



Banco de la República
Bogotá D. C., Colombia

Subgerencia de Informática

**REQUERIMIENTOS TECNICOS PARA LA
CONEXIÓN A LOS SERVICIOS ELECTRONICOS
DEL BANCO DE LA REPUBLICA-SEBRA**

Septiembre del 2005

Versión 4.0

TABLA DE CONTENIDO

1	INTRODUCCIÓN	1
1.1	OBJETO	1
1.2	ALCANCE	1
1.3	AUDIENCIA	2
2	INFORMACION GENERAL.....	3
2.1	INFRAESTRUCTURA GENERAL PARA ACCESO A SEBRA	4
2.2	DIFERENTES ESQUEMAS DE SEGMENTO DE RED LOCAL	9
3	INTERCONEXIÓN RED CORPORATIVA - RED ACCESO SEBRA ...	13
3.1	PROBLEMÁTICA A RESOLVER	13
3.2	CONSIDERACIONES GENERALES PARA LA IMPLEMENTACIÓN.....	14
3.3	CONFIGURACIÓN EQUIPOS CON FUNCIÓN DE FIREWALL	18
3.3.1	Reglas generales para todas las estaciones	18
3.3.2	Reglas para estaciones que utilizan aplicaciones DCV, Omesys y Cud.....	20
3.3.3	Reglas para estaciones que utilizan aplicaciones CEDEC-CENIT	20
3.3.4	Reglas para estaciones que utilizan aplicación SEN.....	21
3.4	ASIGNACIÓN DE DIRECCIONES IP	22



1 INTRODUCCIÓN

1.1 OBJETO

Este documento presenta los conceptos técnicos que deben ser tenidos en cuenta, por parte de las áreas de tecnología de las entidades financieras, en el momento de implementar una infraestructura tecnológica para el acceso a los servicios prestados por el Banco de la República. Todos estos servicios comparten una plataforma única de acceso denominada “Portal SEBRA”.

1.2 ALCANCE

Este instructivo presenta los diferentes conceptos técnicos que deben ser tenidos en cuenta cuando una entidad financiera esté planeando la implementación de una plataforma para el ingreso a “SEBRA”.

El documento recopila todos los pasos conceptuales que el Banco considera necesarios para el correcto funcionamiento del esquema. El documento no especifica los mecanismos o



procedimientos requeridos para realizar la configuración de los diferentes equipos que realizarán las funciones deseadas. El procedimiento de análisis, selección de la topología, instalación y configuración de los equipos es responsabilidad del área de tecnología de cada entidad financiera.

El Banco de la República estará atento a resolver, de forma telefónica y por intermedio de su Centro de Soporte Informático, las dudas relacionadas con los conceptos incluidos en este documento. Este servicio no incluye el soporte técnico a los equipos de propiedad de cada entidad, el cual es responsabilidad de las áreas de tecnología respectivas.

Los esquemas propuestos en este documento han sido preparados por la Subgerencia de Informática y buscan facilitar la implementación y funcionalidad de los esquemas de comunicación entre las entidades financieras y el Banco de la República.

1.3 AUDIENCIA

Este instructivo está dirigido a:

- Las áreas de tecnología de las entidades financieras que utilizan los servicios electrónicos prestados por el Banco de la República.
- Al personal del Centro de Soporte Informático del Banco de la República.
- A las áreas de tecnología informática del Banco de la República (Departamento de Tecnología Informática y Unidad de Seguridad Informática).



2 INFORMACION GENERAL

Para implementar un esquema de comunicaciones que integre la plataforma de red propia de una entidad financiera con los equipos específicos para la conexión a los servicios del Banco de la República es necesario realizar un análisis de las necesidades de cada entidad. Se deben tener en cuenta la cantidad de estaciones cliente, su ubicación dentro de la entidad, el volumen de operaciones y otros factores. Todos estos elementos hacen que el diseño de la solución sea un proceso relativamente complejo que requiere de un conocimiento amplio en el tema de redes de computadores.

