1	0	0	0	0	Servidor	Dell	Dell	$ 13.150.365	$ 26.300.730
2	56	9	11	9	9	9	9	Controladoras	LNL-2200	Lenel	$ 7.200.000	$ 403.200.000
3	33	18	5	0	1	9	0	Modulo interface crecimiento	LNL 1300	Lenel	$ 3.500.000	$ 115.500.000
4	2	0	2	0	0	0	0	molinetes	Boonedam	Boonedam	$ 86.000.000	$ 172.000.000
5	141	36	23	18	19	27	18	Electroimanes	Zebra	Zebra	$ 430.000	$ 60.630.000
6	286	72	50	36	38	54	36	Lectoras de proximidad	RP40	HID	$ 363.000	$ 103.818.000
7	141	36	23	18	19	27	18	Contacto magnético	Zebra	Zebra	$ 12.000	$ 1.692.000
8	56	9	11	9	9	9	9	Módulo de entradas	LNL-1100	Lenel	$ 2.500.000	$ 140.000.000
9	56	9	11	9	9	9	9	Módulo de salidas	LNL-1200	Lenel	$ 2.700.000	$ 151.200.000
10	1	0	1	0	0	0	0	Software Control de acceso	Onguard Access	Lenel	$ 90.000.000	$ 90.000.000
	TOTAL											$ 1.264.340.730

TOTAL COSTO IMPLEMENTACION SISTEMA: COP $1.299.796.984

3. CONCLUSIONES

Una vez finalizado el diseño del Sistema de Control de Acceso se puede concluir que se mejoran las condiciones de seguridad y los índices de rendimiento de la operación en tanto que se facilitara el transito del personal sin generar riesgo para la operación, instalaciones o personas lo cual facilitara y además con un método de identificación costo efectivo.

Adicionalmente esta arquitectura de control de acceso único unificado aporta los siguientes valores estratégicos:

- Mejora la seguridad de las personas, bienes e información transmitiendo una mejora estratégica a la imagen de la compañía.
- Alinea las soluciones de seguridad con las necesidades del negocio Tecnológico (movilidad de empleados entre centros, reduce esperas.)
- Transforma el gasto de seguridad en inversión para el negocio (Cumple exigencias de clientes Ej. auditorias externas e internas.
- Rentabiliza los procesos de seguridad mejorando su eficacia, eficiencia e integración con el resto de procesos del negocio (PKI, Calidad ISO, etc.)
- La protección mediante Control de Accesos reduce los riesgos para la continuidad de negocio (CPDs, salas acceso restringido, etc.)
- Integra la seguridad con la imagen de cordialidad y bienvenida (Tarjeta corporativa unificada).

Ventajas:

- Capacidad de crecimiento más de 100.000 usuarios (empleados, contratistas, etc.)

- Incremento confiabilidad información del sistema de control de acceso.
- Consistencia de la información (gestión unificada en tiempo real).
- Gestión centralizada y única base de datos.
- Integración con el Sistema de Gestión de Personal.
- Reducción de gastos mantenimiento.

Debido a las características funcionales y operativas del sistema diseñado se pueden además de controlar los accesos a las diferentes áreas de las oficinas de la empresa ABC repartidas en el territorio nacional desde una misma plataforma, tendrá la posibilidad de integración con SAP, con plataformas de circuito cerrado de televisión, sistema contraincendios, sistemas de control de iluminación, sistemas de control de aire acondicionado, sistemas de automatización, etc. lo cual será una gran ventaja tanto operativa y finalmente un factor determinante en el uso eficiente de los recursos.

Tal como se estableció en el cuerpo del documento, una vez realizado el análisis costo beneficio de acuerdo a las condiciones de uso, necesidades de la operación, costos de adquisición e implementación, se decidió hacer uso de lectoras y tarjetas de proximidad para controlar el acceso a las instalaciones, con lo que además el personal de seguridad física puede realizar la identificación visual del tarjetahabiente y cotejar en caso de requerirse.

Finalmente gracias a la plataforma de interconexión seleccionada bajo tecnología MPLS tendremos una solución de conectividad que provee la robustez, capacidad y seguridad requerida para una herramienta tan importante para la empresa como lo es la plataforma de control de acceso. Adicionalmente tendremos los respaldos necesarios para poder dar continuidad al servicio en caso de fallas tanto en canales haciendo uso de backups.

4. BIBLIOGRAFÍA

- Norma técnica Colombiana NTC 4490, Referencias documentales para fuentes de información electrónicas
- Norma técnica Colombiana NTC 1486, Documentación. Presentación de tesis, trabajo de grado y otros trabajos de investigación.
- Norma técnica Colombiana NTC 5613, Referencias bibliográficas. Contenido, forma y estructura
- Software de control de acceso [En línea]. Disponible en internet: http://www.lenel.com/sites/default/files/Lenel_SW_Catalog_0607.pdf
- Tecnologías de identificación [En línea]. Disponible en internet: http://www.idenpla.com/ip/

  http://es.wikipedia.org/wiki/Identificaci%C3%B3n_de_personas
- Sistemas de control de acceso [En línea]. Disponible en internet: http://www.lenel.com