UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE UNA NUBE DE SERVICIOS CORPORATIVA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

NILCER FERNÁNDEZ FUSTER

PROMOCIÓN 2007-1

LIMA-PERÚ

2013

IMPLEMENTACIÓN DE UNA NUBE DE SERVICIOS CORPORATIVA

A mis padres y familia por su apoyo incondicional
por mostrarme que nada es imposible y que con
perseverancia se pueden lograr las metas.
A todos mis amigos que me brindaron su amistad
y ayuda desinteresada.

SUMARIO

Nube de servicios corporativa, es un modelo para habilitar convenientemente accesos en la demanda a una red para compartir un conjunto de recursos (servidores, aplicaciones y servicios) que pueden ser implementados y liberados rápidamente.

Es importante llevar a cabo la implementación de la nube de servicios para cumplir con la regulación de la Superintendencia de Banca y Seguros (SBS), evitando de esta manera cualquier observación en la operación del Banco.

Por este motivo el presente informe muestra la metodología empleada por una corporación para la implementación de medidas correctivas en el diseño y arquitectura de red con la finalidad de brindar servicios a más de dos negocio, cumpliendo las normas de seguridad y la regulación local.

El diseño y arquitectura de red se desarrolla a partir de la protección de Red con la implementación de control de accesos (*firewalls*), sistemas de detección y prevención de intrusos y la segmentación de red.

Asimismo, se muestra la metodología *Project Management Institute* (PMI) para la realización del proyecto de implementación de la nube de servicios corporativa.

ÍNDICE

INTRODUCCIÓN

En los últimos años los servicios de la nube están emergiendo como un modelo atractivo de proporcionar tecnología de información (TI) para grandes y pequeñas empresas tanto en sectores públicos como privados.

Para el desarrollo del presente informe se ha realizado un estudio de este nuevo modelo de servicios, estudiando sus aspectos teóricos y fundamentales, analizando las implementaciones con las que al día de hoy podemos encontrar en el mercado. Deberemos tener en cuenta los riesgos que deberemos asumir en la adopción del modelo, aportando soluciones para mitigarlos de la forma más eficiente posible.

El presente informe muestra la aplicación de la metodología empleada para la implementación de la arquitectura de red con la finalidad de reducir los posibles riesgos y observaciones que podría atraer a la corporación adoptar el modelo de nube de servicios corporativa basados en las definiciones *Cloud* del National Institute of Standars and Technology (NIST), así como el desarrollo del proyecto siguiendo las buenas prácticas de Project Managment Institute (PMI), a través del Project Managment Body of Knowledge (PMBOK).

Cabe recalcar que no es parte del alcance de este estudio la elaboración de políticas y procedimientos.

CAPITULO I
MARCO TEÓRICO CONCEPTUAL

1.1 Conceptos de seguridad de la información

Antes de iniciar con el desarrollo del informe debemos definir los conceptos de la seguridad de la información Confidencialidad, Integridad y Disponibilidad, conocidos como la triada CID tal como se muestra en la Figura 1.1, el orden de las letras podrían variar en el acrónimo (algunos prefieren ICD), pero el concepto esencial se mantiene.

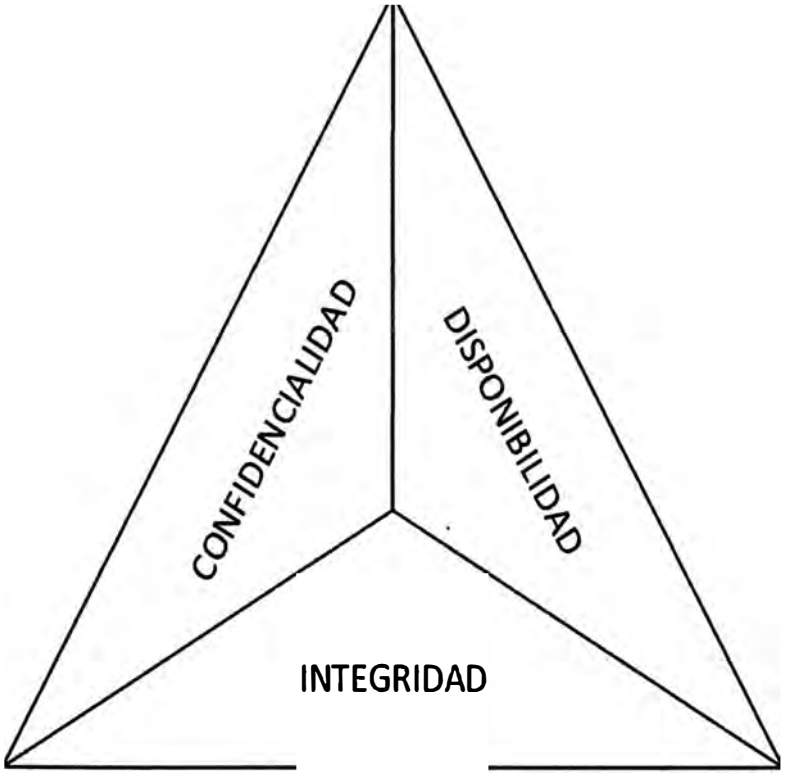

Figura 1.1 Triada CID

Confidencialidad, Integridad y Disponibilidad trabajan en conjunto para asegurar la información y tener los sistemas seguros, es incorrecto asumir que cada uno de los conceptos de la triada sea más importante que la otra. Existen los conceptos opuestos que fuerzan al CID. Como se muestra en la Figura 1.2, estos son Exposición, Alteración y Destrucción (EAD).

