ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO DE UN SISTEMA DE GESTIÓN DE ACCESO PARA LA RED DE UN BANCO PREVINIENDO Y CONTROLANDO LOS RECURSOS Y SERVICIOS QUE ESTE PROPORCIONA"

INFORME DE MATERIA INTEGRADORA

Previa a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

BYRON ALEX ACEBO CORTEZ

CARLOS ALFREDO BUSTAMANTE MENDOZA

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTOS

En primera instancia agradeceremos a Dios, por haber permitido que llegáramos a esta meta que es un sueño tan anhelado.

A LA ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL, por darnos la oportunidad de estudiar y ser profesionales.

También hacemos extenso nuestros agradecimientos a los profesores, que durante toda la carrera profesional han aportado con un granito de arena a nuestra formación académica, y en especial a los profesores el Ing. Albert Espinal, Ing. Rayner Durango, Ing. Miguel Molina y al Ing. Ronald Criollo, por sus consejos, sus enseñanzas y por la amistad que nos han demostrado durante todo este tiempo.

De igual manera agradecer a nuestro profesor de la Materia Integradora, Ing. Robert Stalin Andrade Troya por su visión crítica en muchos aspectos, por su rectitud como docente, por sus sabios consejos, que nos formaron como personas e investigadores.

DEDICATORIA

Este proyecto va dedicado a nuestras familias, que siempre estuvieron apoyándonos incondicionalmente, guiándonos con sus sabios consejos para poder llegar a nuestra meta final.

TRIBUNAL DE EVALUACIÓN

Ing. Robert Andrade

PROFESOR EVALUADOR

Ing. Rayner Durango

PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual."

Byron Acebo Cortez

Carlos Bustamante Mendoza

RESUMEN

El Banco dispone de varias agencias a nivel nacional. El Centro de Datos de esta empresa se encuentra ubicado en el edificio de la Matriz. Todas las transacciones que realizan las agencias se replican en la Matriz, oficina principal en Guayaquil.

Las oficinas en la Matriz tienen problemas al conectarse a los recursos de la red, las estaciones de trabajo no cuentan con sistemas operativos actualizados, la falta de planes de contingencia para los recursos que tiene el Banco no permite llevar una continuidad estable del negocio.

También existe un alto riesgo de ataques a los recursos críticos del banco al no contar con un sistema que regule los accesos a los recursos en la red.

Todos estos aspectos generan que esta entidad tenga la necesidad de desarrollar un sistema de gestión que les facilite la disponibilidad de la información, el acceso a los recursos en la red y la seguridad de poder trabajar sin inconveniente alguno.

Una de las soluciones a implementarse es Active Directory Domain Services de la plataforma Microsoft, esto nos dará buenos resultados para organizar y mejorar el ingreso de los usuarios a los equipos que forman parte de la red, también habrá una notable mejoría del Banco para sus clientes.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1. PROBLEMA ACTUAL

1.1 Antecedentes

El 16 de Agosto del año 1984, el Banco inicia sus operaciones bancarias en la ciudad de Guayaquil, perla del Pacífico, como un Banco Comercial privado, con el objetivo de ayudar al desarrollo de las actividades productivas de la ciudad de Guayaquil. [12]

La iniciativa y el gran esfuerzo de un grupo de empresarios permitieron darle al Banco y a la ciudad de Guayaquil, una institución financiera, que luego de 32 años de trabajo prudente y constante, se ha convertido en un Banco de alcance nacional, contando a la fecha con 45 puntos de atención; entre Sucursales, Agencias y Ventanillas de extensión.

La Matriz del Banco está compuesta por 6 importantes áreas, ellas son el área de Auditoría, Administración, Sistemas, Seguridad Bancaria, Operaciones, Negocio.

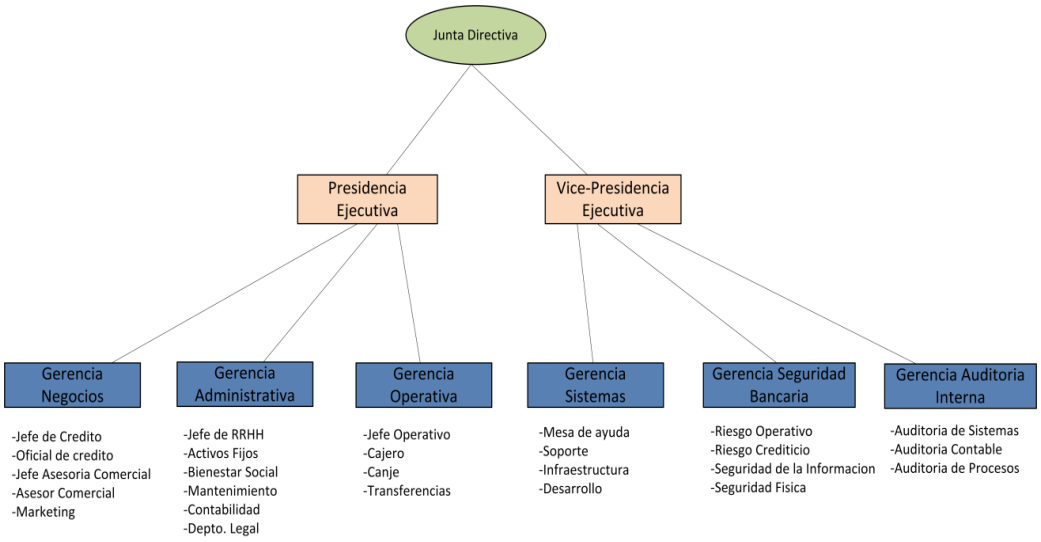


Figura 1.1 Organigrama del banco

El edificio principal de esta empresa es donde se encuentra el área administrativa, posee 6 pisos y un sótano, donde se ubica el Centro de Datos.

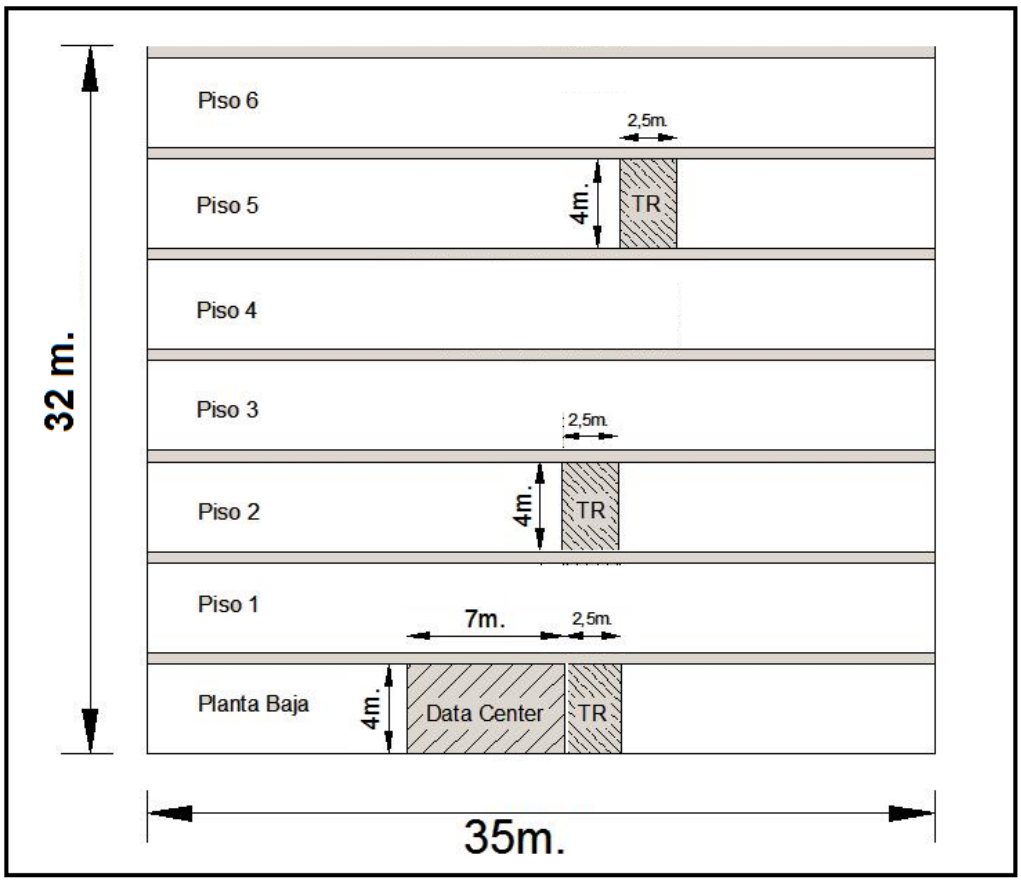


Figura 1.2 Diagrama de dimensión física del Banco

Como podemos ver en la imagen tenemos varios pisos que están dimensionados entre 35 m de largo y 4 metros de alto cada piso. En la planta baja tienen ubicado el Centro de Datos para el servicio correspondiente de Internet, recursos compartidos en la red y aplicaciones del Banco. En el piso 2 y 5 con una dimensión de 2.5metros de ancho y 4m de altura se encuentran los TR, Telecomunication Room, estos son los cuartos en donde se encuentran los equipos de comunicación, switches, que permiten a los

usuarios conectarse a la red del banco. En la siguiente figura mostraremos como la red de la Matriz del Banco se conecta con las demás oficinas por medio de enlaces WAN.

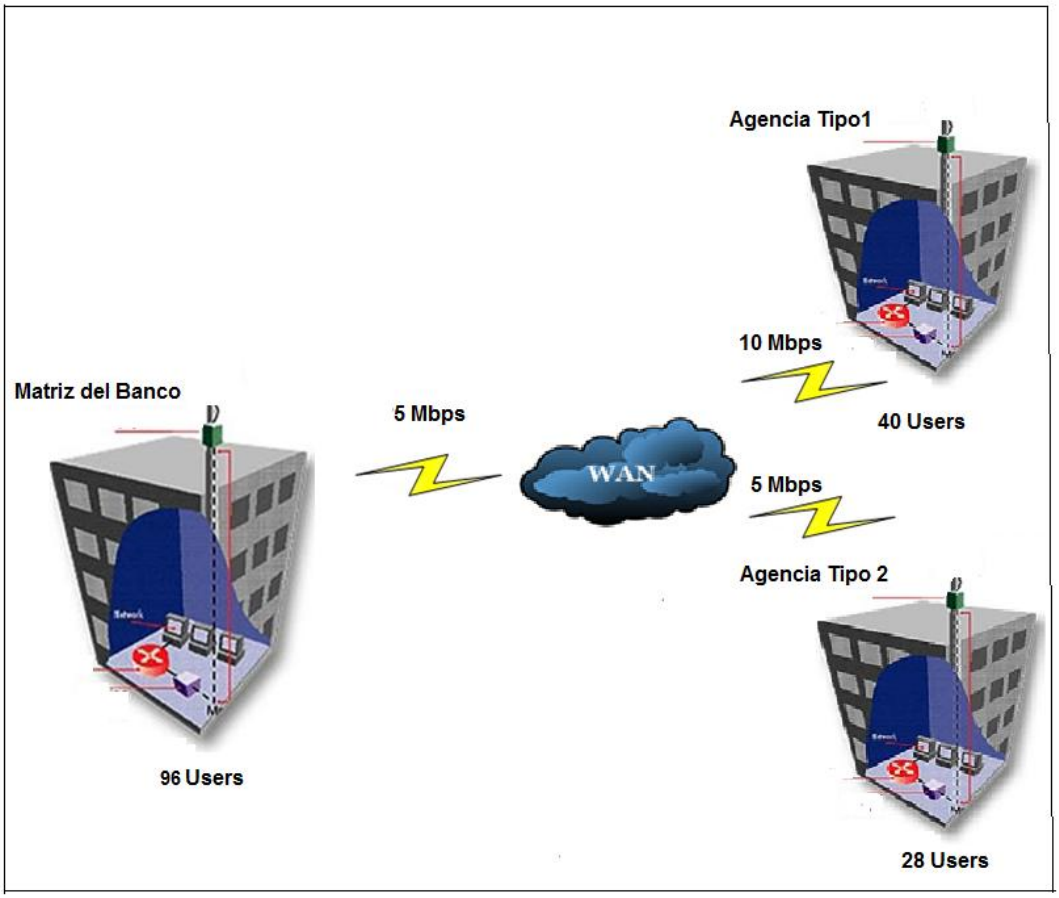


Figura 1.3 Red de Agencias

En la figura 1.3 mostramos como la red de la Matriz del Banco se conecta con las demás oficinas por medio de 1 enlace WAN por cada agencia, de acuerdo a la transaccionalidad de cada agencia constan de entre10 a 5 Mbps de ancho de banda. En la Matriz contamos con 96 usuarios, en la Agencia 1 contamos con 40 usuarios y en la Agencia 2 tenemos 28 usuarios.

En la tabla 1 se mostrará un cuadro informativo indicando la cantidad de ordenadores y características según su área:

Áreas	Cantidad de ordenadores	Sistema Operativo	Memoria RAM	Disco Duro
Sistemas	20	Windows 7	4 GB	320 GB
Negocio	10	Windows 7	2 GB	250 GB
Administración	20	Windows 7	3 GB	250 GB
Seguridad Bancaria	5	Windows 7	4 GB	320 GB
Auditoría	26	Windows 7	2 GB	250 GB
Operaciones	15	Windows 7	4 GB	320 GB
Total de Usuarios en Matriz	96			

Tabla 1: Cuadro informativo de ordenadores.

En la Matriz del Banco que está ubicada en Guayaquil, actualmente cuenta con 96 usuarios los cuales están divididos en las diferentes áreas. Todas las computadoras tienen Windows 7 como Sistema Operativo, cada máquina cuenta con diferente capacidad de memoria RAM y disco duros.