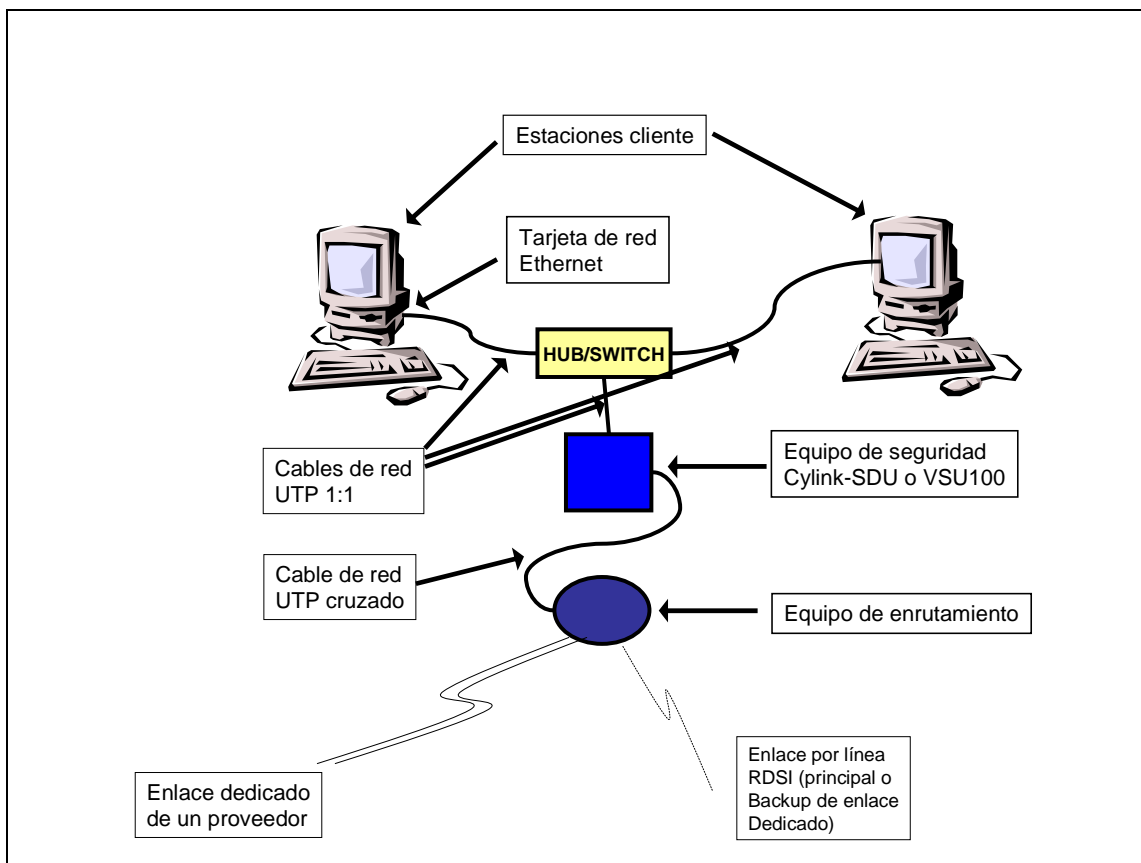
Para comprender las implicaciones de un esquema de “Conexión al Portal Sebra” es importante conocer primero los esquemas básicos de conexión para después determinar las necesidades de cada entidad y decidir si se requiere un esquema de integración de redes.



2.1 INFRAESTRUCTURA GENERAL PARA ACCESO A SEBRA

Los diferentes servicios electrónicos prestados por el Banco de la República (DCV, SUBASTAS, CUD, SEN, CEDEC y CENIT) requieren una infraestructura de redes y seguridad que garantice la comunicación segura y eficiente entre las diferentes estaciones de usuarios y los servidores centrales de dichas aplicaciones.

La infraestructura básica que requiere una entidad financiera para conectarse a los servicios electrónicos del Banco de la República se ilustra en la gráfica 1.



Gráfica 1

La descripción de cada elemento se presenta a continuación:



1. Enlace entre la sede de la entidad financiera y la sede del Banco de la República

Normalmente este es un enlace dedicado que se contrata con uno de los proveedores de servicios de telecomunicaciones que poseen infraestructura para llegar al Banco de la República. En la actualidad se puede contratar con cualquiera de los siguientes proveedores: Impsat, Diveo, Telmex, Telefónica Data Colombia o Emtelco.

La capacidad requerida por cada entidad depende del número de estaciones y el tipo de aplicación utilizada. Para la fecha de publicación de este documento, las capacidades mínimas recomendadas son las siguientes:

- A. Para la conexión de estaciones que utilizan los servicios DCV, Subastas, Cuentas de Depósito, Cedec y Cenit se debe contar con un canal con capacidad mínima de 64Kbps. Este ancho de banda permitirá la conexión de hasta cuatro (4) estaciones de forma simultánea.
- B. Para la conexión de estaciones que utilizan el sistema SEN se debe contar con una capacidad de mínimo 64Kbps por cada estación que ingrese a dicho sistema.
- C. Para los dos casos anteriores, se recomienda como una “buena práctica” que el área de tecnología de cada entidad cuente con las herramientas, propias o de su proveedor de telecomunicaciones, necesarias para llevar un registro en línea del nivel de utilización de cada enlace. Este registro se puede utilizar para verificar que la utilización promedio de cada enlace se mantenga por debajo del 80% de su capacidad máxima. Mantener este margen de operación permite contrarrestar efectos de picos de tráfico que pueden causar una saturación del canal, lo que se refleja en una degradación de los tiempos de respuesta que experimentan los usuarios.



Ejemplo 1: Una entidad desea montar una infraestructura para la conexión de dos (2) estaciones al servicio SEN: En este caso, el enlace debe contar con una capacidad mínima de 128Kbps. Luego de instalar este enlace se debe llevar un monitoreo permanente del nivel de utilización del enlace para verificar que el nivel de utilización, durante el horario de operación del servicio, no supera en la mayor parte del tiempo los 102Kbps. Si se observa que el nivel de utilización tiende a ocupar la capacidad máxima del canal de debe realizar un proceso de diagnóstico para determinar si hay otras fuentes que estén generando tráfico adicional o consultar con el Banco de la República si la aplicación ha tenido un incremento en su requerimiento de ancho de banda debido, para el caso del SEN, a un mayor número de operaciones en el mercado. El Banco de la República estará atento a determinar los requerimientos de ancho de banda vigentes para cada servicio y publicará las actualizaciones necesarias de este documento.