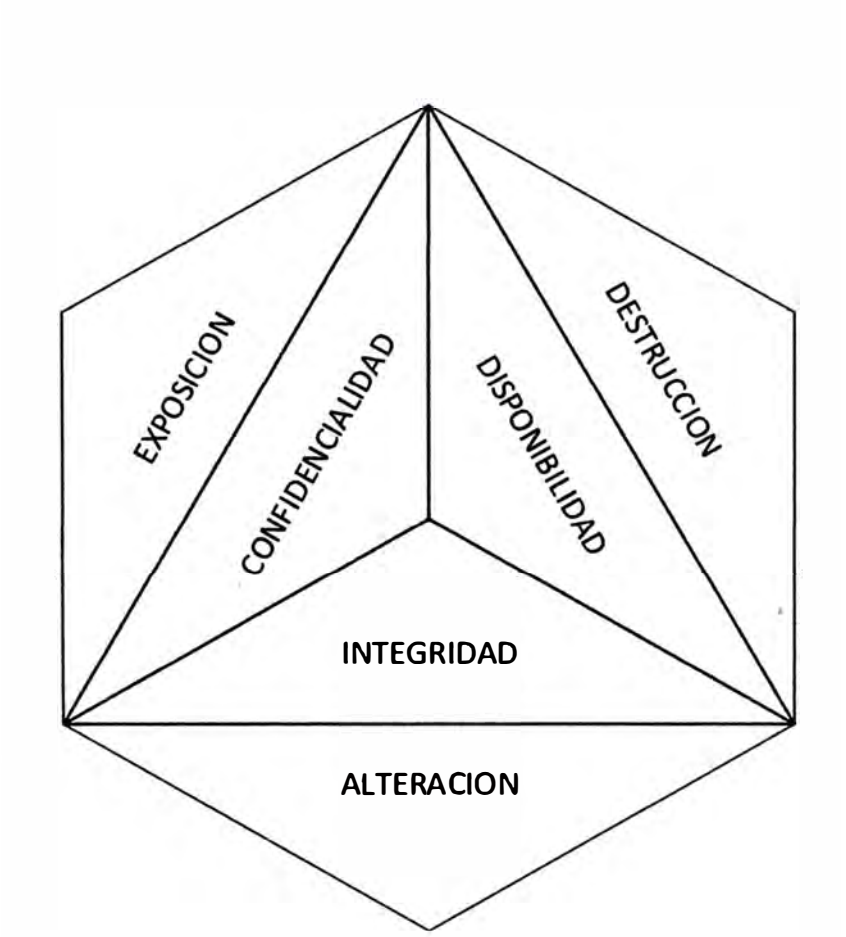

Figura 1.2 Conceptos opuestos que fuerzan al CID (EAD)

1.1.1 Confidencialidad

La confidencialidad busca prevenir la exposición de la información a entes no autorizados, mantiene la información secreta. La información solo debe ser accesible a los usuarios que tienen un acceso formal y aprobado.

1.1.2 Integridad

La integridad busca prevenir la modificación de la información por entes no autorizados. Existen 2 tipos de integridad: integridad de la información y la integridad de los sistemas. Por ejemplo, si una persona accede a la base de datos de los sistemas para alterar la información, estaría violando la integridad de la información. Sin embargo, si instala un software malicioso en el sistema para permitir un acceso futuro del tipo backdoor, estaría violando la integridad de los sistemas.

1.1.3 Disponibilidad

La disponibilidad asegura que la información esté disponible cuando sea necesitada, los sistemas necesitan estar disponibles para el uso normal del negocio. Un ejemplo de un ataque sobre la disponibilidad podría ser ataque DoS en el cual existe una denegación de Servicio lo cual traería como consecuencia la "destrucción" del servicio.

1.2 Conceptos de servicios en la Nube

1.2.1 Definición

Según el NIST (National Institute of Standars and Technology), el *Cloud Computing* es un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda en red a un conjunto compartido de recursos de computación configurables y compartidos por ejemplo: redes, servidores, equipos de almacenamiento, aplicaciones y servicios, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de gestión reducido o interacción mínima con el proveedor del servicio.