Función	Cantidad	Sistema Operativo	Memoria RAM	Disco Duro
Servidor de Aplicaciones	15	Windows Server 2003	8 GB	500 GB
Servidor de Correo	2	Windows Server 2003	16 GB	750 GB
Servidor de Base de Datos	5	Windows Server 2003	16 GB	750 GB
File Server	2	Windows Server 2003	8 GB	1 TB
Router – Enlace de Agencias	1	Cisco IOS	128 MB	64 MB
Router – Enlace de Internet	1	Cisco IOS	128 MB	64MB
Switch Core	1	ZyXel IOS	64 MB	32MB
Switch de acceso a usuarios	5	ZyXel IOS	64 MB	32 MB
Switch de acceso a Servidores	2	ZyXel IOS	64 MB	32 MB
Total de equipos	47			

Tabla 2: Informativo de servidores

En la tabla 2 se detalla las características de los servidores que se encuentran en el Centro de Datos como servidores de Base Datos, de Aplicaciones, de Correo y Web. Todos los Servidores cuentan con software sin licenciamiento, tienen capacidad de memoria de entre 8 a 16 Gigabits y discos duros de entre 500 a 750 gigabits de almacenamiento.

También cuentan con routers y Switchs cisco, estos dispositivos le dan la comunicación a la red dentro y fuera del Banco.

La Matriz del Banco cuenta con 5 MB de ancho de banda para conexión con sus agencias, también constan con 75 puntos de red en el edificio, los mismos que conectan a las aplicaciones empresariales.

Aproximadamente 350 usuarios diariamente se conectan a la red del Banco ya sean clientes o empleados de la entidad Bancaria.

1.2 Problemas.

Actualmente la red no se encuentra segmentada por servicios, existe una única red para todos los ambientes que tiene el Banco, estos ambientes corresponden a los servidores de producción, servidores de desarrollo y la red de usuarios:

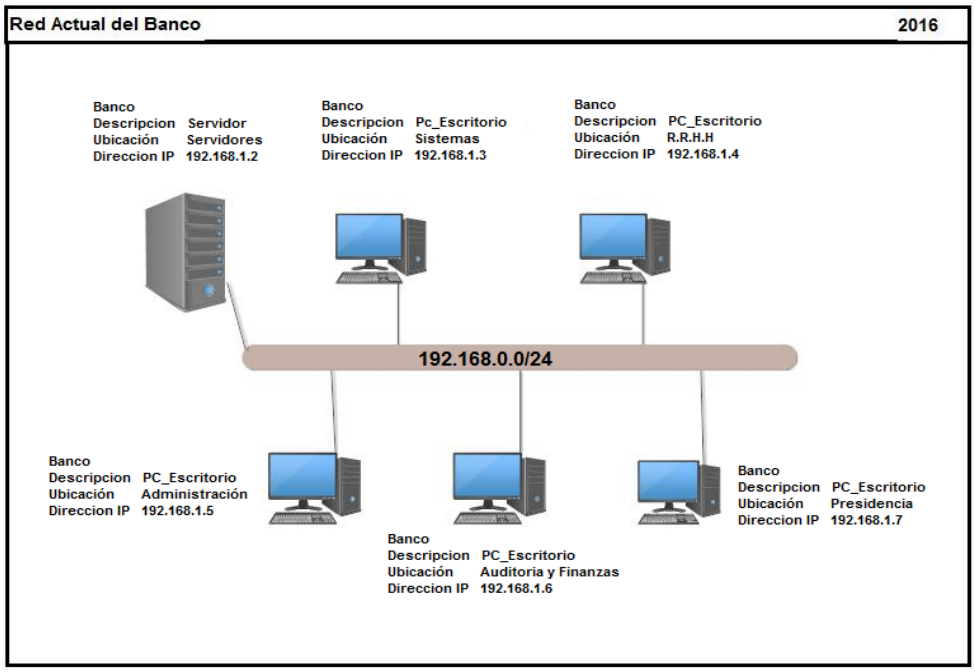


Figura 1.4: Diseño de la red actual del Banco

En la figura 1.4 se puede apreciar que un servidor se encuentra en la misma VLAN de usuarios sin ningún tipo de filtro o protección, esto implica que los servicios en la red no se encuentran diferenciados.

Los usuarios reportan constantemente que se pierde la conexión con el correo electrónico, navegación por internet, carpetas compartidas. El Banco posee equipos de red obsoletos con año de fabricación de 2003 y 2004.

La disponibilidad de la red es de 94.56% debido a fallas con los enlaces WAN de las agencias, cortes del suministro de energía eléctrica y problemas con los switches de acceso a los usuarios. A continuación se detalla las pérdidas de conexión con las Agencias.

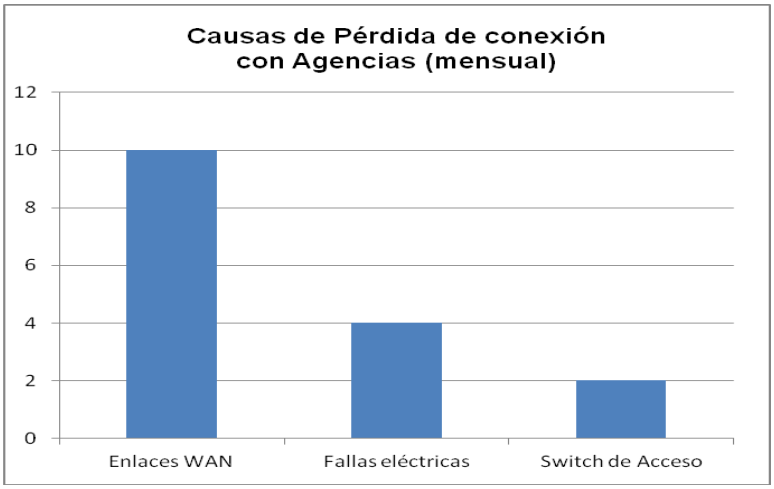


Figura 1.5: pérdida de conexión con Agencias

En el cuadro podemos observar que la mayoria de las causas por las que se pierde conexión con las Agencias es por fallas en los enlaces WAN del proveedor de servicios, seguido de las fallas electricas y errores en los switches de acceso a los usuarios.

Agencias	Disponibilidad
Agencia Quevedo	74.63%
Agencia Autobanco 10 de Agosto	85.20%
Agencia Arenillas	86.40%
Agencias Balsas	89.35%
Agencia Chacras	90.51%
Agencia Gye Sur	91.13%
Agencia Centro de Servicio Santa Rosa	91.27%
Agencia Santa Rosa	92.31%
Agencia Hipermarket Norte	92.37%
Agencia Centro de Servicio Cuenca	92.68%
Agencia Valencia	92.75%
Agencia Puerto Inca	92.76%
Agencia Ponce Enríquez	92.83%
Agencia UTM	92.83%
Agencia UESS	92.84%
Agencia Parque California	93.85%
Agencia Centro de Servicio Pasaje	93.86%

Agencia Pasaje	93.87%
Agencia Manta	94.90%
Agencia Cuenca	94.91%
Agencia Milagro	94.92%
Agencia Eco mundo	94.93%
Agencia Híper Albán Borja	94.94%
Agencia Atahualpa	94.94%
Agencia El Triunfo	94.95%
Agencia Remigio Crespo	94.96%
Agencia Centro de Servicio Matriz	94.96%
Agencia Puerto Bolívar	94.97%
Agencia Guabo	95.97%
Agencia Zaruma	95.97%
Agencia Quito Sur	95.98%
Agencia Loja	96.98%
Agencia Municipio de Machala	96.98%
Agencia Brisas	96.98%
Agencia Ambato	96.98%
Ag. Sitio Alterno	97.98%
Agencia Rio Plaza	97.98%
Agencia Bahía	97.98%
Agencia Huaquillas	97.98%
Agencia Matriz Machala	98.98%
Agencia Santo Domingo	98.99%
Agencia Ambato Sur	98.99%
Agencia Quito Centro	98.99%
Agencia Mercado 25 de Junio	99.99%
Agencia Quito	99.99%
Agencia Rio Zamora	99.99%
Agencia Portobello	99.99%
Promedio	94.56%

Tabla 3: Detalle de Caídas de enlace de Agencias Semestral

En esta tabla se detalla la disponibilidad de cada una de las agencias y su promedio en el primer semestre el cual es de 94.56%.

El Banco no cuenta con un control para el acceso a los recursos en la red, como Base Datos, File Servers, DVRs y Cámaras IP; existe el riesgo de un acceso no autorizado hacia equipos críticos y la información sensible de la empresa se vea comprometida.

Los equipos de red tienen usuarios y claves por defecto.

La red de cajeros se encuentra configurada bajo una VPN IPSec con algoritmo de autenticación en 128 bits, el cual es vulnerable, exponiendo al riesgo información de tarjetas de débito y credenciales de los usuarios..

Los firewalls no actualizan sus módulos de IPS ni sus bases de antivirus, esto implica que de existir algún tipo de ataque no pueda ser detectado ni bloqueado. Tampoco existe un sistema de bloqueo a un equipo ajeno a la red de la entidad.

Existe además un uso indebido del correo electrónico al utilizarlo para uso personal y no del Banco, uso de los recursos computacionales sin la debida autorización, software instalado sin el debido licenciamiento.

No se cuenta con un diagrama de la infraestructura de la red actual del banco.

El Centro de Datos no cuenta con los puntos de datos debidamente etiquetados y certificados.

El Centro de Datos no cumple con una especificación de la norma ANSI-TIA 942, la cual determina la ubicación correcta de los gabinetes.

La entidad bancaria no realiza respaldos de seguridad a las aplicaciones que tienen los datos de los usuarios.

No existe la debida documentación para realizar los soportes técnicos, esto generará una pérdida de tiempo y molestias al usuario cuando surja algún problema de acceso o servicio en la red.

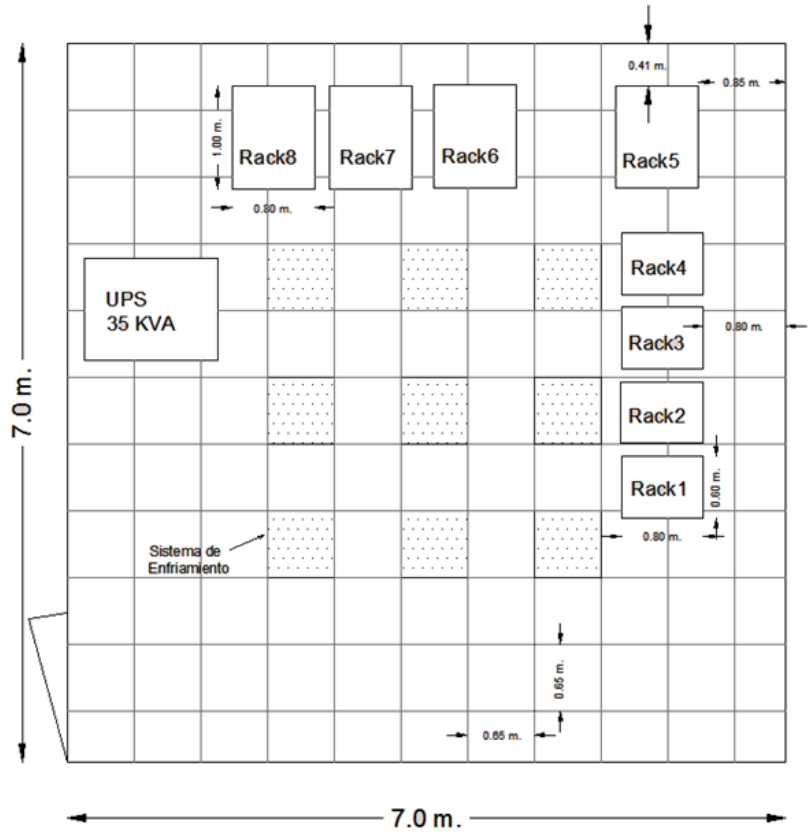


Figura 1.6: Diagrama del Centro de Datos vista aérea

Como podemos apreciar en la figura 1.6 los racks se encuentran a muy poca distancia, lo que genera desorden en el cableado de datos y cableado eléctrico y tampoco se puede aprovechar al máximo el sistema de refrigeración.

1.3 Análisis de las causas posibles.

En esta entidad existe la necesidad de desarrollar un sistema de gestión que facilite la disponibilidad de la información en la red, de esta forma mejorar la eficiencia del servicio que presta el banco a sus clientes.

El estudio que se realizó se orientará en un plan de seguridad informática, rediseño de la red, protección de recursos y servicios, esto nos permitirá satisfacer las necesidades de comunicación de datos a través de la red en las diferentes sucursales.

Problemas	Causas
a. No están segmentados los servicios.	a.1) No se realizó ninguna restructuración de la red en más de 10 años.
b. Estaciones de trabajo y servidores con sistema operativos desactualizados.	b.1) No existe ningún procedimiento que establezca las directrices bajo las cuales los equipos deban ser instalados.
c. Niveles de seguridad bajos en navegación.	c.1) Equipos se seguridad (firewalls) con configuraciones básicas.
d. No existe backup de la información crítica.	d.1) En caso de dañarse algún servidor no existirá un respaldo de la información vital para las labores diarias de los usuarios.
e. Centro de Datos sin etiquetado.	e.1) Riesgo de alguna falla en la conexión.
f. Falta de información del área de Sistemas.	f.1) No se ha realizado un inventario de equipos ni diagramas de red.
g. Recepción de correos basura.	g.1) Uso indebido del correo electrónico.
h. Equipos de red con usuario y clave por defecto.	h.1) No hay una política de credenciales robustas.

Tabla 4: Cuadro de resumen de problemas.

CAPÍTULO 2

2. OBJETIVOS

2.1 Objetivos Generales

Diseñar un sistema de gestión de acceso a la red del banco para prevenir y controlar los recursos y servicios que se proporcionan a los usuarios internos de la entidad bancaria.

2.2 Objetivo Específico

- ✓ Estructurar un plan de seguridad informática para mitigar los riesgos detectados.
- ✓ Diseñar una nueva infraestructura de red.
- ✓ Mejorar el tiempo de disponibilidad de la red.