Existe la posibilidad, para el caso de entidades que manejan un volumen bajo de operaciones en los servicios DCV, Subastas y CUD con un número reducido de estaciones, de utilizar como medio de comunicación un enlace de 64Kbps a través de líneas tipo RDSI-BRI que se adquieren con las telefónicas locales.

Igualmente, para las entidades que tienen un enlace dedicado contratado con un proveedor, existe la posibilidad de utilizar una línea RDSI-BRI como esquema de redundancia con capacidad máxima de 64Kbps. *Si está interesado en habilitar un esquema de contingencia por línea RDSI para su canal dedicado, contacte a su proveedor de servicio.*

2. Equipo de enrutamiento

Este equipo realiza la conexión lógica, a nivel de protocolo IP, entre la subred de la entidad financiera y la red central del Banco de la República, a través del canal de



comunicación previamente descrito. Este equipo puede ser de propiedad de la entidad financiera o puede ser suministrado por el proveedor del enlace en calidad de arriendo como parte del servicio.

3. Equipo de seguridad

Este equipo permite encriptar, autenticar y mantener la integridad de la información que se transmite entre la entidad y el Banco o viceversa. El equipo a utilizar debe ajustarse a las especificaciones que señala la Unidad de Seguridad de Informática del Banco de la República. Algunas entidades poseen un equipo SDU marca Cylink y otras entidades tienen un equipo VSU marca AVAYA.

NOTA:

El Banco de la República ha venido trabajando en la definición de una nueva plataforma de Redes Privadas Virtuales (VPN), para lo cual se ha centrado en la investigación y pruebas sobre plataformas VPN del estilo Hardware-Software buscando una mayor seguridad al extender el trayecto seguro o túnel y su administración hasta las máquinas mismas de los clientes.

Dado que la existencia de equipos para préstamos del Banco de la República se agotaron, recomendamos no adelantar nuevos requerimientos de dichas máquinas mientras el nuevo esquema sale en producción a finales de este año. Es importante aclarar que la migración a este nuevo esquema se hará gradualmente y no requerirá de equipos adicionales por parte de los Intermediarios Financieros.

Para las entidades que requieran ingresar por primera vez a alguno de los servicios SEBRA, se les solicita comunicarse con el Centro de Soporte Informático.



4. Segmento de red local

Es la porción de la red de datos de la entidad financiera que interconecta los computadores o estaciones cliente con los equipos de telecomunicaciones y seguridad antes mencionados. Cuando se habla de un segmento de red local, este puede corresponder a un simple cable de red UTP cruzado entre una sola estación y el equipo de encriptación o puede involucrar varios equipos de red que hacen parte de la infraestructura propia de la entidad.

La complejidad del segmento de red local estará determinada por las mismas necesidades de la entidad en lo relacionado con número de estaciones, ubicación física de los usuarios, políticas de seguridad de la empresa, etc. En la siguiente sección se describen algunos esquemas de segmentos de red local típicos.

5. Tarjetas de red de las estaciones SEN

Para las estaciones de SEN, la conexión de red entre la estación Sun y el equipo al cual esta se encuentre conectada directamente no debe ser autonegociada sino que debe estar forzada en ambos extremos:

- Si la estación Sun está conectada directamente al encriptador (SDU o VSU) la tarjeta de la estación debe quedar forzada a 10Mbps-half duplex.
- Si la estación se conecta a un concentrador o “hub”, la tarjeta de la estación debe quedar forzada a 10Mbps-halfduplex.
- Si la estación se conecta a un “switch”, ”, la tarjeta de la estación debe quedar forzada a 10Mbps-halfduplex. De igual forma, el puerto del “switch” también se debe configurar a 10Mbps-halfduplex sin autonegociación.