1.2.2 Características

Para poder entender de una manera rápida y sencilla cuales son las claves del concepto del *Cloud Computing*, se recurre a una serie de características principales que lo diferencian de los sistemas tradicionales de explotación de las TIC. Entre las características asociadas al *Cloud Computing* se encuentran en la Figura 1.3:

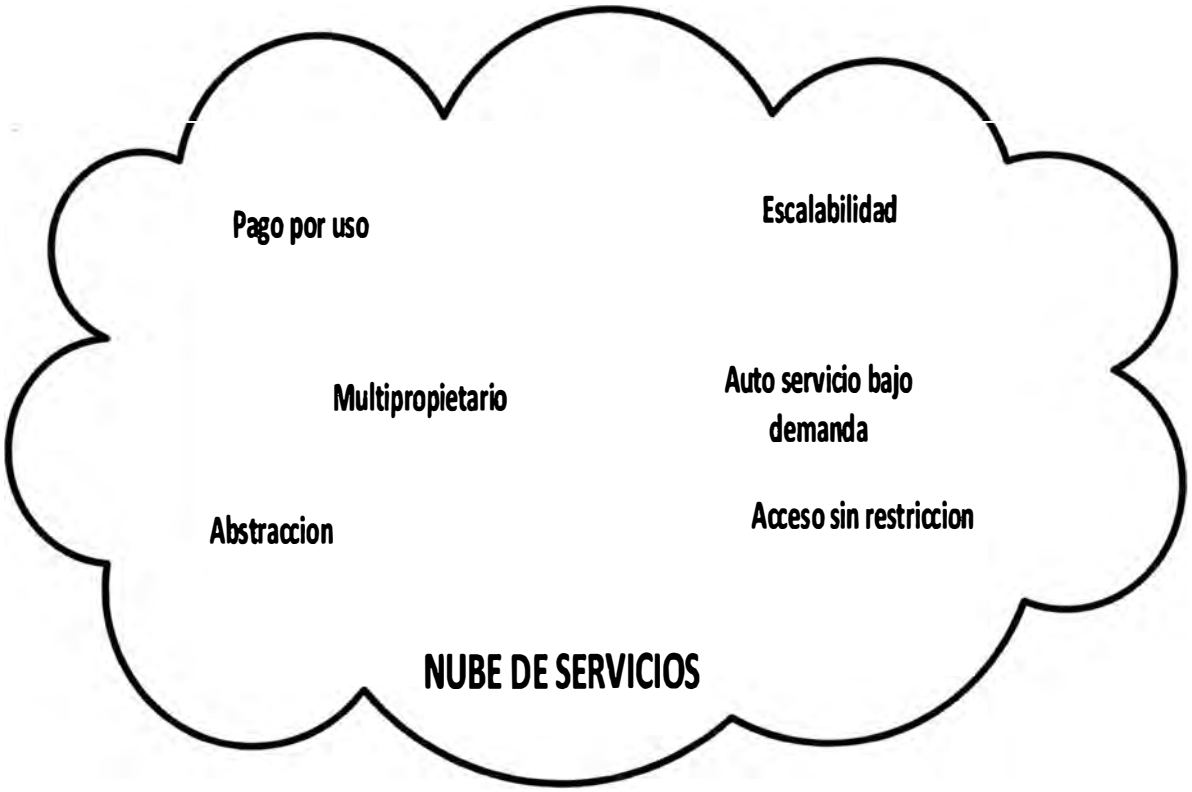

Figura 1.3 Características asociadas a la nube de servicios

a) Pago por uso: Una de las características principales de las soluciones *Cloud* es el modelo de facturación basado en el consumo, es decir, el pago que debe abonar el cliente varía en función del uso que se realiza del servicio *Cloud* contratado.

b) Abstracción: Característica o capacidad de aislar los recursos informáticos contratados al proveedor de servicios *Cloud* de los equipos informáticos del cliente. Esto se lleva a cabo gracias a la virtualización, con lo que los usuarios no requieren de

personal dedicado al mantenimiento de la infraestructura, actualización de sistemas, pruebas y demás tareas asociadas que quedan de lado del servicio contratado.

c) Agilidad en la escalabilidad: Característica la cual consiste en aumentar o disminuir las funcionalidades ofrecidas al cliente, en función de sus necesidades puntuales sin necesidad de nuevos contratos ni penalizaciones. De la misma manera, el coste del servicio asociado se modifica también en función de las necesidades puntuales de uso de la solución. Esta característica, relacionada con el pago por uso, evita los riesgos inherentes de un posible mal dimensionamiento inicial en el consumo o en la necesidad de recursos.

d) Multiusuario: Capacidad que otorga el *Cloud* la cual permite a varios usuarios compartir los medios y recursos informáticos, permitiendo la optimización de su uso.

e) Autoservicio bajo demanda: Esta característica permite a los usuarios acceder de manera flexible a las capacidades de computación en la nube de forma automática a medida que las requiera.

f) Acceso sin restricciones: Consiste en la posibilidad ofrecida a los usuarios de acceder a los servicios contratados de *Cloud Computing* en cualquier lugar, en cualquier momento y con cualquier dispositivo que disponga de conexión a redes de servicio IP.

1.2.3 Clasificación de soluciones de Cloud Computing

Las soluciones de *Cloud Computing* que tenemos en el mercado en la actualidad admiten diferentes clasificaciones según el aspecto que se tenga en cuenta para realizar dicha clasificación.

Se definen tres características fundamentales que marcan la clasificación de las soluciones *Cloud*: familias, formas de implementación y agentes intervinientes.

Estas tres características, junto con sus diferentes tipos de soluciones asociadas, se pueden representar en un cubo de tres dimensiones, tal y como se muestra en la Figura 1.4.