2.3 Alcance del Problema

El alcance va a cubrir un sistema de gestión de acceso a la red del banco para prevenir y controlar los recursos y servicios que proporciona la Matriz del Banco.

2.4 Justificación.

La cantidad de usuarios que acceden a la red del banco internamente genera un tráfico muy significativo, debido a que acceden a los diversos servicios que brinda el Banco. Se estima que 350 usuarios internos se conectan a los recursos que presta el banco cada día.

El diseño actual de la red y los niveles de seguridad implementados en el banco no están acorde a las normas y estándares mínimos para un desempeño óptimo. La Superintendencia de Bancos y Compañías es la institución pública que rige las directrices bajo las cuales deben acogerse todas las instituciones financieras, las cuales inciden en los cambios tecnológicos que se deben realizar en el Banco.

Con los constantes problemas de conectividad que tiene la institución y la falta de un control sobre los recursos y servicios que el Banco proporciona, se llega a la conclusión que los objetivos fundamentales sean proponer un proyecto que mitigue los riesgos existentes y beneficie la entidad Bancaria y a sus clientes.

2.5 Metodología del Proyecto.

Recolección de Datos.

Técnicas

En la recolección de información se necesitará utilizar varios tipos de técnicas, herramientas que nos ayuden a encontrar información que nos será útil para la ejecución del proyecto.

Instrumentos

Tendremos que tener una visualización muy eficaz para la adquisición de información del Banco, esto conlleva a detectar rasgos y elementos que estén siendo utilizados. [10]

2.6 Procedimiento de la Investigación.

Para realizar la investigación se llevó a cabo varias fases que nos permitieron diseñar el objetivo principal del Banco.

- ✓ Determinaremos el estado actual de la red del Banco.
- ✓ Identificaremos los requerimientos del Banco para los sistemas de información.
- ✓ Analizaremos los sistemas de red.
- ✓ Definiremos las estrategias y planes de despliegue de solución para la red del Banco.

2.6.1 Determinaremos el estado actual de la red del Banco.

Se determina el estado actual del Sistema de Red, esto será para poder analizar posteriormente la efectividad el soporte técnico del Banco.

La determinación del estado actual del sistema deberá realizarse respecto a sus tres aspectos básicos que son:

- ✓ El estado actual de la Infraestructura de la red.
- ✓ El estado actual de los aplicativos del banco.
- ✓ El estado actual del Banco y sus procesos.

2.6.2 Identificar los requisitos del Banco para los sistemas de información.

La segunda fase del Diseño de la red, una vez identificado el contexto y la estrategia del Banco, es determinar cuáles son los requerimientos del Banco que necesitan para contribuir con el Diseño de la red.

Para nosotros poder identificar los requisitos de una manera concisa y estratégica, debemos revisar las necesidades del Banco desde varios niveles de análisis.

Debemos tener en cuenta los siguientes modelos de análisis que son: las Debilidades, las Amenazas, las Fortalezas y las Oportunidades.

2.6.3 Análisis de los sistemas de red.

Ya sabiendo cuales son los requerimientos del Banco y determinando el estado actual de estos se deberá realizar un análisis para identificar cuáles son los puntos fuertes a mantener y las debilidades a mejorar.

Esto conlleva a realizar un análisis de los siguientes niveles:

Análisis estratégico del sistema de red.

Evaluación de coste/beneficio de las aplicaciones o servicios adquiridos para el Banco.

El análisis identificará que acciones debemos tomar para mejorar la red del Banco.

Podemos realizar un análisis de las partes afectadas en la red para poder mejorar la productividad, mitigar riesgos posibles de robos de información en la red, nuevos ingresos, recursos necesarios para su implementación tanto humana como material.

2.6.4 Definir las estrategias y planes de despliegue de solución para la red del Banco.

La fase final del Diseño será la Planificación estratégica del diseño de un sistema de gestión de acceso a la red de un banco previniendo y controlando los recursos y servicios que este proporciona.

En base a las necesidades estratégicas, se identificarán los objetivos estratégicos y bajo a esto se agrupará las acciones correctivas.

CAPÍTULO 3

3. PLAN DE SEGURIDAD INFORMATICA PARA EL BANCO.

A continuación se detallará el proceso que se llevará a cabo en el plan de seguridad informática, aplicable al Banco, lo cual nos permitirá mitigar y minimizar los eventos causantes de los daños que puedan ocurrir en la entidad

Este plan será realizado en varias actividades las cuales se agruparan y cada una tendrá un objetivo, un tiempo de ejecución para ser cubiertas en cada actividad identificada y tendrán sus etapas de implementación.

Las actividades a realizarse para el Banco serán:

- ✓ Inventario de todos los accesos a los sistemas
- ✓ La seguridad de la red y las comunicaciones.
- ✓ Adaptación de contratos con los proveedores.
- ✓ Verificación y adaptación de los sistemas del Banco.
- ✓ Estandarización de la configuración del software
- ✓ Revisión y adaptación de procedimientos complementarios.

En cada una de las actividades a realizarse se ha elaborado una breve descripción de las tareas, con un tiempo de duración. [16]

3.1 Inventario de todos los accesos a los sistemas

Responsable: Jefe de Soporte de Servicios Informáticos

Tiempo de estimación a realizarse (12 semanas).

Objetivo: Al necesitar un adecuado control sobre el acceso de los usuarios a los sistemas del Banco, debemos realizar un inventario de todos los accesos que poseen ellos sobre cada uno de los sistemas. El inventario deberá ser actualizado al ser modificado el perfil de acceso de algún usuario. Se deberá

realizar revisiones periódicas de los accesos que se le otorgará en los sistemas del Banco.

Etapas

- ✓ Se elaborará un inventario de todas las aplicaciones y sistemas del Banco.
- ✓ Se elaborará un inventario de todos los perfiles de acceso al Sistema.
- ✓ Se verificará los perfiles definidos en los sistemas para cada usuario.
- ✓ Se procederá a una revisión y aprobación de los accesos a los usuarios por parte de las gerencias.
- ✓ Se realizará un mantenimiento periódico de los inventarios.

3.2 La seguridad de la red y las comunicaciones

Responsable: Jefe de Soporte de Servicios Informáticos

Tiempo de estimación a realizarse (17 a 21 semanas).

Objetivo: Se evitará la manipulación de los equipos de comunicación por personal no autorizado y se garantizará que la configuración que poseen los equipos en el Centro de Datos brinde la mayor seguridad y eficiencia a las comunicaciones.

Etapas:

3.2.1 Adaptación del sistema de comunicaciones a políticas de seguridad.

Tiempo de estimación a realizarse (4 a 5 semanas).

La elaboración de un inventario de equipos de comunicaciones (Routers, switches, firewalls, etc.)

La elaboración de estándares de Configuración para los equipos de comunicación estos será basada en las políticas de seguridad.

3.2.2 Adaptación a la arquitectura de red propuesta

Tiempo de estimación a realizarse (7 a 8 semanas)

- ✓ Creación de la extranet para controlar mediante un firewall la comunicación entre la red del Banco y redes externas como Banred y routers, esto evitará la actividad no autorizada desde dichas redes hacia los equipos de la red del Banco.

- ✓ Se implementará una red Desmilitarizada DMZ para evitar el ingreso de conexiones desde Internet hacia la red interna de datos. Dentro de la DMZ se implementará un sistema de inspección de contenido con el propósito de monitorear la información que es transmitida vía correo electrónico entre el Banco e Internet.
- ✓ El sistema de inspección funcionará de la siguiente manera:
  a. Recibirá todos los correos enviados desde Internet.
  b. Revisará su contenido.
  c. Si el contenido esta óptimo será enviado al servidor Exchange, este se encargará de entregar a su destinatario final.
  d. Al salir un correo de parte del usuario dentro del Banco el servidor Exchange enviará el correo al servidor de inspección de contenido, quien revisará el contenido del mensaje, para transmitirlo a través de Internet a su destino final.
- ✓ Se implementará un sistema de antivirus para los servicios de Internet (SMTP, FTP, HTTP). Al Implementar un Gateway Antivirus de servicios de Internet, estos pasarán por las comunicaciones establecidas entre la red interna del Banco e Internet.
  Tiempo de estimación a realizarse (2 semanas).
- ✓ Se implementará un sistema que sea de Alta Disponibilidad de firewalls en las conexiones donde fluye información crítica y se requiera una alta disponibilidad de las comunicaciones. Para esto instalaremos dos firewalls. Tiempo de estimación a realizarse (3 semanas).
- ✓ Implementaremos un sistemas que se encargue de monitorear y detectar los intentos de intrusión o ataques desde redes externas hacia la red de datos del Banco. También se implementará un sistema en la red interna del Banco donde se ubican los servidores críticos de tal manera que detecte intentos de intrusión o ataques realizados desde la red interna del Banco hacia los servidores.
  Tiempo de estimación a realizarse (3 semanas).

3.2.3 Complementario

Se realizará una evaluación de seguridad de la red inalámbrica y aplicaciones de controles de ser necesarios.

Se verificará la configuración de servidor Proxy, firewalls y servidor de correo. Tiempo de estimación a realizarse (3 a 4 semanas).

3.3 Adaptación de contratos con los proveedores

Responsable: Jefe de Soporte de Servicios Informáticos

Tiempo de estimación a realizarse (15 semanas).

Objetivo: Para asegurar el cumplimiento de las políticas de seguridad del Banco con respecto al servicio brindado por parte de los proveedores de Internet, se realizará una revisión de los mismos, su grado de cumplimiento respecto a las políticas de seguridad definidas y si es necesario de modificar los contratos para el cumplimiento de las políticas de seguridad del Banco.

Etapas

Se elaborarán clausulas estandarizadas referentes a la seguridad de información, estas serán incluidas en los contratos con los proveedores.

Se realizará un inventario de los contratos que existen con proveedores de Internet del Banco.

Se realizará una revisión de contratos y se analizará el grado de cumplimiento de la política de seguridad.

3.4 Verificación y adaptación de los sistemas del banco

Responsable: Jefe de Soporte de Servicios Informáticos

Tiempo de estimación a realizarse (18 semanas).

Objetivo: Verificar el cumplimiento de las políticas de seguridad en los sistemas del Banco y adaptarlos en caso de que no estén cumpliendo con las políticas.

Etapas

La adaptación del sistema a la política de seguridad ya sea en diseño, desarrollo, pruebas, actualización y documentación.

Se realizará controles de estandarización.

Control de contraseñas a los sistemas.

Control de enlace de Datos en la red.

3.5 Estandarización y configuración de los softwares.

Responsable: Jefe de Soporte de Servicios Informáticos

Tiempo de estimación a realizarse (12 semanas).

Objetivo. Será proteger adecuadamente la información existente en los servidores y ordenadores, se deberá realizar una adecuada configuración de los parámetros de seguridad de los softwares que soportan las aplicaciones del Banco**.**

Etapas

Actualizaciones de los Sistemas Operativos de todas las computadoras con su debido licenciamiento.

Se elaborará un inventario de los Sistemas Operativos de Servidores y computadoras del Banco.

Se elaborará un inventario de base datos existentes.

Se evaluarán los sistemas operativos existentes.

Se evaluarán las adaptaciones de los softwares a la política de seguridad.

3.6 Revisión y adaptación de procedimientos complementarios.

Responsable: Jefe de Soporte de Servicios Informáticos

Tiempo de estimación a realizarse (9 semanas).

Objetivo. La adaptación de los procedimientos y controles complementarios del Banco**.**

Etapa Se procederá a la revisión y adaptación de los estándares para el desarrollo de la entidad.

Se elaborarán procedimientos de monitoreo en la red, se verificará periódicamente las carpetas compartidas de la red, se generarán copias de respaldo de información de los usuarios, aplicaciones y servidores.

Se elaborarán procedimientos de monitoreo y reportes sobre la administración de los sistemas y herramientas de seguridad, entre ellas son: antivirus, servidores de seguridad de contenido, servidor proxy, firewall, sistemas de detección de intrusos, servidor de correo, servidor de dominio.

Se establecerá controles para la información que es transmitida a clientes y proveedores. [2]

3.7 Cronograma de implementación del plan de seguridad

Las actividades que se mencionaron deberán ser lideradas por el área de seguridad informática, se presentará un cronograma sugerido de la realización de las actividades al presente plan de seguridad.

Actividades	**Mes1**	**Mes2**	**Mes 3**	**Mes 4**	**Mes 5**	**Mes 6**	**Mes 7**	**Mes 8**	**Mes 9**	**Mes 10**	**Mes 11**	**Mes 12**
Inventario de todos los accesos a los sistemas.												
La seguridad de la red y las comunicaciones.												
Adaptación de contratos con los proveedores.												
Verificación y adaptación de los sistemas del Banco.												
Estandarización de la configuración del software												
Revisión y adaptación de procedimientos complementarios												

Tabla 5: Cronograma del Plan de Seguridad.

La duración de las actividades estará sujeta a variaciones dependiendo de la situación existente y el análisis realizado previo a cada una de las actividades.