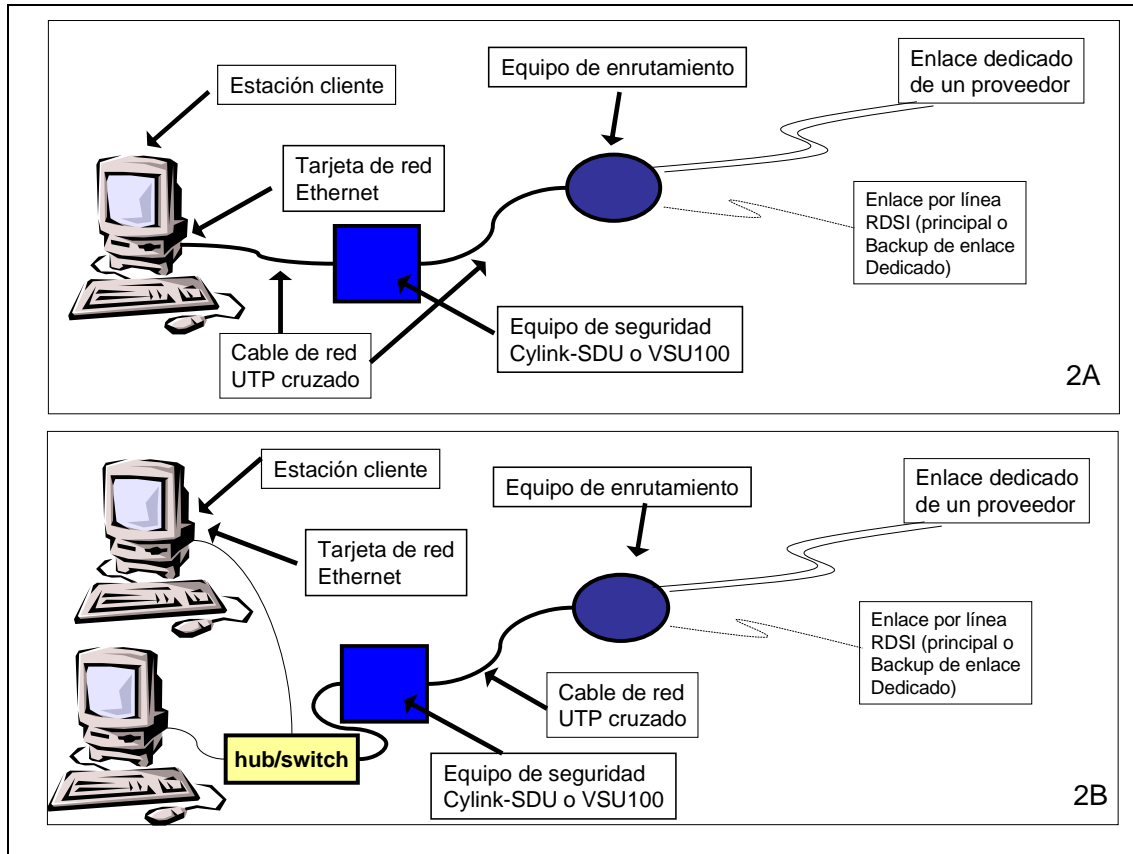


6. Software estaciones cliente

Todas las estaciones que utilizan los servicios electrónicos que presta el Banco de la República tienen instalado un software cliente que realiza todo el proceso de autenticación de los usuarios ante un servidor central. El servidor central, junto con los diferentes aplicativos que garantizan la autenticación de los usuarios en el momento de ingreso y sirven como interfaz única para todas las aplicaciones es denominado “Portal de servicios SEBRA”.

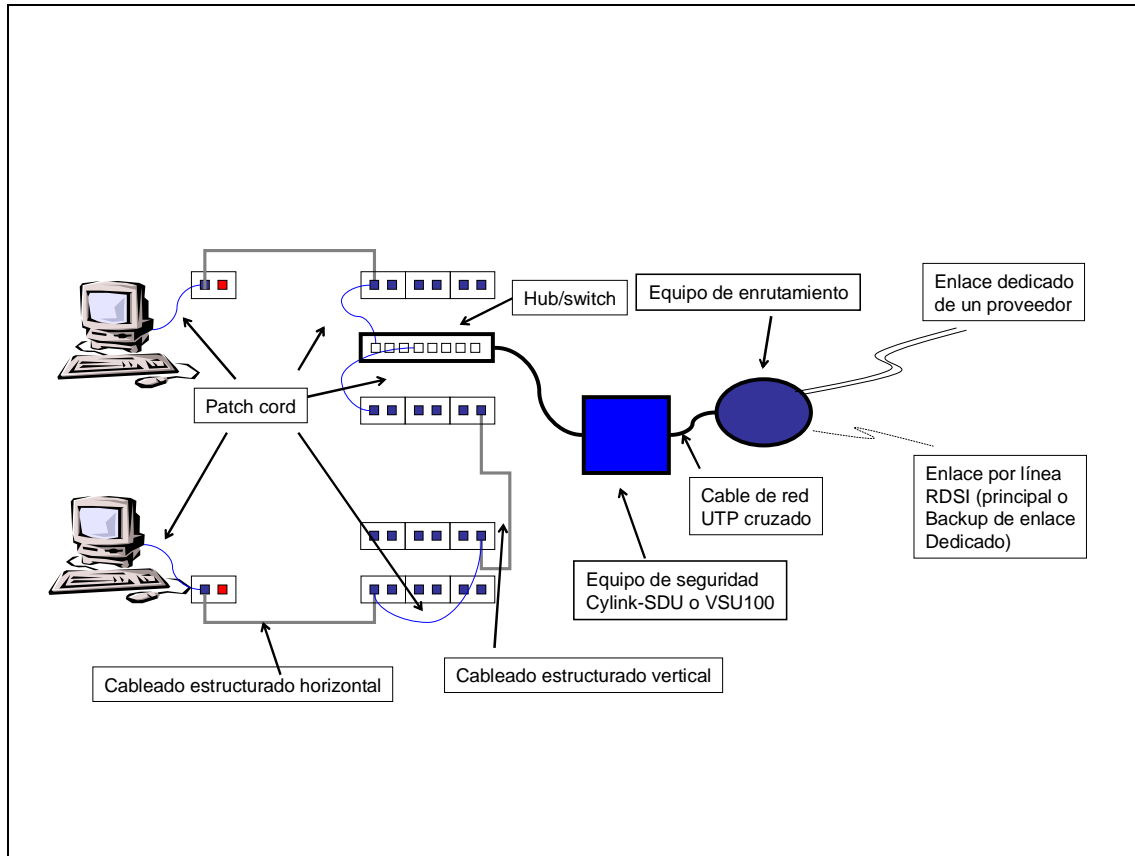
2.2 DIFERENTES ESQUEMAS DE SEGMENTO DE RED LOCAL