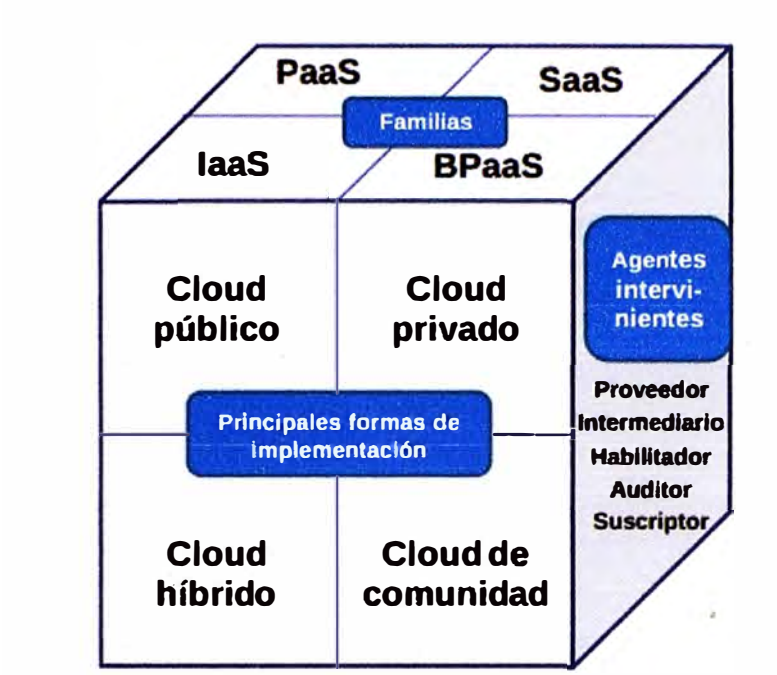

Figura 1.4 Clasificación de Soluciones en la Nube

(Fuente: ONTSI)

Mediante la combinación de estas tres dimensiones se detallan los diferentes tipos de *Cloud Computing* existentes en el mercado, así como sus principales agentes.

a) Por familias *Cloud* (modelos de servicio)

- **Infraestructure as a Service (IaaS)**

Familia de *Cloud Computing*, la cual pone a disposición del cliente el uso de la infraestructura informática (capacidad de computación, espacio de disco y bases de datos entre otros) como un servicio

Los usuarios que optan por este tipo de familia *Cloud* en vez de adquirir o dotarse directamente de recursos, como pueden ser los servidores, el espacio del centro de datos o los equipos de red optan por la externalización en busca de un ahorro en la inversión en sistemas TI

Con esta externalización, las facturas asociadas a este tipo de servicios se calculan en base a la cantidad de recursos consumidos por el cliente, basándose así en el modelo de pago por uso.

- **Software as a Service (SaaS):**

Familia de *Cloud Computing* la cual entrega aplicaciones como servicio, siendo un modelo de despliegue de software mediante el cual el proveedor ofrece licencias de su aplicación a los clientes para su uso como un servicio bajo demanda.

Los proveedores de los servicios SaaS pueden tener instalada la aplicación en sus propios servidores web permitiendo a los clientes acceder, por ejemplo, mediante un navegador web, o descargar el software en los sistemas del contratante del servicio.

En este último caso, se produciría la desactivación de la aplicación una vez finalice el servicio o expire el contrato de licencia de uso.

- **Platform as a Service (PaaS):**

Familia de *Cloud Computing* la cual entrega, como un servicio, de un conjunto de plataformas informáticas orientadas al desarrollo, testeo. Despliegue, *hosting* y mantenimiento de los sistemas operativos y aplicaciones propias del cliente.

Las principales características asociadas al Platform as a Service como solución *Cloud* son:

- Facilita el despliegue de las aplicaciones del usuario, sin el coste y la complejidad derivados de la compra y gestión del hardware y de las capas de software asociadas.
- Ofrece a través de redes de servicio IP todos los requisitos necesarios para crear y entregar servicios y aplicaciones web.

- **Business Process as a Service (BPaaS)**

Familia de *Cloud Computing* consistente en la provisión como servicio de procesos de negocio end-to-end altamente estandarizados a través de su entrega dinámica, la modalidad de pago por uso y los modelos de consumo de autoservicio bajo demanda. Su característica principal es que los recursos utilizados mediante esta solución para ejecutar los procesos de negocio, son compartidos entre los diferentes usuarios del proveedor. En muchos casos, este hecho proporciona un aporte de valor al negocio.

b) Por principales formas de implementación (formas de integración y explotación)

- **Cloud Público (Externo)**

Forma de implementación que se caracteriza por la oferta de servicios de computación virtualizados (bases de datos, sistemas operativos, plataformas de desarrollo, aplicaciones, etc.) por parte de los proveedores para múltiples clientes, accediendo éstos a dichos servicios a través de Internet o redes privadas virtuales (VPNs).

Como características inherentes a esta forma de implementación podemos citar las siguientes:

- Reducido plazo de tiempo para la disponibilidad del servicio.
- No se requiere llevar a cabo inversión monetaria para su implementación.
- Permite la externalización a un proveedor de servicios *Cloud* de todas las funciones básicas de la empresa.
- Posibilita el aprovechamiento de la infraestructura de los proveedores de servicios, permitiendo adicionalmente una alta escalabilidad y flexibilidad en la modificación del dimensionamiento del servicio.