3.8 Propuesta del diseño de red

3.8.1 Diseño físico de la red bancaria

Como parte de la solución que se propondrá para cumplir con uno de los objetivos específicos, el cual será realizar un nuevo diseño de red el cual se ajustará a los requerimientos solicitados, también se propone una reubicación del [13] Centro de Datos como se muestra a continuación:

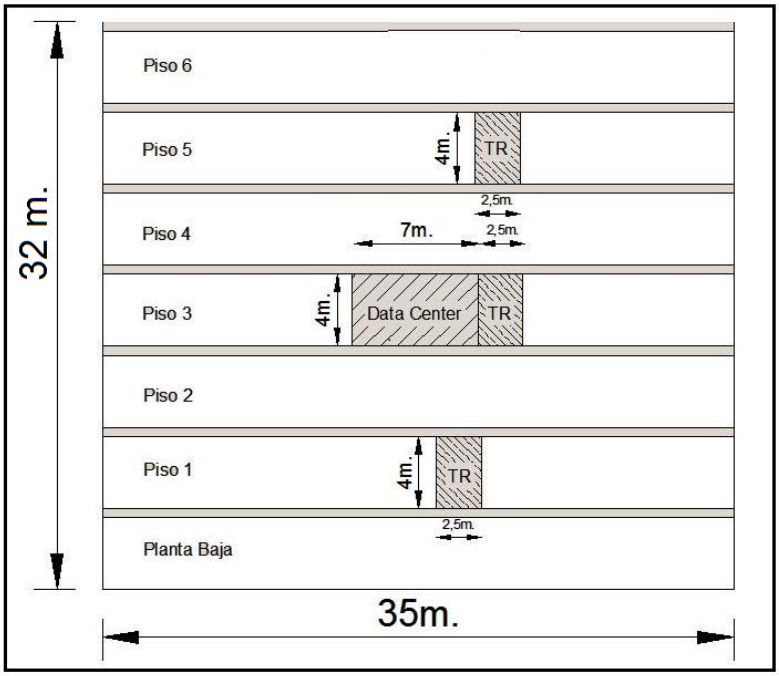


Figura 3.1: Propuesta de reubicación del Centro de Datos

En la imagen podemos observar que se propone reubicar el Centro de Datos en el tercer piso y los TR's en los pisos 1, 3 y 5. Esto nos ayudará a que no sea de un fácil acceso a personal no autorizado y se podrá tener un mejor alcance para todo el edificio.

Diseño de la red:

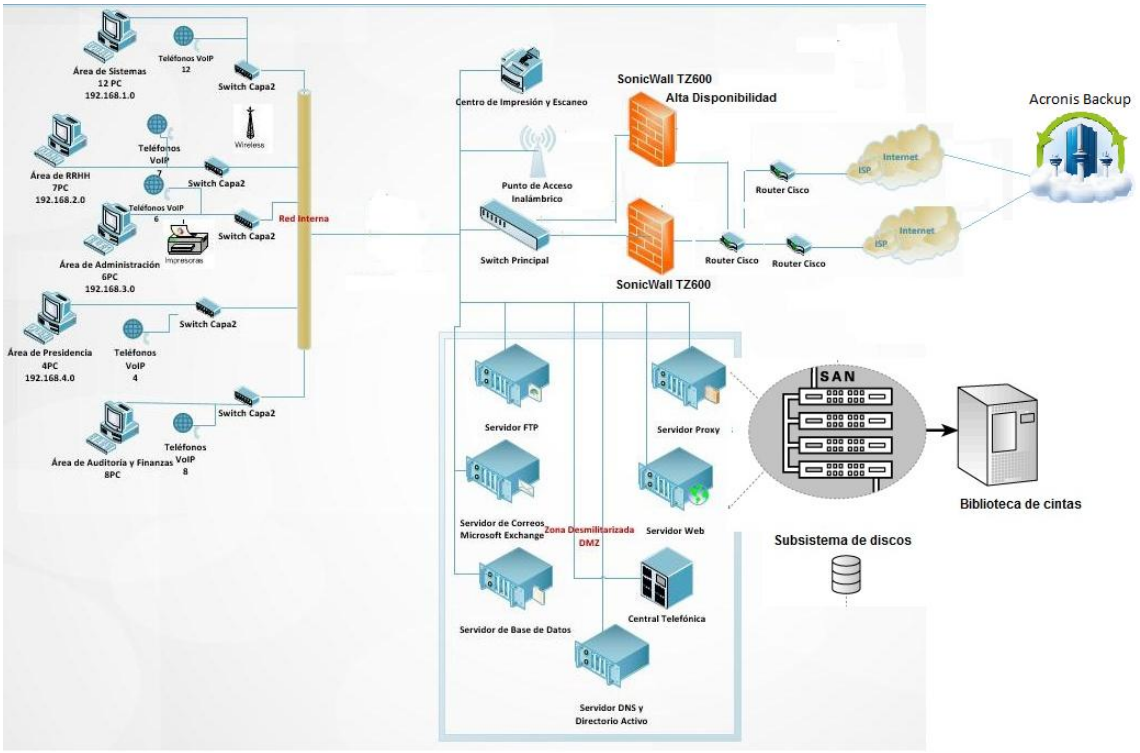


Figura 3.2: Diseño de red propuesta

Con el nuevo diseño de red mejorado se adquirirán dos proveedores de Internet, esto nos ayudará en gran parte a solucionar el problema de Intermitencia a navegar por web; se instalarán dos equipos de firewalls, para poder lograr tener una alta disponibilidad en caso de que fallara un dispositivo el otro entrara a funcionar como principal; también se instalará un Switchs capa 3 que permitirá crear Vlans, Routing para tener un mejor tráfico en la red.

Entre la red interna y la zona de internet se propone diseñar una zona desmilitarizada. Dicha zona impedirá que los intrusos penetren a la red interna y puedan causar daños. También conocida como DMZ se podrá acceder desde la red interna y desde internet. De aquí la importancia de definir la existencia de esta zona. [1]

En cada uno de los pisos existen diferentes áreas en la cual se reestructura la red de tal manera que existirá estabilidad, escalabilidad y seguridad.

El piso donde se encuentran el Centro de Datos, su interconexión es mediante fibra óptica con los demás dispositivos.

En cada uno de los departamentos tendrá un Switch y estos se conectarán a los ordenadores.

La conexión a Internet estará diseñada por los router de nuestros 2 nuevos proveedores de Internet estos se conectarán con los firewalls que están en alta disponibilidad, si en caso de que nuestro operador principal falle en la conexión entrara el otro a funcionar como Backup. Lo mismo será en caso de que nuestro firewall principal deje de funcionar por alguna razón, nuestro segundo firewall entrara a ser el principal

A continuación tendremos la figura de cómo estará el diseño de la red Wan del Banco.

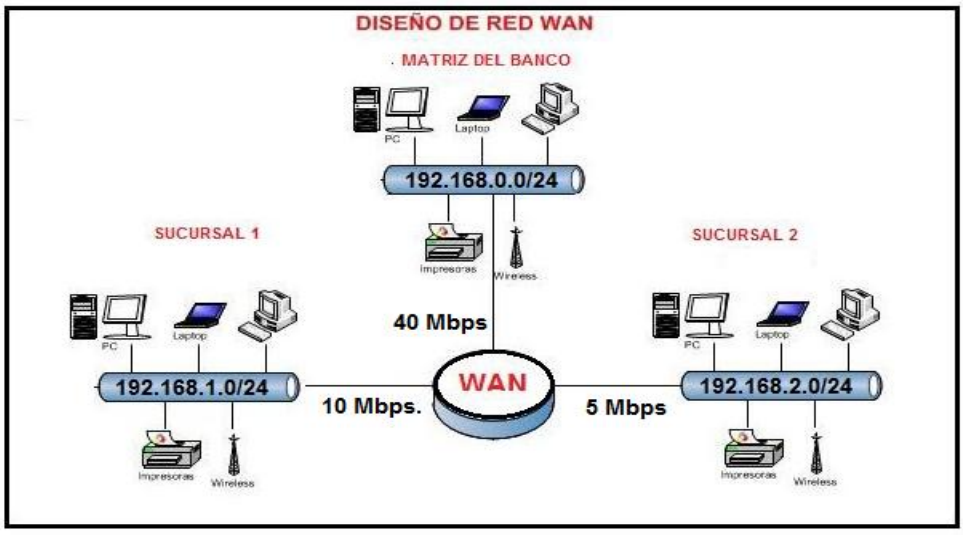


Figura 3.3: Propuesta de diseño WAN

Como se muestra en la imagen quedará el diseño de la red Wan del Banco, se aumentará el ancho de banda de la Matriz a 40 Mbps para la conexión con las Agencias.

A continuación tendremos la imagen de cómo estará el diseño de la red LAN del Banco.

Los ordenadores serán actualizados, siempre y cuando cumplan con las normas de licenciamiento y configuraciones para recibir actualizaciones ya sean de sistemas operativos o antivirus.

Función	Cantidad de ordenadores	Sistema Operativo	Memoria RAM	Disco Duro
Servidor FTP	1	Windows Server 2014	16 GB	1TB
Servidor Proxy	1	Windows Server 2014	16 GB	1TB
Servidor de Correo	2	Microsoft Exchange 2016	32 GB	1TB
Servidor Web	7	Windows Server 2014	32 GB	1TB
Servidor de Base de Datos	5	Microsoft SQL Server 2014	32 GB	1TB
Servidor DNS	2	Windows Server 2014	32 GB	1TB
Servidor de Dominio	2	Windows Server 2014	32 GB	1TB
Switch Core	2	Comware 5	256 MB	32 MB
Switch de acceso a usuarios	5	Comware 5	128 MB	16 MB
Switch de acceso a servidores	2	Comware 5	128 MB	16 MB
Total de equipos	29			

Tabla 6: Prestaciones de los Servidores

Como vemos en la tabla En el Centro de Datos se instalará nuevos dispositivos y se los configurará, tales como: servidores FTP, Proxy, Web y DNS, así como una central telefónica IP, a través de la cual se gestionarán los teléfonos de esta entidad [14].

También se configurará un punto de acceso inalámbrico, para facilitar a los trabajadores la fácil conexión a través de portátiles, y la ágil gestión de sus labores dentro de la empresa.

Áreas	Cantidad de ordenadores	Sistema Operativo	Memoria RAM	Disco Duro
Sistemas	20	Windows 10	8 GB	750 GB
Negocio	10	Windows 8	4 GB	320 GB
Administración	20	Windows 8	6 GB	320 GB
Seguridad Bancaria	5	Windows 10	8 GB	750 GB
Auditoría	26	Windows 8	6 GB	320 GB
Operaciones	15	Windows 8	6 GB	320 GB
Total	96			

Tabla 7: Actualizaciones de los activos informáticos

Como se muestra en la tabla 7 las actualizaciones que tendrán los dispositivos informáticos para el diseño de red propuesto, si llegasen a necesitar cambio de equipo se le evaluará el antiguo equipo y procederá al cambio de un nuevo equipo.

3.9 Diseño lógico de la red del Banco

Para el diseño lógico de la red se tendrán en cuenta 3 aspectos fundamentales.

- ✓ Topología de la red del Banco.
- ✓ Modelo de direccionamiento.
- ✓ Enrutamiento de redes.

3.9.1 Topología de la red del Banco:

La red del banco tendrá un diseño de topología en estrella, debido a que la conexión se establecerá, desde el nodo central a las áreas existentes y viceversa. En la figura, se muestra la imagen del diseño lógico para la red del Banco. [2]

Como se puede presenciar en la figura 3.2, los datos fluirán desde el Core hasta cada una de las áreas del banco.

3.9.2 Modelo de Direccionamiento:

El protocolo de TCP/IP abarca el modelo de direccionamiento, ya que las direcciones IP pertenecen a este protocolo.

SERVICIOS	VLANS	RANGOS P	MÁSCARA
SERVIDORES	150	192.168.51.0	255.255.255.0
DATOS	151	192.168.52.0	255.255.255.0
VOZ	152	192.168.53.0	255.255.255.0
CCTV	153	192.168.54.0	255.255.255.0
WIRELESS	154	192.168.55.0	255.255.255.0
DATAFAST	155	192.168.56.0	255.255.255.0
MEDIANET	156	192.168.57.0	255.255.255.0

Tabla 9: Servicios con su VLAN

Como podemos observar en la tabla 9 se muestra la distribución de las Vlans y direcciones IP para la red del Banco.

El tercer octeto de cada dirección IP identifica la subred a la que pertenecen los servicios del banco.

Los servicios de DataFast y MediaNet son equipos utilizados para los cobros de las tarjetas de créditos.

En la figura 3.4 se muestra la estructura de las direcciones IP y VLANS por servicios.

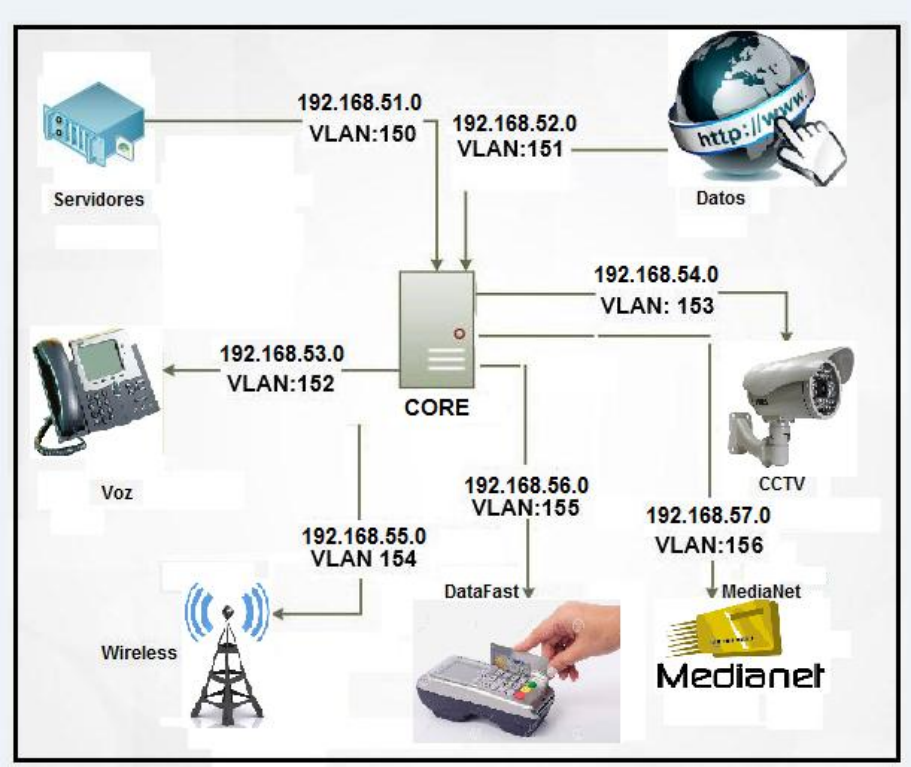


Figura 3.4: Diseño Lógico

En la figura 3.4 vemos que las VLANS creadas, serán exclusivamente utilizadas para la red bancaria, además de los puertos configurados en los Switch para la conexión de la red del Banco.