1. El esquema más sencillo corresponde a una entidad que sólo tiene una estación cliente de los servicios del Banco. En este caso puede tenerse una conexión directa por medio de un cable de red cruzado entre la estación y la interfaz interna del equipo de seguridad. La interfaz externa del equipo de seguridad suele conectarse de forma directa con el equipo de enrutamiento, también con un cable UTP cruzado. La gráfica 2 A es un ejemplo de este tipo de topología.
2. Cuando una entidad posee dos o más estaciones, ubicadas en una misma oficina y aisladas del resto de la red corporativa, estas pueden ser conectadas directamente a un concentrador (“hub”) o “switch” tipo Ethernet que las interconecta con la interfaz interna del equipo de seguridad. La interfaz externa del equipo de seguridad suele conectarse de forma directa con el equipo de enrutamiento, también con un cable UTP cruzado. La gráfica 2 B ilustra este tipo de topología.



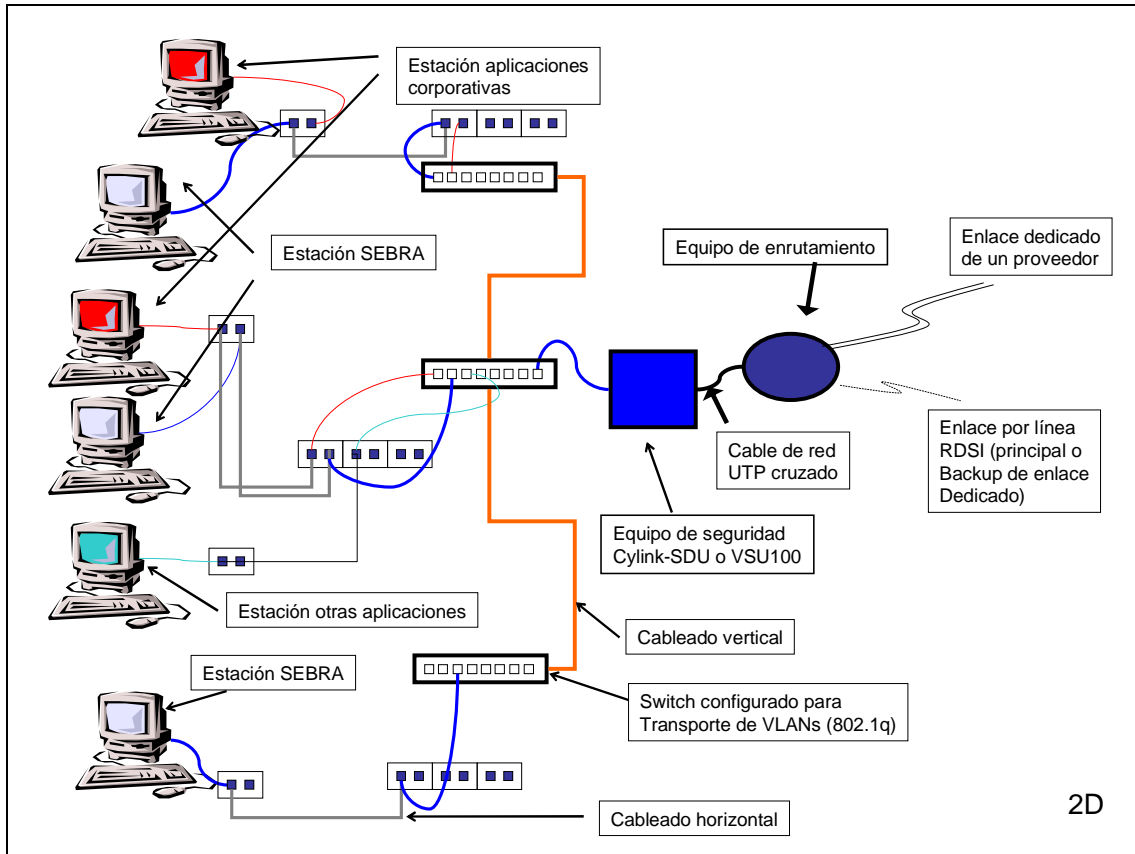
Gráfica 2

3. Cuando las estaciones están distribuidas en diferentes pisos de un mismo edificio se puede aprovechar la infraestructura de cableado estructurado de la entidad para extender hacia cada oficina los puntos de red del “hub” o “switch” mencionado en el numeral anterior. En este caso se debe garantizar, a través de una correcta administración de las **conexiones físicas de nivel 2**, que a ese “hub” o “switch” solo se conectarán las estaciones que deben tener acceso a los servicios electrónicos del Banco de la República. La gráfica 3 ilustra este esquema.