- Favorece la utilización de conjuntos de software estándar.
- Lleva asociadas unas cuotas iniciales de pago más bajas que el resto de implementaciones. Adicionalmente los costes del *Cloud* público son variables, cumpliendo el principio de pago por uso.
- La información corporativa se encuentra alojada en la nube pública junto a la del resto de clientes del proveedor, lo que implica, además de no poder tener localizada físicamente dicha información, imponer al proveedor una serie de requisitos de alta exigencia en temas de seguridad y protección de datos.

➢ **Cloud Privado (Interno)**

Forma de implementación caracterizada por el suministro por parte del proveedor de entornos virtualizados que pueden ser implementados, usados y controlados por la misma empresa contratante del servicio. Esto indica no solo que la solución *Cloud* puede ser administrada por la organización contratante, por el proveedor o por un tercer actor; sino que puede existir en las instalaciones propias del cliente o fuera de las mismas.

Como características propias de esta forma de implementación se enumeran las siguientes:

- Reducido plazo de tiempo para la puesta en servicio y una alta flexibilidad en la asignación de recursos.
- Al contrario que el Cloud público, requiere de inversión económica para la implementación de la solución contratada.
- Lleva asociados sistemas y bases de datos locales.
- Ofrece la posibilidad de aprovechar el personal existente y las inversiones en sistemas de información realizadas con anterioridad.
- Implica más especificidad en la solución adquirida, ya que está diseñada para ajustarse a las necesidades propias de la empresa contratante.
- Permite disponer de un control total de la infraestructura, de los sistemas y de la información corporativa tratada por éstos.
- Facilita el control y la supervisión de los requisitos de seguridad y protección de la información almacenada.

➢ **Cloud de comunidad**

Se trata de *Clouds* utilizados por distintas organizaciones cuyas funciones y servicios sean comunes, permitiendo con ello la colaboración entre grupos de interés.

Ejemplos de esta forma de implementación son los *Clouds* de comunidades de servicios de salud (en inglés, healthcare community *Cloud*) para facilitar el acceso aplicaciones e información crítica de carácter sanitario, y los *Clouds* de comunidad

gubernamentales (G*overnment Community Cloud*) para facilitar el acceso a recursos de interoperabilidad entre organismos públicos y Administraciones Públicas.

Al analizar un *Cloud de comunidad*, se debe considerar que, en principio, sus fortalezas y debilidades se sitúan entre las del privado y las del público. En general, el conjunto de recursos disponibles con un *Cloud de comunidad* es mayor que en el privado, con las ventajas evidentes que ello conlleva en términos de elasticidad. Sin embargo, la cantidad de recursos es menor que los existentes en una solución de *Cloud* público, limitando la elasticidad respecto a dicho *Cloud* público. Por otra parte, el número de usuarios de este tipo de nube es menor que los de la nube pública, lo que la dota de mayores prestaciones en cuestiones de seguridad y privacidad.

- **Cloud Híbrido**

Forma de implementación cuya infraestructura *Cloud* se caracteriza por aunar dos o más formas de *Clouds* (privado, comunitario o público), los cuáles continúan siendo entidades únicas interconectadas mediante tecnología estandarizada o propietaria, tecnología que permite la portabilidad de datos y aplicaciones por ejemplo el rebalanceo de cargas entre nubes. Una entidad que emplee esta forma de implementación se podría beneficiar de las ventajas asociadas a cada tipo de *Cloud*, disponiendo con ello de una serie de características adicionales las cuales son:

- Ofrece una mayor flexibilidad en la prestación de servicios de TI, al mismo tiempo que se mantiene un mayor control sobre los servicios de negocio y de datos.
- Con una solución de *Cloud* híbrido, al igual que en los casos detallados anteriormente, se consigue una rápida puesta en servicio.
- Implica mayor complejidad en la integración de la solución *Cloud*, como consecuencia de ser una solución que se compone de dos formas distintas de implementación de servicios en la nube.
- Permite integrar las mejores características de las dos formas de implementación *Cloud*, en cuanto al control de los datos y a la gestión de las funciones básicas de la entidad.
- Posibilita la selección por parte del proveedor, de infraestructura escalable y flexible, permitiendo una alta agilidad en el redimensionamiento de la solución.
- Permite el control interno de los servicios *Cloud* desde la propia entidad.

c) Por agentes intervinientes en el negocio

Como principales agentes intervinientes en el negocio se pueden definir: el proveedor, el intermediario, el habilitador, el auditor y el suscriptor, los cuales se muestran en la Figura 1.5.