3.9.3 Seguridad de la red bancaria Interna.

Para garantizar la seguridad de la red del Banco, se configurarán VLANS privadas, se define que el acceso a la red sea por direcciones MAC, y se garantizará la seguridad de acceso a los equipos de comunicación.

Se puntualizará lo siguiente:

- ✓ Se configurarán y se administrarán las VLANS.
- ✓ Se bloqueará las unidades extraíbles en los ordenadores del Banco.
- ✓ Todos los equipos deberán tener instalado el antivirus.
- ✓ Solo se instalará programas básicos con su debido licenciamiento.
- ✓ Se limitará la navegación al Internet para los ordenadores del Banco.
- ✓ Todos los ordenadores deberán estar ingresados al Dominio.

Se obtendrá:

- ✓ Seguridad en las comunicaciones de la Agencia Bancaria.
- ✓ Serán adaptables a la infraestructura del Banco.
- ✓ Se garantizará un mejor desempeño en el área de trabajo.

3.9.4 Acceso a la red por direcciones MAC:

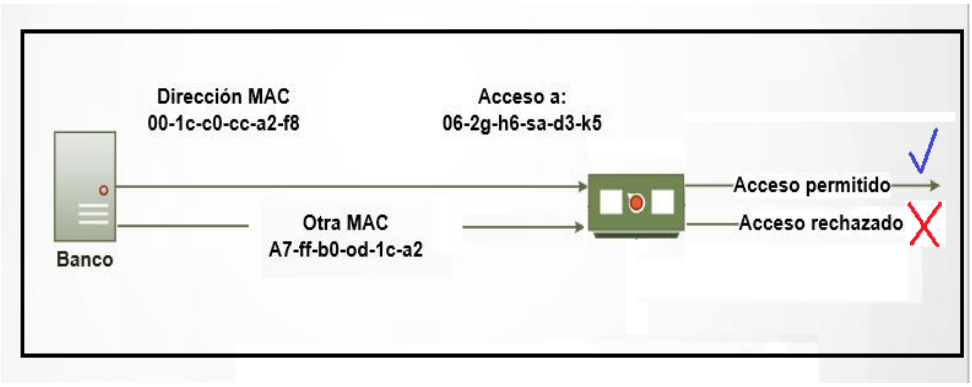


Figura 3.5: Acceso a la red por MAC

En la figura 3.5 vemos que para gestionar el acceso a la red se tomó en consideración máquinas virtuales instaladas en las estaciones de los usuarios y switches instalados en puntos de acceso para usuarios. También se realizó un inventario de aplicaciones y recursos en la red.

En cada puerto de los switches se deberá grabar la dirección MAC de cada estación y en caso de que alguna estación tenga instalada una máquina virtual, se deberá grabar también la dirección MAC de la máquina virtual. El método para grabar las direcciones MAC puede ser manual o dinámico, se recomienda hacerlo dinámico, esto quiere decir que el puerto graba automáticamente la dirección MAC al conectar la estación de trabajo. Con este método se otorga conexión física a las estaciones de trabajo.

Con esto se puede asegurar que otro dispositivo de red que no haya sido admitido, acceda a través de los puertos de los Switch.

3.9.5 Acceso a la red por direcciones IP:

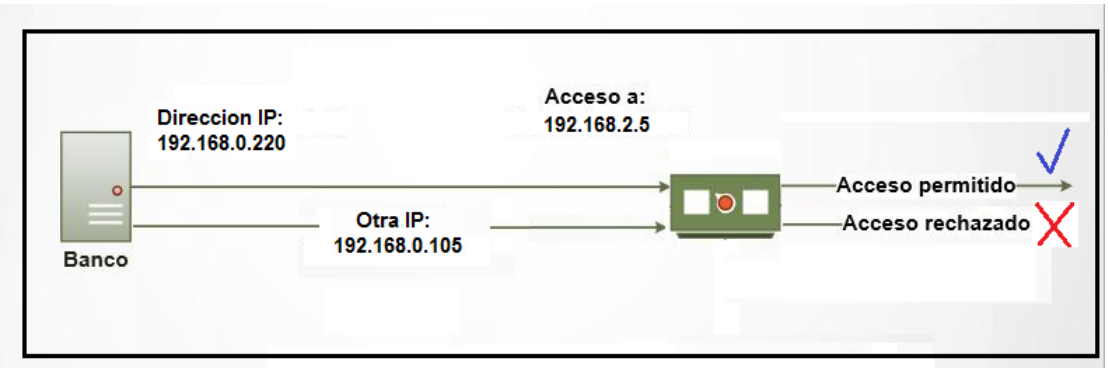


Figura 3.6: Acceso por IP

Se crearán ACLs (Access Control List) que permitan a los usuarios acceder únicamente a los recursos que están autorizados. Se creará una plantilla base para que todos los usuarios tengan acceso a los servicios básicos de la institución:

Equipo	Servicios
File Server	tcp445
Web Servers	tcp443
Intranet	tcp80
Domain Controller	all tcp/udp
DNS	tcp53/udp53
Impresora	9100

Dependiendo de las funciones de cada usuario se agregarán ACLs personalizadas para cada Estación de trabajo.

3.9.6 Disponibilidad de la red:

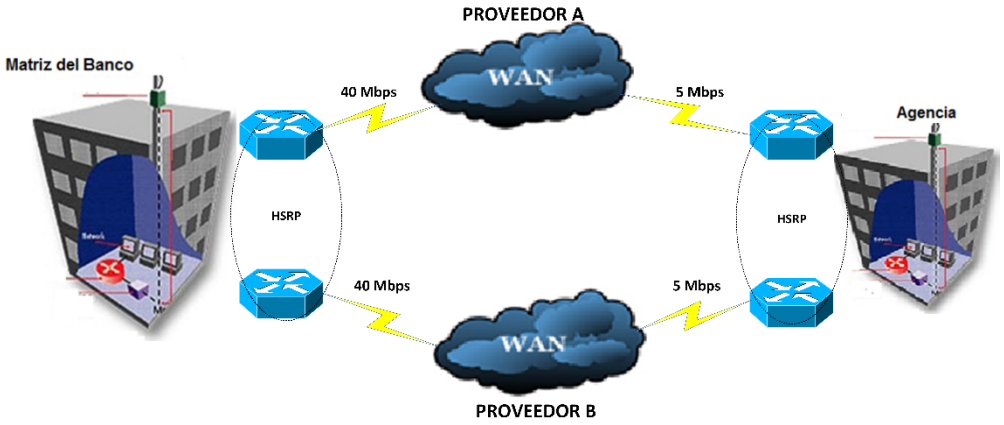


Figura 3.7: Disponibilidad de la Red

Para mejorar la disponibilidad de la red se propone la contratación de otro proveedor de enlace de datos para las agencias y la Matriz, como el actual proveedor cuenta con equipos marca CISCO esta implementación conlleva a que los equipos que instale el nuevo proveedor también deben ser marca CISCO para no afectar en mayor proporción la infraestructura actual, esto implica que el Switch que conecte a estos dos Routers soporte el protocolo IGMP para el intercambio de mensajes

HSRP entre los Routers y de acuerdo al inventario realizado; ningún Switch soporta este protocolo por lo que deberán ser cambiados.

Del levantamiento de información se tiene que 7 de las 47 Agencias no cuentan con UPS, por lo que se propone la compra de 7 UPS para mantener energía eléctrica al menos 3 horas en caso de existir corte del suministro eléctrico público.

Junto con la reestructuración que se realizará en la Matriz se garantizará tener una disponibilidad del %99.99.

3.10 Diseño de Active Directory para la red del Banco

Previo al diseño de Active Directory, es necesario conocer que para que este funcione correctamente los servidores DNS (Domain Name System) y DHCP (Dynamic Host Configuration Protocol) deben ser configurados con antelación, ya que el Active Directory responde a un dominio. [11]

El Active Directory (AD) emplea el servidor DNS para obtener nombres de host de direcciones IP específicas, y para asignar nombres de dominios a los diferentes hosts, así como facilitar la búsqueda de distintos objetos, por lo que la implementación del servidos DNS resulta imprescindible.

El servidor DHCP permite asignar direcciones IP de manera dinámica, así como evitar que dichas direcciones se repitan, y causen un conflicto IP. Al igual que el DNS, resulta fundamental su implementación.

Al nosotros implementar Active Directory, nos permitirá separar la estructura lógica conformada por el dominio de la estructura física, constituida por la topología de la red. Esto constituye una ventaja, pues permite que el esquema sea independiente de la topología de la red empleada para el Banco y que se pueda administrar de forma independiente.

A través de la implementación de Active Directory, lograremos organizar y mejorar la búsqueda de los equipos que forman parte de la red. Así como se

garantizará la autenticación de los usuarios y ordenadores. Los recursos de la red se compartirán de una manera óptima.

Para implementar AD (Active Directory), se realizó un estudio inicial de la infraestructura interna de la red, lo que permitió identificar las falencias y necesidades de la empresa. Seguidamente, se muestra el esquema general del AD, para la red del Banco.

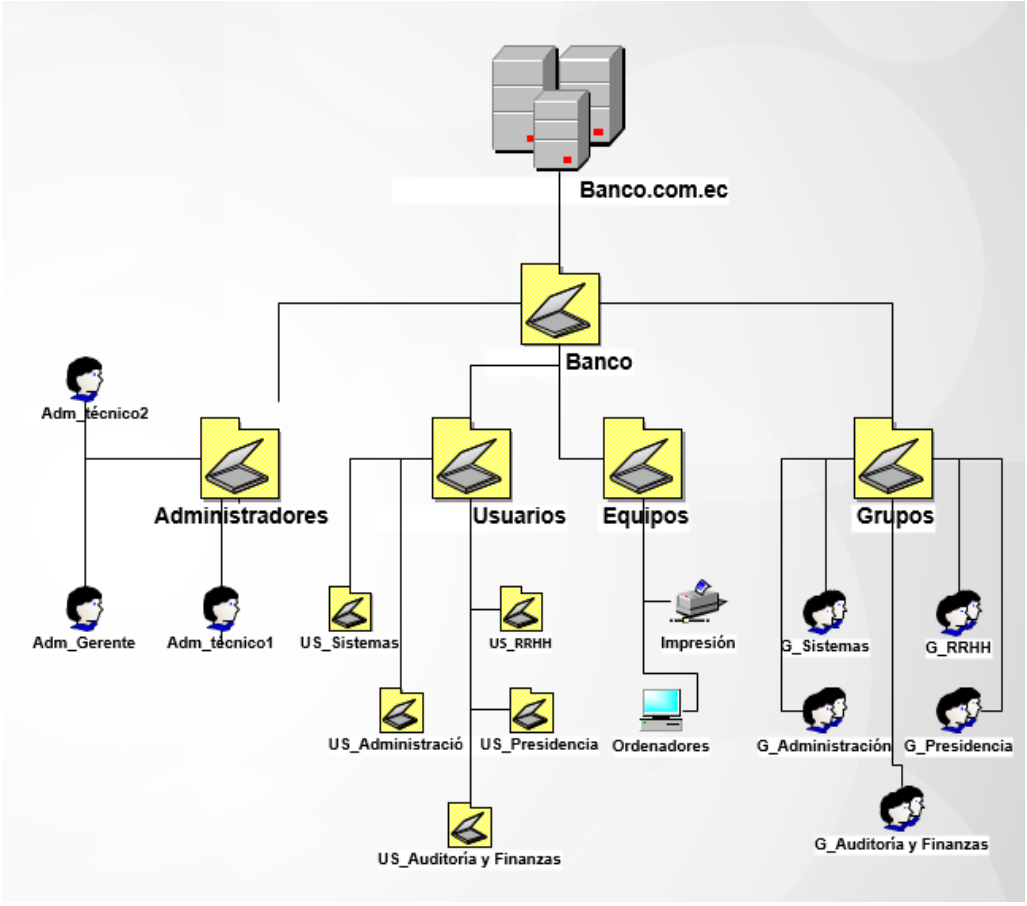


Figura 3.8: Directorio Activo (DA) o Active Directory (AD)

3.11 Estructura lógica

Como vimos en la imagen anterior se propone llamar al dominio de la organización por Banco.com.ec, porque es un nombre sugerente para la entidad y no existe otra institución con un dominio a nivel mundial similar a este.

Con el objetivo de organizar el diseño y evitar confusiones entre las Unidades Organizativas con siglas (UO), se implementa una UO (Unidades Organizativas), llamada Banco_Ecuador. Dentro del LDAP (Lightweight Directory Access Protocol) se configurarán las UO (Unidades Organizativas) y se definirán sus nombres, los cuales serán: Administradores, Equipos, Usuarios y Grupos.

A continuación, se describen cada unidad administrativa y los objetos que la conforman:

- **UO Administradores**: Cuenta con todos los objetos usuario que sean administradores del dominio, dichos usuarios podrán realizar todo tipo de modificaciones, en el servidor del dominio y en los equipos cliente. Se crearán 3 cuentas con el perfil de administrador: 1 será para el gerente de sistemas, el cual tendrá acceso total a los elementos de la red y 2 cuentas también con el perfil de administrador para 2 técnicos, con las cuales podrán gestionar los procesos informáticos del banco y brindar apoyo a los mismos.