Gráfica 3

4. En el caso de entidades que tienen estaciones distribuidas en un mismo edificio, o en diferentes edificios que están interconectados por una infraestructura de switches, cableado UTP y fibra óptica, se puede utilizar la funcionalidad de redes virtuales, conocidas como VLANs (estándar IEEE802.1q), para transportar las conexiones de las diferentes estaciones con el segmento de red que conecta al equipo de seguridad. En este caso las estaciones que se conectan a los servicios electrónicos del Banco deben **aislarse a nivel lógico**, de las demás estaciones de la entidad financiera. La gráfica 4 ilustra este tipo de topología.



Gráfica 4

Existen entidades que debido a sus necesidades, cuentan con varias estaciones cliente ubicadas en sedes distantes, localizadas incluso en diferentes ciudades.

En estos casos se hace necesario implementar un esquema de comunicaciones que integre la plataforma de red propia de una entidad financiera con los equipos específicos para la conexión a los servicios del Banco de la República. Las consideraciones generales para implementar un esquema de este tipo se explican en la siguiente sección.



3 INTERCONEXIÓN RED CORPORATIVA - RED ACCESO SEBRA

3.1 PROBLEMÁTICA A RESOLVER

Cuando una entidad posee estaciones distribuidas en diferentes sedes y desea que todas ellas se comuniquen con los servicios del Banco de la República utilizando un único enlace de telecomunicaciones, la única opción es conectar las estaciones a través de la red corporativa que posea la entidad.

En este caso las estaciones cliente utilizadas para acceder a los servicios electrónicos del Banco de la República hacen parte de la red corporativa de la entidad y posiblemente puedan utilizar los servicios de red propios de la organización, tales como impresoras de red, servicios de correo electrónico, Internet etc.



Estas estaciones muy seguramente estarán cobijadas por las políticas de seguridad en redes propias de la entidad financiera, con el fin de evitar que personas externas a la organización aprovechen los recursos de comunicación de la plataforma de acceso SEBRA para ingresar de forma no autorizada a sus servicios de red.

Los factores antes mencionados hacen que la integración de las dos plataformas, la red corporativa de la entidad y los equipos de acceso a SEBRA, conformen una infraestructura compleja donde estarán involucrados:

1. Elementos de la red de área local de la entidad (cableado estructurado, concentradores, switches Ethernet nivel 2 o nivel 3)
2. Elementos de la red de área amplia de la entidad (enlaces entre sus oficinas, equipos de enrutamiento)
3. Elementos de seguridad de red de la entidad (Principalmente Firewalls)

La interacción de todos estos elementos requiere de un cuidadoso trabajo de análisis y diseño que es responsabilidad del área de tecnología de cada entidad.

3.2 CONSIDERACIONES GENERALES PARA LA IMPLEMENTACIÓN

Para facilitar la tarea de interconectar la red corporativa de las entidades financieras con la red de acceso a los servicios SEBRA y garantizar que el acceso de las estaciones cliente se realiza de manera flexible, eficiente y segura, la Subgerencia de Informática ha resumido los principales aspectos técnicos que han que tenerse en cuenta en el momento de diseñar el esquema de red a utilizar.

Estos aspectos técnicos son los siguientes:



1. Las estaciones que pertenecen a la red corporativa de la entidad deben tener una dirección IP propia de esta red.
2. El Banco de la República asigna un rango continuo de direcciones IP para cada una de las estaciones que se conectarán a la red de SEBRA. Estas direcciones IP hacen parte de un esquema de direccionamiento privado acorde con las recomendaciones del RFC 1918. La utilización de estas direcciones es un requisito indispensable para tener acceso a los servicios electrónicos que ofrece el Banco de la República.
3. Los servicios prestados por el Banco de la República se acceden conectándose a un grupo de servidores que están instalados en las subredes IP **172.16.0.0**, **192.168.8.0**, **192.168.14.0**, **192.168.15.0** y **192.168.61.0**.

Nota Importante: En la red corporativa del cliente no deben existir ni conocerse las subredes IP antes mencionadas (**172.16.0.0**, **192.168.8.0**, **192.168.14.0**, **192.168.15.0** y **192.168.61.0**). Si la red corporativa incluye estas direcciones o se conecta con otras redes que utilizan este direccionamiento, no se puede instalar esta topología y las estaciones SEBRA deben formar un segmento Ethernet totalmente independiente de la red corporativa de la entidad financiera similar al presentado en las gráficas 3 y 4 de este documento.

4. Por cada estación que se conecta a los servicios electrónicos vía el portal SEBRA, se requiere una dirección IP en el rango asignado por el Banco de la República para poder establecer una relación fija de correspondencia uno a uno.



Para lograr que las estaciones conectadas a la red corporativa, con direcciones IP de la entidad financiera, se vean desde el Banco de la República como estaciones con direcciones IP válidas, es indispensable que en la red de telecomunicaciones de la entidad financiera se implemente un mecanismo de traducción de direcciones *NAT (Network Address Translation) uno a uno*, para que reemplace la dirección IP origen contenida en los datagramas que envían las estaciones cliente por una dirección IP dentro del rango mencionado en el punto 2.