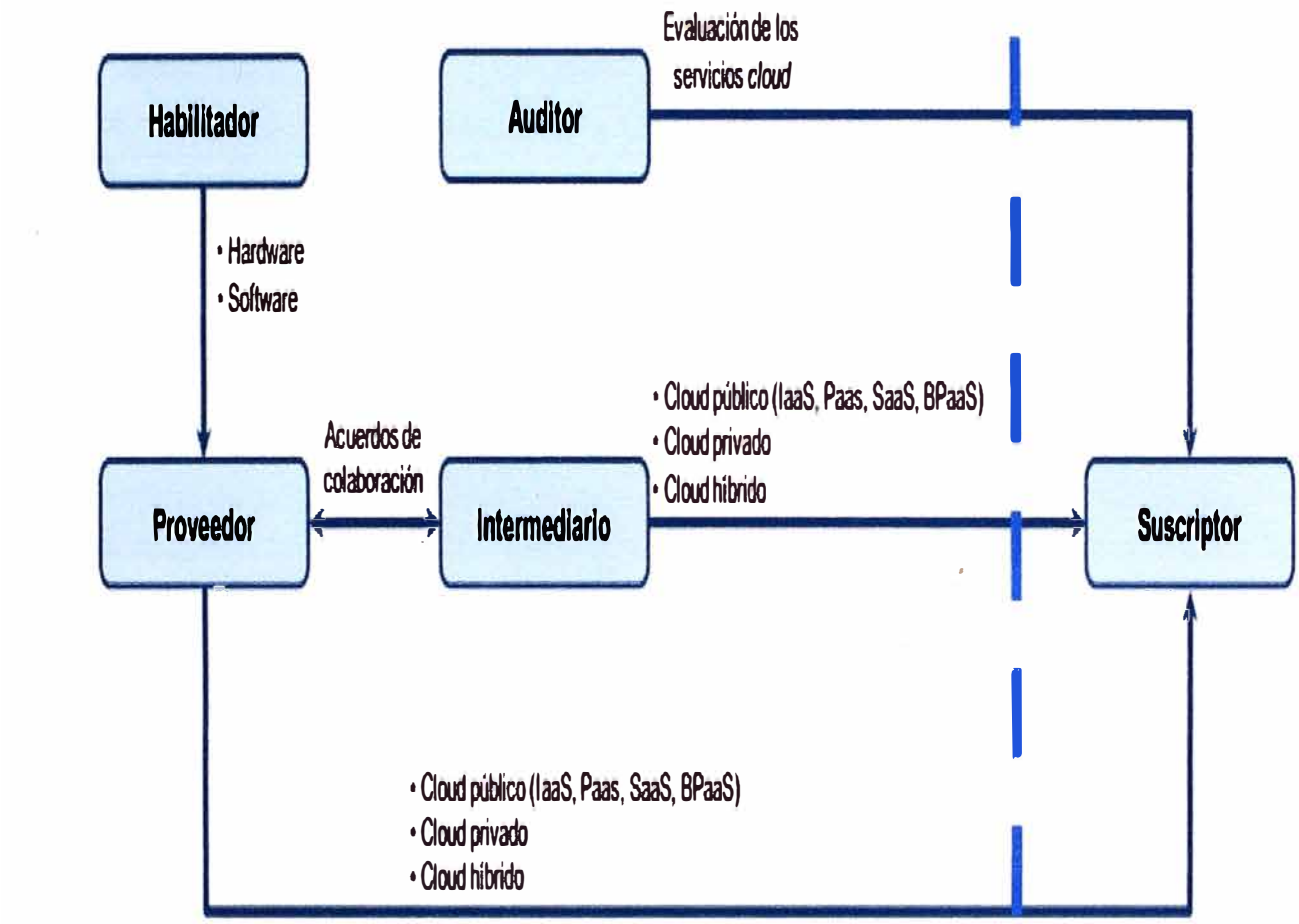

Figura 1.5 Diagrama de bloques del proceso

(Fuente: ONTSI)

- **Proveedor**

El proveedor presta servicios a través de la nube a suscriptores o intermediarios, es decir, el servicio ofertado por la empresa proveedora al cliente, ya sea de forma directa o a través de un intermediario.

- **Intermediario**

El intermediario presta servicios de intermediación entre los usuarios finales y los proveedores en un mercado dinámico de oferta y demanda como es el *Cloud Computing* se pueden mencionar por ejemplo, los servicios frontales o las intermediaciones extremo-extremo.

- **Habilitador**

Se trata de un agente proveedor típicamente enfocado al mercado de proveedores de *Cloud*. Son empresas que proveen de software y hardware a proveedores de servicios *Cloud*, para que éstos desarrollen y ofrezcan al usuario servicios en la nube.

- **Auditor**

El auditor es el agente encargado de llevar a cabo las evaluaciones independientes de los servicios en la nube, de las operaciones asociadas a los sistemas de información, del rendimiento y de la seguridad en el uso de la solución Cloud.

- **Suscriptor**

La figura denominada suscriptor se corresponde con el usuario contratante de los servicios *Cloud*, por lo que se puede identificar a esta figura como el cliente de los proveedores, los intermediarios y los auditores.

1.3 Seguridad en Redes y Telecomunicaciones

La seguridad en redes y telecomunicaciones abarca las estructuras, métodos de transmisión formatos de transporte y las medidas de seguridad usadas para proporcionar la confidencialidad, integridad y disponibilidad de las transmisiones sobre las redes de comunicaciones públicas y privadas.

La seguridad en las Redes como todos los controles es lo mejor y más efectivo si son aplicados proactivamente, si se espera que las vulnerabilidades se materialicen y se apliquen controles bajo condiciones de crisis siempre será más costoso y menos efectivo que planificar y administrar políticas, procedimientos y tecnologías de seguridad en las redes.