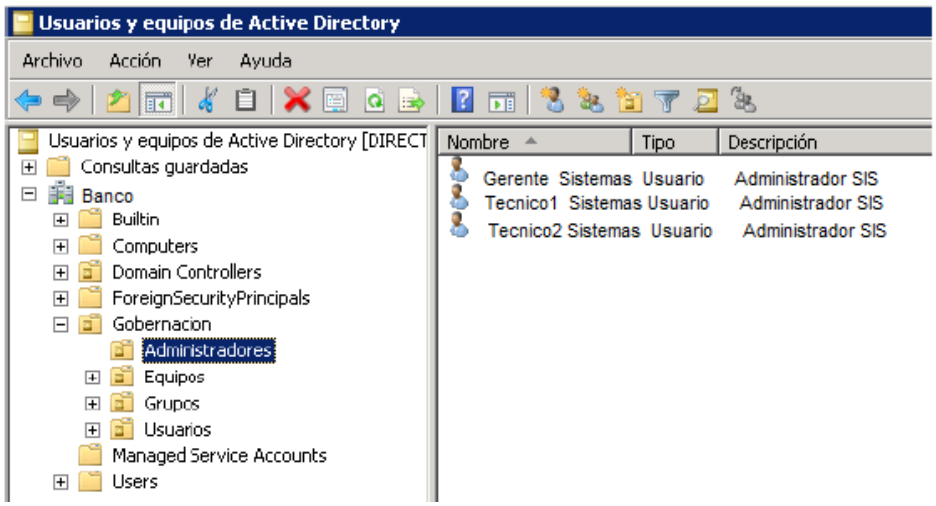


Figura 3.9: Administración de DA (Directorio Activo).

- **UO Usuarios**: En esta unidad se encuentran todos los usuarios que pertenecen a la red Banco, los mismos se agruparán según las áreas a las que pertenezcan. Cada objeto con nombre usuario tendrá definido el nombre de usuario, la contraseña, el nombre completo, la dirección del usuario, cargo en el que se desempeña, teléfono, dirección de correo y área a la que pertenece.

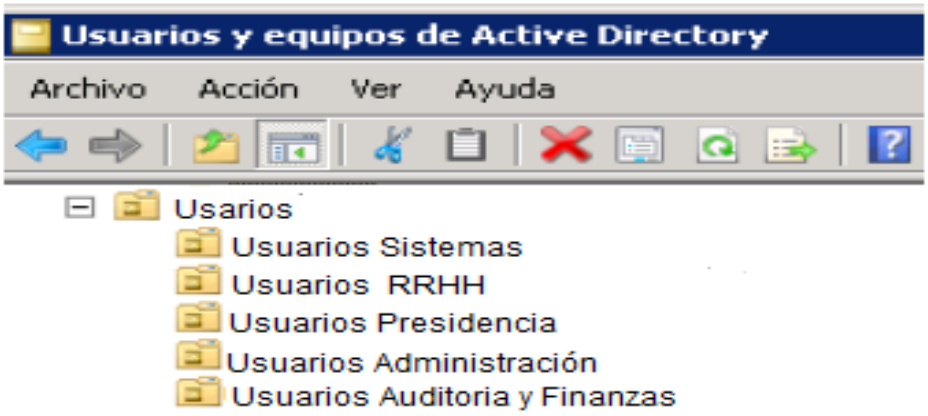


Figura 3.10: Administración de usuarios

- **UO Grupos**: En esta unidad se guardará la información referente a los grupos pertenecientes al directorio activo. Se definió que se realizará un grupo por área. Los grupos serán los que se muestran a continuación:

  ✓ B_Sistemas.

  ✓ B_RRHH.

  ✓ B_Presidencia.

  ✓ B_Administración.

  ✓ B_Auditoría_Finanzas.

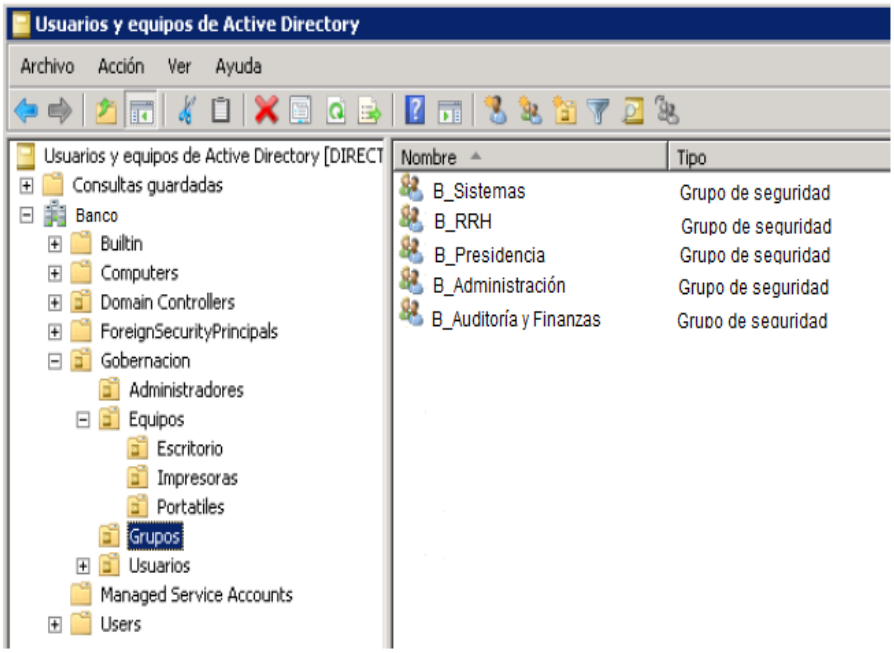


Figura 3.11: Administración de grupos

- **UO Equipos**: Esta unidad está conformada por dos unidades organizativas. Una de ellas es la unidad llamada impresión, que contiene todas las impresoras de la entidad bancaria y la otra es la unidad de ordenadores que incluye todas las PC.

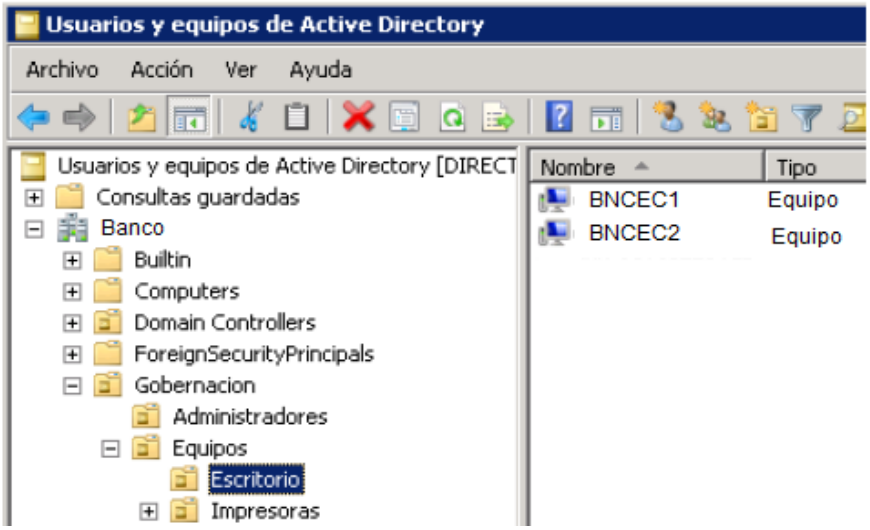


Figura 3.12: Administración de equipos

3.12 Políticas de Grupo

Luego de realizar un análisis sobre las políticas definidas para la entidad bancaria, se definen como Políticas de Grupo Iniciales:

- Restricción para la instalación de programas: Se limitará a los usuarios las posibilidades de instalar software que no necesiten para realizar sus funciones dentro de la entidad.
- Restringir el ingreso al panel de control: Con esta política se evitará que los usuarios cambien la configuración de los ordenadores.
- Definir los fondos y protectores de pantalla: A través de esta política, los equipos tendrán los protectores y fondos establecidos para el Banco.
- Configurar la página web del banco como página de inicio del Internet Explorer.
- Establecer controles de acceso: Se evitará que los usuarios de un área diferente puedan acceder a los ordenadores de otra área, en dependencia de los requerimientos.
- Establecer controles de activos a nivel de hardware: Se incluirá en cada ordenador un sello que lo identifique e se incluirá en cada activo un número de inventario, para evitar que estos sean trasladados de sitio.

- Establecer un formato para la complejidad de la contraseña: Esto permitirá que la integridad de las contraseñas que se les asigna a cada usuario no sea violada.

A continuación se mostrará la estructura lógica del Banco con políticas de grupo:

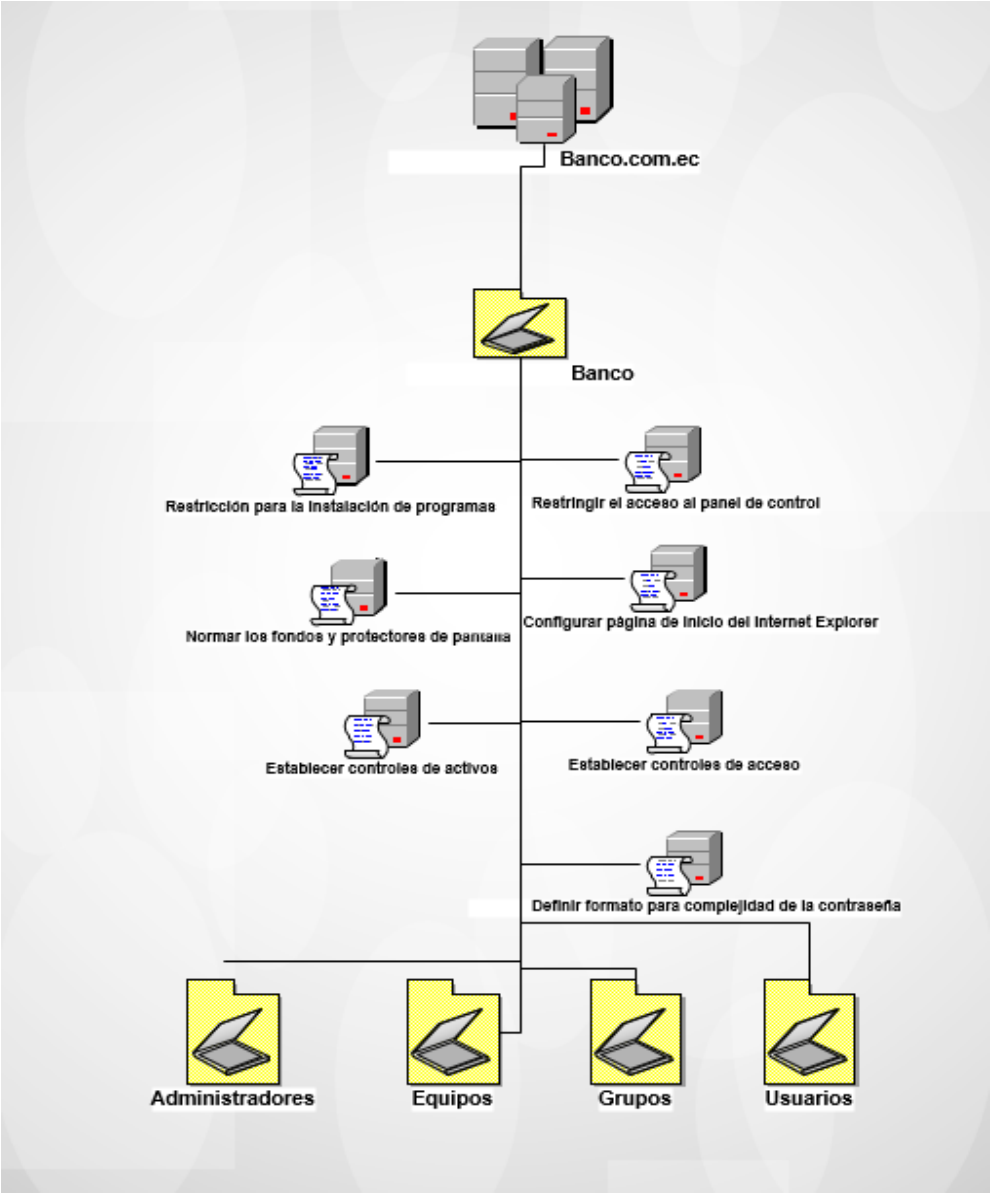


Figura 3.13: Directorio Activo con GPO (Group Policy Object)

Como podemos apreciar en la imagen tenemos el nombre del Dominio como cabecera, luego vienen los recursos o datos de la empresa, seguidos por las políticas del Banco, y para terminar los grupos ya sea administradores o usuarios.

3.13 Selección de proveedores a utilizar

El enlace que se utilizará, será a través de la fibra óptica, la cual se desplegará desde la empresa proveedora de Internet Punto Net y TelcoNet hasta la red Bancaria.

Se determina utilizar la fibra óptica por las ventajas que tienen, las cuales se listan debajo:

- ✓ Son ligeras y de tamaño pequeño.
- ✓ Son capaces de soportar grandes anchos de banda a altas velocidades de transmisión de datos.
- ✓ Están relativamente libres de la interferencia electromagnética.
- ✓ Tienen un reducido ruido y cruce de datos comparados con los cables de cobre convencionales.
- ✓ Tienen relativamente valores bajos de atenuación debido al medio de transmisión.
- ✓ Tienen una alta fiabilidad junto con una larga vida operativa.
- ✓ Tienen aislamiento eléctrico y están libres de conexión a tierra.

3.14 Equipos de seguridad y enlace

3.14.1 Firewall

Como firewall para la red del Banco se instalará un Dell SonicWall TZ600 Secure upgrade plus 2yr, ideal para el Banco ya que tiene oficinas remotas. [17]

Este firewall nos ofrecerá seguridad de alto rendimiento, prevención de intrusiones, examina simultáneamente el tráfico de todos los puertos; esto permitirá al Banco obtener más seguridad.

Suscripción a asistencia las 24 horas del día, los 7 días de la semana por 2 años.

Suscripción al Servicio de antivirus y prevención de spyware e intrusiones por 2 años, esto nos ayudará a mitigar el ingreso de virus a la red.