5. El equipo que realiza la función NAT debe poseer dos interfaces Ethernet (Interna y Externa). La interfaz interna del NAT se debe conectar a la red corporativa del cliente. La interfaz externa del NAT se debe conectar con la interfaz privada del equipo de seguridad. El equipo de seguridad puede ser una *SDU Cylink (Secure Domain Unit – interfaz Clear)* o una *VSU100ZR (Virtual Private Network – Interfaz Private)* de Avaya.
6. El equipo que realiza la función NAT constituye la frontera entre la red corporativa del cliente y la red de acceso con el Banco de la República. Para proteger la red corporativa del cliente de posibles intrusos, se recomienda que este equipo también realice funciones básicas de Firewall.
7. La interfaz pública del equipo de seguridad, ya sea una *SDU Cylink (Secure Domain Unit – Interfaz Cipher)* o un *VSU100ZR (Virtual Private Network – Interfaz Public)* marca Avaya, se debe conectar con un cable de red UTP cruzado a la interfaz Ethernet del enrutador que recibe el enlace dedicado que comunica con el Banco de la República.



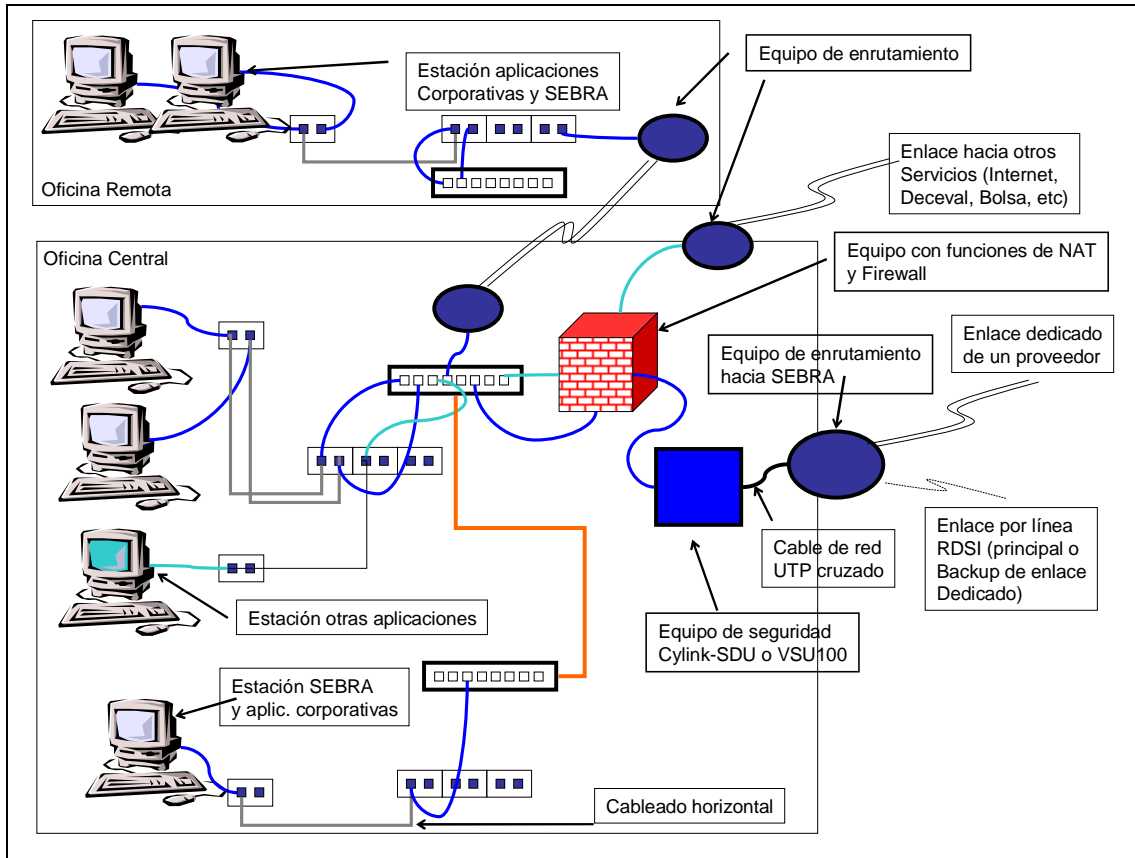
NOTA:

El Banco de la República ha venido trabajando en la definición de una nueva plataforma de Redes Privadas Virtuales (VPN), para lo cual se ha centrado en la investigación y pruebas sobre plataformas VPN del estilo Hardware-Software buscando una mayor seguridad al extender el trayecto seguro o túnel y su administración hasta las máquinas mismas de los clientes.

Dado que la existencia de equipos para préstamos del Banco de la República se agotaron, recomendamos no adelantar nuevos requerimientos de dichas máquinas mientras el nuevo esquema sale en producción a finales de este año. Es importante aclarar que la migración a este nuevo esquema se hará gradualmente y no requerirá de equipos adicionales por parte de los Intermediarios Financieros.