1.3.1 Conceptos de Redes de Comunicación

Las redes de comunicación son usualmente descritas en términos de capas. Existen muchos modelos de capas; los que se usan comúnmente son:

- Modelo de referencia OSI, estructurado en 7 capas (capa Física, capa de Enlace, capa de Red, capa de Transporte, capa de Sesión, capa de Presentación y capa de Aplicación).
- Modelo TCP/IP, estructurado en 4 capas (capa de Enlace, capa de Red, capa de Transporte y capa de Aplicación).

Una característica común para ambos modelos y altamente relevante desde una perspectiva de seguridad es la encapsulación. Esto significa que no solo las capas operan independientemente una de otra pero también están aisladas.

a) Modelo OSI

Las siete capas del modelo OSI fueron definidas en 1984 y publicadas como un estándar internacional (ISO/IEC 7498-1). La última revisión de este estándar fue en 1994.Figura 1.6

Figura 1.6 Arquitectura del modelo OSI

b) Modelo TCP/IP

El departamento de defensa de Estados Unidos de Norteamérica desarrolló el modelo TCP/IP el cual es muy similar al modelo OSI, pero con menos capas tal como se muestra en la Figura 1.7 la capa de Acceso de red corresponde a todo lo requerido para implementar Ethernet. La capa de Internet incluye todo lo que se requiere para mover data entre redes, corresponde al protocolo IP pero también al ICMP.

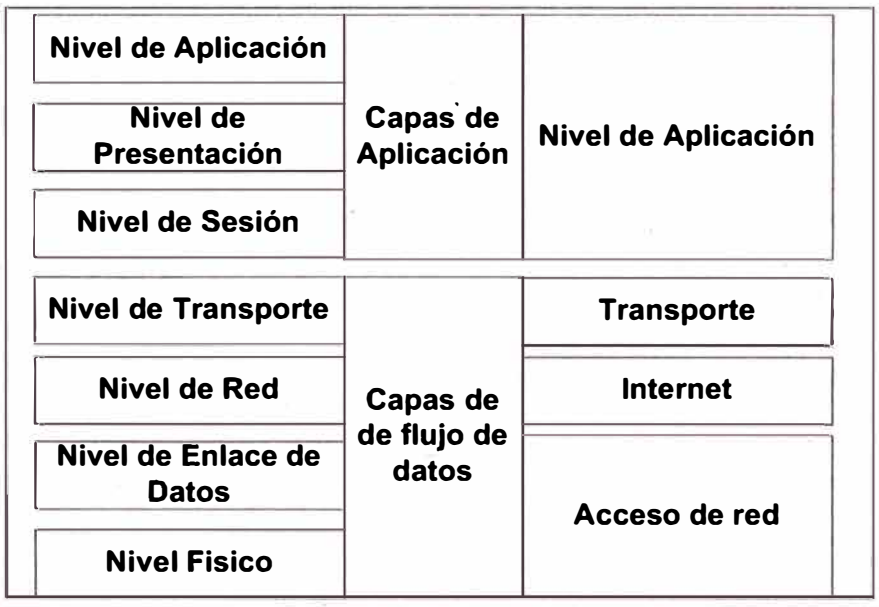

Figura 1.7 Arquitectura TCP/IP

La capa de Transporte incluye todo lo que se requiere para mover data entre aplicaciones. Esto corresponde al TCP y UDP. La capa de Aplicación cubre todo lo que se refiere a las capas del modelo Sesión, Presentación y Aplicación.

c) Protocolo de Internet (IP)

El protocolo de Internet (IP) es responsable de llevar paquetes desde los hosts origen hacia el destino, ya que es un protocolo no confiable no garantiza que los paquetes lleguen libre de errores o en el orden correcto.

Los hosts se distinguen por la dirección IP de sus interfaces de Red. Las direcciones son expresadas en cuatro octetos separados por puntos, cada octeto tiene un valor entre 0 y 255, sin embargo no se puede usar el 0 y 255 como direcciones hosts. Cada dirección se subdivide en dos partes la dirección de red y el host.

Originalmente la parte de la dirección que representaba a la red tenía una dependencia con las clases de red tal como se muestra en la TABLA Nº 1.1.

TABLA Nº 1.1. Subredes en la arquitectura TCP/IP

Clase	Rango del primer octeto	numero de octetos	numero de hosts en la red
A	1-127	1	16777216
B	128-191	2	65536
C	192-223	3	256
D	224-239	Multicast	
E	240-255	Reservado	

1.3.2 Componentes de Seguridad de Redes

Adicionalmente a dimensionar el *throughput*, la arquitectura de red debería también ayudar a proteger sus componentes. Los principales conceptos los cuales se enfocan en aislar las redes en los diferentes dominios de confianza son:

- Enrutamiento seguro, significa que el tráfico de datos solo viajará por rutas predeterminadas que sean conocidas, evitando así que la información se vea comprometida.
- Routers de borde, su función principal es filtrar el tráfico externo que nunca debería alcanzar la red interna.
- Segmentación de Red, es una manera efectiva de reforzar las políticas de seguridad, en dominios de confianza, controlando que tráfico se puede re direccionar entre segmentos.
- Zona desmilitarizada, permite a una organización brindar a hosts externos acceso limitado a recursos públicos quitándole los derechos de acceso no controlados a la red interna.