3.14.2 Switch

Para tener un mejor desempeño en la red y no sufrir por una alta carga de usuario conectados al mismo instante, instalaremos un Switch HP 5120-24G para cada uno de los departamentos, con esto tendremos un mejor rendimiento y disponibilidad en la red.[18]

Se obtendrá un mejor desempeño en el Banco ya que nos permitirá a su vez instalar tecnologías a futuro. Los usuarios estarán debidamente ordenados sin tener pérdidas de conexión a la red.

3.14.3 Router de inalámbrico

Se instalará en el área de Gerencia un router de inalámbrico de pared para las reuniones de alta gerencia; con esto ayudaremos a que los dispositivos móviles y los dispositivos inalámbricos en las reuniones puedan conectarse a la red pero tendrán una clave de acceso para poder controlar los accesos no permitidos por el área de Sistemas.

3.14.4 SAN (backup)

Como una solución para tener una copia de seguridad de alto rendimiento, opcionamos escoger SAN (IBM storwize v5000) ya que realiza copias para grandes volúmenes de datos. [15]

Figura 3.14: SAN 1

Proporcionará un gran beneficio al Banco ya que realiza copias de seguridad de alto rendimiento en la red.

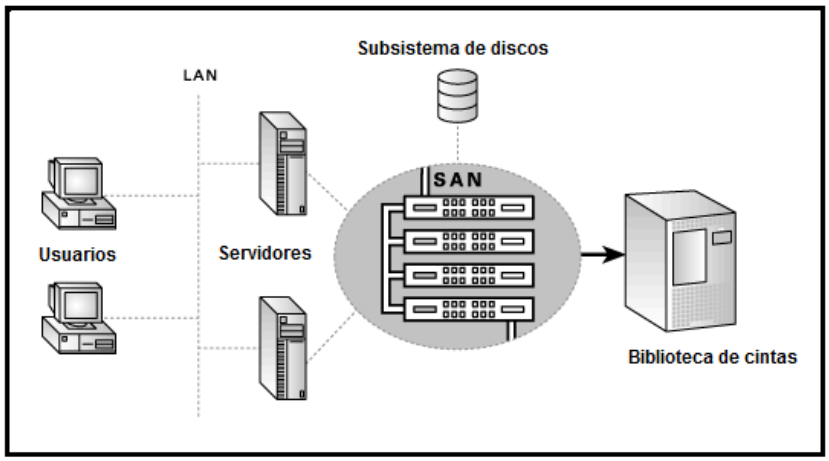


Figura 3.15: Esquema SAN

Los datos son almacenados en una librería de dispositivos de cinta compartida. Todo esto lo podemos hacer ya sea manualmente o automáticamente.

3.14.5 Acronis (Backup)

Otro sistema de respaldo que tendremos será Acronis Backup [19], este es un servicio de backup en la nube. Estos servidores están en la ciudad de Boston-EEUU. Tendremos una copia de respaldo de todos los servidores, de las aplicaciones que usa el banco, de los correos en Microsoft Exchange, de Active Directory, de las máquinas virtuales, archivos individuales y no solo realizará la copia de respaldo, este servicio estará protegiendo todos los Servidores de algún fallo de hardware. Se podrá recuperar todos los datos, tendrá servicio técnico las 24 horas del día los 7 días de la semana durante 3 años. La licencia es ilimitada, se podrá escoger una capacidad de almacenamiento de acuerdo a la necesidad del Banco.

3.15 Tipo de conexión en el Banco.

La fibra óptica que se utilizará para la conexión de la red del Banco, será Multimodo, ya que esta fibra según la Norma ISO soporta 10Gbits, esto nos dará un mejor enlace y como se conoce este dispositivo saldrá de Punto Net y TelcoNet hasta el router del Banco. Debe mencionarse que este medio de transmisión es físico y pertenece a la capa física teniendo en cuenta el modelo OSI. Este tipo de conexión también nos ayudara a soportar en enlace que tendrán nuestros servidores Backup ya que ellos necesitarán un enlace que soporte hasta 10G de conexión.

3.16 Microsoft Exchange 2016

En los grupos de trabajo, es esencial el envío y recepción de mensajes. La herramienta de Microsoft Exchange 2016 de la plataforma de Microsoft se basa en varios componentes de mensajería, los cuales interactúan para preparar un sistema de envío y recepción de mensajes de una organización.

Cada cuenta tendrá un máximo de 300 Mb de almacenamiento. Los gerentes de departamento y la presidencia contarán con el almacenamiento ilimitado.

3.16.1 Restricciones de envío y entrega:

- ✓ El tamaño máximo de los mensajes de entrada y salida del Banco serán de 25 Mb.
- ✓ Emitirá alertas de buzón lleno.
- ✓ Prohibir el envío de mensajes, al llegar al máximo de almacenamiento del buzón.

3.16.2 Restricciones de mensaje

- ✓ Los usuarios con niveles de acceso restringidos, no podrán enviar mensajes directamente a la presidencia del banco.
- ✓ Los filtros antiespam serán configurados, con el objetivo de evitar que los usuarios reciban correos no deseados o spam.
- ✓ Los usuarios tendrán la opción de configurar filtros en el cliente de correo para restringir mensajes que provengan de otro usuario, según requieran.

CAPÍTULO 4

4. IMPLEMENTACIÓN

PLAN DE ACTIVIDADES

Actividades	Mes1	Mes2	Mes3	Mes4	Mes5	Mes6	Mes7	Mes8	Mes9	Mes10	Mes11	Mes12
Cableado en el Centro de Computo												
Cambio de equipos de red (Switches)												
Migración de estaciones a nueva red, con seguridad en puertos y ACLs												
Implementación de enlace de backup para Agencias												
Implementación de sistema de respaldo												
Implementación de equipos de seguridad												
Plan de seguridad												
Documentación y procedimientos												

Tabla 9: Plan de Actividades

La implementación demorará de 12 meses, esto conllevará pruebas en las respectivas áreas, el diseño está previsto para realizar posibles implementaciones a futuro. Se detallan las tareas que incluyen cada actividad que se muestra en la tabla:

Cableado del Centro de cómputo

Esta actividad incluye el cambio de patch cord, instalación de canaletas, instalación de tuberías, peinado de cableado.

Cambio de equipos de Red

Se realizará cambios de Switches en agencias y en la Matriz, esto permitirá dar inicio a las actividades de migración de estaciones y de implementar enlaces de backup para las agencias.

Migración de estaciones a nueva red

Se creará un inventario de direcciones IP asociadas a los usuarios, también se detallará el puerto del Switch al que quedan conectados para facilitar futuros soportes

Implementación de enlaces de backup para agencias

Van a interactuar los 2 proveedores de servicios ya que ellos deben configurar HSRP en sus Routers y realizar pruebas de conmutación, también se debe habilitar IGMP en el switch que conectan los 2 routers.

Implementación de sistema de respaldo

Se va a trabajar sobre el mismo medio físico pero se va a separar el trafico de respaldo en otra VLAN por lo que se deberá configurar los puertos en modo troncal

Implementación de equipos de seguridad

Se creará un inventario de aplicaciones y servicios para la configuración y verificación de permisos, también se realizará pruebas de redundancia con Firewall de backup.

A continuación se detalla presupuesto para el proyecto.

CABLEADO ESTRUCTURADO	Cantidad	Precio Unitario	Total
Canaletas 40x25 con división interna (caja x 10u)	100	$ 85,00	$ 8.500,00
Canaletas 20x12 con división interna (caja x 50u)	80	$ 160,00	$ 12.800,00
Jack cat 6 (van en cada lado de los puntos)	80	$ 2,80	$ 224,00
Caja dexson 40mm	80	$ 2,00	$ 160,00
face Plate 2 servicios	75	$ 2,50	$ 187,50
Patch cord 1ft cat 6	0	$ 1,05	$ 0,00
Patch cord 3ft cat 6	0	$ 1,40	$ 0,00
Patch cord 5ft cat 6	75	$ 2,63	$ 197,25
Patch cord 7ft cat 6	70	$ 3,15	$ 220,50
Patch Cord Fibra Optica 3mt	10	$ 20,00	$ 200,00
Organizador simple 80x80 19" 2UR	20	$ 8,50	$ 170,00
Cinta velcro 3/4" x 10yrd	5	$ 13,96	$ 69,80
Amarras 30cm funda por 100 unidades	10	$ 5,00	$ 50,00
Conector rj45 cat 6 funda por 50 unidades	5	$ 34,00	$ 170,00
Botas para conector rj45 funda por 50 unidades	5	$ 4,75	$ 23,75
Conectores UY lock joint caja por 100 unidades	2	$ 5,00	$ 10,00
UTP Cat. 6 rollo de 305 mt.	10	$ 200,00	$ 2.000,00
Tubería BX 3/4", rollo de 50mt. (manga metálica)	50	$ 50,00	$ 2.500,00
Conector BX 3/4" recto	180	$ 2,00	$ 360,00
Conector EMT 3/4"	150	$ 0,50	$ 75,00
Unión EMT 3/4"	150	$ 0,50	$ 75,00
Tubería EMT 3/4", unidad	100	$ 2,00	$ 200,00
Caja metálico 4x4" con tapa	15	$ 1,25	$ 18,75
Servicios Profesionales	1	$5.660.00	$5.660.00
Total	**1272**		**$ 33.871.55**

Tabla 10: Costos de la instalación del Centro de Datos

Como se puede apreciar en la tabla 10 tenemos un total de $33.871.55 esto equivaldrá a la reubicación y renovación completa del Centro de Datos junto con los préstamos de los servicios profesionales, este nuevo Centro de Datos cumplirá con todas las normas correspondientes.

Adquisición de equipos y servicios

Descripción	Valor unitario	Cantidad	Total
HP 5500-48G-4SFP HI	$ 7.401.00	2	$ 14.802.00
HP 5120-24G EI	$ 1.780.00	3	$ 5.340.00
HP 5120-48G SI	$ 2.990.00	6	$ 17.940.00
HP 5120-24G SI	$ 1.575.00	53	$ 83.475.00
IMC Network Module(monitoreo de la red)	$ 35.000.00	1	$ 35.000.00
Diseño e implementación de la solución	$ 1.400.00	5	$ 7.000.00
Peinado y etiquetado del Centro de Datos	$ 35.00	750	$ 26.250.00
Instalación y Soporte	$ 240.00	15	$ 3.600.00
Enlace de datos secundario para Agencias	$ 320.00	48	$ 15.360.00
Subtotal			$ 217.867.00
IVA			$ 30.501.38
Total			$ 239.268.38

Tabla 11: Costos de equipos y servicios

En la tabla 11 se adquirirán equipos de comunicación, enlaces, servicios como es el peinado y etiquetado del Centro de Datos, instalación y soporte de los mismos.

Equipos de protección eléctrica

PROTECCION ELECTRICA	Cantidad	Precio Unitario	Total
Multitoma rackeable 19" con protección de voltaje	4	$ 35,00	$ 140,00
UPS Wadkin 20KVA Online	1	$ 10.350,00	$ 10.350,00
UPS APC 3000VA 3KVA	7	$1.300.00	$9.100.00
Total	5		$ 19.590,00

Tabla 12: Costos de equipos de protección

En la tabla 12 tenemos un costo de $19.590,00 esto será para la adquirir los equipos de protección de eléctrica que son los UPS y las Multitoma, esto nos ayudara en caso de existir algún tipo de alto de voltaje o sin servicio eléctrico, mantendrá los equipos operativos.

4.1 Costos de sistemas Operativos y licencias.

SISTEMAS OPERATIVOS	Cantidad	Precio Unitario	Total
Windows Server 2014 Estándar R2 (válida para 1 instalación)	6	$ 1.200,00	$ 7.200,00
Microsoft Exchange 2016 (válida para 1 instalación)	1	$ 5.000,00	$ 5.000,00
Microsoft SQL server (válida para 1 instalación)	1	$ 1.200,00	$ 1.200,00
Licencia de Acronis Backup Windows Server Essentials(licencia Limited)	4	$ 11.785,00	$ 11.785,00
Total	**12**		**$ 25.185,00**

Tabla 13: Costos de Sistemas Operativos para los servidores

En la tabla 13 vemos los costos de los Sistemas Operativos a adquirir y la licencia de Acronis; esto será para tener un mejor rendimiento en la red y el respaldo de nuestros archivos en la nube.

Equipos de seguridad y backup.

SEGURIDAD PERIMETRAL	Cantidad	Precio Unitario
Dell SonicWall TZ600 secure upgrade plus 2yr	1	$ 3.714,00
Dell SonicWall TZ600 high availability	1	$ 1.767,00
Stateful HA upgrade for TZ600 licencia perpetua	1	$ 554,00
Dell SonicWall TZ600 rack mount kit	2	$ 435,00
SonicWall Analyzer reporting software for TZ600	1	$ 382,00
Servicio de instalación y configuración	1	$ 500,00
Acronis backup (2años)	1	$14.142,00
IBM storwize v5000 (SAN)	1	$50.000.00
Total	**7**	**$ 71.494,00**

Tabla 14: Costos de equipos y software de Backup

En la tabla 14 tenemos un costo de $ 71.494,00, esto será por la adquisición de equipos de seguridad como es el SonicWall y sus aplicaciones, la aplicación de Acronis Backup para que todos nuestros servidores tengan copia de seguridad en la nube y nuestra copia en físico IBM Storwize o SAN.

4.2 Costo final del proyecto

Implementación del cableado	$ 33.871.55
Implementación de equipos de red	$ 239.268.38
Implementación de equipos de protección	$ 19.590,00
Sistemas Operativos	$ 25.185.00
Software de Respaldo	$ 71.494.00
Costo Total	$ 389.408.93

Tabla 15: Costos del proyecto

En la tabla de costo final del proyecto que estamos apreciando, entre los servicios prestados por instalación y mano de obra tendremos un valor de $389.408.93 este valor equivale al cambio total del Centro de Datos, instalación de los dispositivos de backup, actualización de S.O. y equipos de enlace.

CONCLUSIONES Y RECOMENDACIONES

Con este proyecto el Banco tendrá mejor rendimiento en la red y una mejor disponibilidad de sus recursos internos en la red.