Para las entidades que requieran ingresar por primera vez a alguno de los servicios SEBRA, se les solicita comunicarse con el Centro de Soporte Informático.

La gráfica No. 5 presenta un ejemplo típico de topología donde se integra la red corporativa de una entidad financiera con la red de acceso a SEBRA. La topología exacta que tendrá una entidad financiera depende de sus características propias.



Gráfica 5

3.3 CONFIGURACIÓN EQUIPOS CON FUNCIÓN DE FIREWALL

Si el equipo que realiza las funciones de NAT tiene funciones de Firewall o la entidad dispone de un equipo dedicado para esta función, las reglas de validación deben tener en cuenta lo siguiente:

3.3.1 Reglas generales para todas las estaciones

Las siguientes reglas de Firewall deben ser configuradas para todas las estaciones cliente que posea la entidad, sin importar el tipo de aplicación o servicio que utilicen:



Servicio	Tipo	Origen	Destino	Puerto	Nombre del Servidor
SEBRA	TCP	Estación cliente	172.16.107.60	30.000 – 30.006	Sebra
SEBRA (Versiones)	TCP	192.168.61.1	Estación cliente DCV/Cud	7.730	
SEBRA (Versiones)	TCP	192.168.61.1	Estación Cliente SEN	1024 en adelante	
WEB SEBRA	TCP	Estación cliente	192.168.14.4	80, 3.000, 110 y 25	Websebra
HTRANS	TCP	Estación cliente	192.168.15.11 y 192.168.15.12	80, 443, 15500	Sweb1a Sweb2b
PKI	TCP	EC	192.168.15.6 192.168.15.9	389, 636 y 640 829	Spki-1 Ca-ppal

Estas reglas corresponden a la aplicación de autenticación de los usuarios ante el portal de acceso SEBRA y otras aplicaciones comunes a todos los servicios electrónicos ofrecidos por el Banco.



3.3.2 Reglas para estaciones que utilizan aplicaciones DCV, Omesys y Cud

Servicio	Tipo	Origen	Destino	Puerto	Nombre del Servidor
CUD	TCP	EC	192.168.15.11	9001 y 7777	Sweb1a
DCV/SUBASTAS	TCP	EC	192.168.14.27	80, 443	Sat1a

3.3.3 Reglas para estaciones que utilizan aplicaciones CEDEC-CENIT

Servicio	Tipo	Origen	Destino	Puerto	Nombre del Servidor
CEDEC	TCP	EC	192.168.14.214	8.000 – 8.001	Sach1a
CEDEC Pruebas	TCP	EC	192.168.14.215	8.000 – 8.001	Sach2b
CENIT	TCP	EC	192.168.14.214	8.002 – 8.003	Sach1a
CENIT Pruebas	TCP	EC	192.168.14.215	8.002 – 8.003	Sach2b



3.3.4 Reglas para estaciones que utilizan aplicación SEN

Servicio	Tipo	Origen	Destino	Puerto
SEN	TCP	EC	192.168.8.2 – 4	1.500, 1.601-1.625 Y 80
VERSIONES CLIENTE SEN	TCP	192.168.63.50	ECSSEN	21 (FTP) y 23 (TELNET)

Nota Importante: Cuando la entidad financiera utilice un equipo con funciones de firewall dentro del esquema de comunicaciones propio, debe verificar la existencia de las versiones adecuadas de los siguientes archivos en las estaciones del cliente:

- *c:\sebra\sebra\system\ClientConnect.class, tamaño 17 Kb, fecha 10-08-99*
- *c:\sebra\sebra\util\CopyThread.class, tamaño 2Kb, fecha 21/01/99*

Si no cuenta con estos archivos debe solicitarlos al Centro de Soporte Informático del Banco de la República.



3.4 ASIGNACIÓN DE DIRECCIONES IP

Con el fin de facilitar la administración de las direcciones IP que se utilizan en la red de acceso SEBRA, se deben tener en cuenta las siguientes recomendaciones. Para facilitar su comprensión, se presentan la recomendaciones por medio de un ejemplo:

Se supone que se asignó a una entidad financiera la subred **172.31.115.0** y se definió la máscara de subred como 255.255.255.0:

- El enrutador donde se recibe el canal de comunicaciones del proveedor de telecomunicaciones debe configurarse con la primera dirección del rango asignado: **172.31.115.1**.
- El equipo de seguridad debe configurarse con la segunda dirección válida del rango asignado: **172.31.115.2**.
- A la interfaz externa del equipo que hace las funciones *NAT* se debe asignar la última dirección válida del rango asignado: **172.31.115.254**.
- Para configurar las estaciones que accesan las diferentes aplicaciones, se puede utilizar el resto de direcciones válidas en este rango. Sin embargo, con el objetivo de tener toda la información de las estaciones, el Banco realiza el proceso de asignación para cada estación en particular.

Para tal efecto, cuando una entidad financiera desea instalar una nueva estación, simplemente debe informar al Centro de Soporte Informático del Banco de la República sobre la nueva estación, los usuarios que la utilizarán y las aplicaciones que allí funcionarán. Las personas del Banco informarán a la entidad, los datos de configuración de dirección IP para la estación.