Los usuarios podrán ingresar a su sistema con total seguridad, tendrán respaldos de todos sus archivos y aplicaciones, los clientes podrán realizar sus operaciones bancarias con toda seguridad y no correrán con el riesgo de que su información privada sea robada y su cuenta bancaria manipulada por personal no autorizado debido a que el Centro de Datos tendrá el respaldo de todas sus actividades realizadas.

El logro fundamental de este trabajo fue planificar, analizar y documentar la red del Banco para su desarrollo se tuvieron en cuenta los estándares de cableado estructurado existentes; el rediseño propuesto, es el principal aporte de este trabajo, ya que se puede afirmar que es óptimo, escalable, administrable y además funcional. Por ende se adaptará a las necesidades futuras del Banco.

Este diseño está siendo implementado con tecnología a futuro para un mejor rendimiento, el reordenamiento de políticas de seguridad para todo tipo de área, se realizó un inventario detallado, preciso y completo de todo el hardware existen ya sean modelos y números de series de cada elemento también de las aplicaciones y componentes, esto ayudará a poder implementar nueva tecnología a futuro.

El plan de contingencia que se enfoca en realizar copias de seguridad de los datos y recuperación de datos, es la base fundamental del banco para que el cliente se sienta seguro que su información no vaya ser robada; se recomienda realizar mantenimiento a las aplicaciones de igual forma a los equipos para mejorar y optimizar los recursos tecnológicos con que cuenta el banco. Como último punto también se recomienda realizar actualizaciones en las documentaciones de los procesos tecnológicos para evitar errores y mejorar el rendimiento de los servicios que presta el banco a sus clientes.

BIBLIOGRAFÍA

[1] Digital Guide, “DMZ zona desmilitarizada y protege tu red interna”2015 de 1&1 Internet España S.L.U.disponible en : https://www.1and1.es/digitalguide/servidores/seguridad/en-que-consiste-una-zona-desmilitarizada-dmz/

[2] Electronica Unicrom,” Topologia de Redes de Computadoras”, 2016 disponible en:http://unicrom.com/topologias-de-redes-estrella-malla/

[3] Franco Espiño, B. (2010). RTA(Red de Transparencia y Acceso a la Información*)*. Disponible en: http://mgd.redrta.org/guia-de-implementacion-operacional-control-de-acceso/mgd/2015-01-28/092509.html

[4] Lamilla.Rubio,(2009, octubre 16) “Desarrollo de Políticas de Seguridad Informática e Implementación de Cuatro Dominios en Base a la Norma 27002, para el área de Hardware en la MEpresa Uniplex Systems.SA en Guayaquil. Guayaquil: ESPOL”, disponible en: http://dspace.espol.edu.ec/handle/123456789/7709.

[5] Administración de redes, (2014 mayo 19), disponible en: https://serviciosderednoona.wordpress.com/dns/manual-de-instalacion-y-configuracion-del-dns-en-windows-server-2008/

[6] Molreo, L. “Planificación y gestión de redes*”.* Venezuela, 2013

[7] Peláez, A., & Rodríguez, J. (s.f.). Entrevista*, 2008*

[8] SATCOM. (2015, septiembre 16). *Sistema de Gestion de Red.* Thales Alenia.

[9] Villegas, J. (2009, febrero 22). TecnoSeguro. Disponible en: https://www.tecnoseguro.com/faqs/control-de-acceso/%C2%BF-que-es-un-control-de-acceso.html

[10] John L. Ward, (2010, marzo 9) Strategic Planning for Information Systems, disponible en:

http://www.cynertiaconsulting.com/sites/default/files/PDF/Cynertia_Planificacion_estrategica_sistemas_resumen.pdf

[11] Administración de redes, (2014, febrero 19), disponible en https://serviciosderednoona.wordpress.com/servicio-hcp/dhcpwindowsserver/

[12] Banco de Machala (2015) https://www.bancomachala.com/institucional/historia/l

[13] Aarroyo (2016) http://es.slideshare.net/kacjoa/diseo-y-normas-para-data-centers

[14] Monografías SA (2010)http://www.monografias.com/trabajos81/seguridad-en-redes/seguridad-en-redes2.shtml

[15] Unylogix (2010)http://www.unylogix.com/data_storage/backup/SANbackup.htm

[16] UNMSM (2007) Oficina General del Sistema de Bibliotecas y Biblioteca Centralhttp://sisbib.unmsm.edu.pe/bibvirtual/tesis/Basic/cordova_rn/contenido.htm

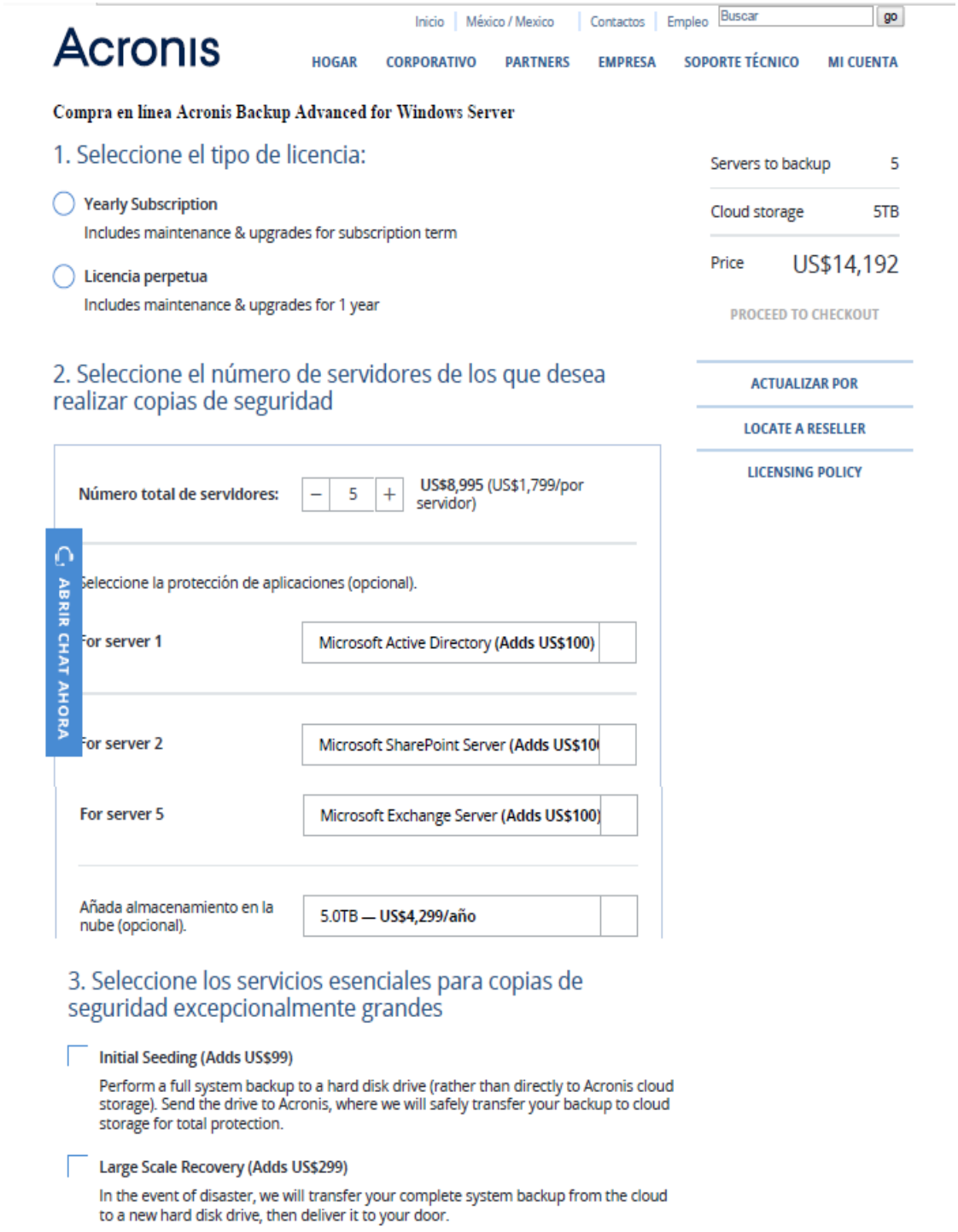
[17] SonicWall, Tz600 Network Security Firewall, 2016 disponible en: https://www.sonicwall.com/mx-es/products/tz600/

[18] HP Development Company, Conmutador Hp 5120-24G IE con 2 ranuras de interfaz, 2016 disponible en: http://www8.hp.com/lamerica_nsc_carib/en/products/oas/product-detail.html?oid=4174785

[19] Acronis International, Acronis Backup 12 protección de datos vía remotas, en la nube ya sea de forma privada o pública, 2002 disponible en: http://www.acronis.com/es-es/business/backup/

ANEXO

COTIZACIONES



3 – Opción de pago de la propuesta

Proponemos al cliente el siguiente plan de pago sin intereses, manteniendo los precios anteriormente cotizados:

- 40% de contado a partir de su aceptación
- 20% a 30 días después del anticipo
- 20% a 60 días después del anticipo
- 20% a 90 días después del anticipo

3.1 – Tiempo de implementación de la propuesta

El tiempo de implementación de la propuesta dependerá de las reuniones preliminares que se hagan con el cliente final y los proveedores de forma general podemos indicar lo siguiente:

- Reuniones con el cliente y proveedores (1.5 semanas)
- Configuración de los equipos activos fuera de línea (1 semana)
- Cambios en la red del cliente actual (1 semana)
- Pruebas de implementación de la solución. (1 semana)
- Implementacion y puesta en producción de la solución junto con monitoreo de la misma (1 semana)
- Monitoreo de la red y verificación y configuración de alarmas y revisión de las mismas (1 semana).

4.- Observaciones Importantes

Este proyecto es de propiedad intelectual de Gensystems., y es traspasado en una relación de confianza a su empresa. Razón por la cual, queda absolutamente prohibida su reproducción total o parcial, duplicación y traspaso a terceros sin expresa autorización escrita del autor.

MacroLite

VALORES Y FORMA DE PAGO

Propuesta de la Solucion

BANCO .- Atencion Departamento Financiero

Edgar Paredes representante de la empresa MACROLITE, quien suscribe esta propuesta, declara que:

A. Se examinaron los requerimientos detalladamente y no se tienen reservas a los requisitos solicitados, incluyendo las adendas o modificaciones a la presente convocatoria.
B. Me comprometo brindar servicios profesionales designados por el solicitante.
C. El precio de los equipos está dispuesto en moneda americana y la cantidad es ***Veinte Ocho Mil Cuatrocientos Diez y Seis con Noventa y Cinco USD.***
D. El detalle de los costos son:

Codigo	Producto	Cant.	Valor Unit.	Subtotal	TOTAL
ECUCONFRED02	**Sw-Core 24 Puertos -** HP HI 5500-24G-4SFP: 24 puertos 10/100/1000 + 4 puertos SFP+, FULL CAPA3	1	$ 6,421.00	$ 6,421.00	$ 6,421.00
ECUCONFEQUI03	**Switch de Borde 24 Puertos -**HP 1950-48G-2SFP+-2XGT: 48 Puertos 10/100/1000 + 2 Puertos SFP+ Y 2 puertos a 10GB por UTP - Rack	3	$ 1,023.00	$ 3,069.00	$ 3,069.00
ECUCONFEQUI09	**Switch de Borde 24 Puertos -** HP 1950-24G-2SFP+-2XGT: 24 Puertos 10/100/1000, + 2 Puertos SFP+ Y 2 puertos a 10GB por UTP - Rack	5	$ 1,798.75	$ 8,993.75	$ 8,993.75
ECUEQUICIS023	HP IMC Std Plat w/50 Nodes E-LTU -HP Intelligent Management Center Standard Software Platform, Highly flexible and scalable, deployment, Powerful administration control, Rich resource management, Detailed performance monitoring and management, flexible centralized reporting	1	$ 7,233.20	$ 7,233.20	$ 7,233.20
ECUCONFCIS002	Reingenieria, Diseño e Implementación de red " Centro de Datos de la Matriz ", Configuracion de Vlans, Configuración de rutas, Protocolos de Enrutamientos, Optimización de rutas	1	$ 2,700.00	$ 2,700.00	$ 2,700.00
	Servicio y mantenimiento Garantía limitada de por vida Detalles de Servicio y Mantenimiento Garantía limitada - repuesto - de por vida ¦ Garantía limitada - fuente de alimentación y ventiladores - 5 años ¦ Actualización de nuevas versiones				**$ 28,416.95**

E. La propuesta se mantendrá vigente por los días que se indican a continuación, contados a partir de la fecha fijada documentos: 7 días calendario.
F. Esta propuesta será aceptada en cualquier momento hasta antes del término de dicho periodo.
G. Manifiesto no haber sido declarado(a) inelegible por el BANCO para presentar propuestas.
H. Entiendo que esta propuesta constituirá una obligación contractual, hasta la preparación y ejecución del contrato formal.

CONDICIONES COMERCIALES

	Detalle
	✓ Los precios señalados están expresados en Dólares Americanos. ✓ Los precios señalados no incluye IVA. ✓ Para servicios adicionales durante la ejecución del proyecto, se podrá llegar a un acuerdo con el proveedor. ✓ Se consideran locales los servicios entregados en la ciudad de Guayaquil – Ecuador, por lo tanto los servicios se facturaran acorde a las leyes de ese país. ✓ Los precios foráneos mencionados no incluye los viáticos para el consultor, tales como, alimentación, hospedaje, movilización, en caso de realizar su labor fuera del área metropolitana de la ciudad o fuera del país del cual proviene la empresa contratada donde el consultor desarrollará su ejercicio profesional. ✓ Se cancelará: **Por concepto equipos & servicios** $ 28,416.95 USD – De acuerdo a las fases

Se estima que la inversión que se realizará será recuperada aproximadamente en 11 meses. Con la propuesta de garantiza cobertura para los nuevos clientes y total disponibilidad de los servicios.