a) Firewalls

Firewalls son dispositivos de control de accesos que refuerzan la administración de políticas de seguridad filtrando el tráfico de datos basado en un conjunto de reglas, mientras que siempre son usados como gateways de internet también existen

consideraciones para ubicarlos en la Interna tal como se muestra en la Figura 1.7. Firewalls deberían estar ubicados entre entidades que tienen diferentes dominios de confianza. Por ejemplo si el segmento LAN del departamento de los servidores está en la mismo segmento LAN que los usuarios en general, deberían existir dos dominios de confianza, instalando un firewall entre estos dos dominios de confianza se protege el acceso no autorizado hacia los servidores protegiendo de esta manera la información sensible que estos contienen.

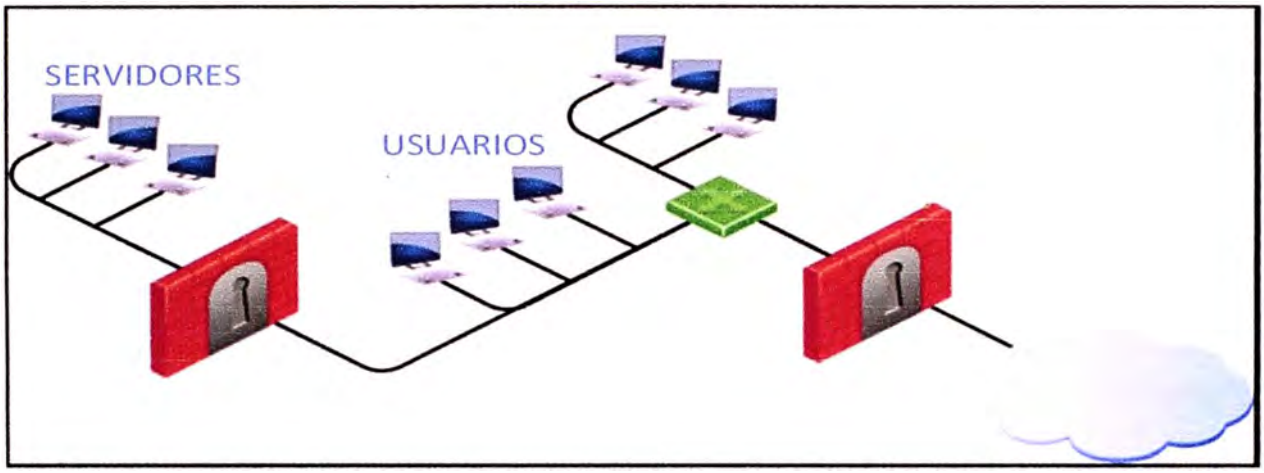

Figura 1.7 Arquitectura del cortafuego

(Fuente Checkpoint)

b) IPS (Sistema de Prevención de Intrusos)

De sus siglas en ingles un Sistema de Prevención de Intrusos tiene como principales funciones identificar las conexiones anómalas, contenido inapropiado, entre otros; esto se debe que a diferencia del Firewall, un IPS puede identificar código malicioso dentro de los paquetes, aunque las características de los paquetes estén aparentemente correctas.

En la implementación del IPS en su configuración por defecto viene con reglas y firmas predeterminadas por lo cual se recomienda ponerlo en modo IDS solamente como analizador, para identificar qué es lo que reconoce como trafico malicioso y así evitar los falsos positivos.

CAPITULO II
PLANTEAMIENTO DEL PROBLEMA

2.1 Descripción del Problema

La corporación en la cual se centra el presente informe se inició como tiendas por departamento, para luego formar una financiera, la misma que posteriormente sería el Banco por lo cual los recursos y servicios eran compartidos entre ellas, incumpliendo de esta manera las exigencias del ente regulador la SBS.

Actualmente, la corporación cuenta con 2 negocios: una Tienda por departamentos y un Banco; el Banco se encuentra regulado por la SBS, por lo cual debe cumplir con las exigencias que ésta demande, una de ellas es la de tener los servicios del Banco totalmente independientes.

El primer paso que se realizó fue diferenciar las redes de ambos negocios, lo cual conllevaría a tener una doble inversión en los sistemas y servicios.

Debido a lo expuesto anteriormente, el principal problema para la corporación es la de centralizar los servicios comunes de los negocios, para de esta manera realizar la optimización de recursos y servicios.

2.2 Objetivo del informe

El presente trabajo tiene por objetivo:

- Describir la implementación de una nube privada de servicios corporativa.

2.3 Evaluación del problema

Para poder realizar la optimización de recursos usados en la corporación se busca un modelo que cumpla con los requisitos necesarios, es importante conocer los procesos, las normas o políticas internas, la infraestructura tecnológica y recursos humanos que procesan, transmiten o almacenan la información de las empresas.

En la Figura 2.1 se muestra el diagrama de red actual sobre el cual se debe diseñar la arquitectura de la nube interna.

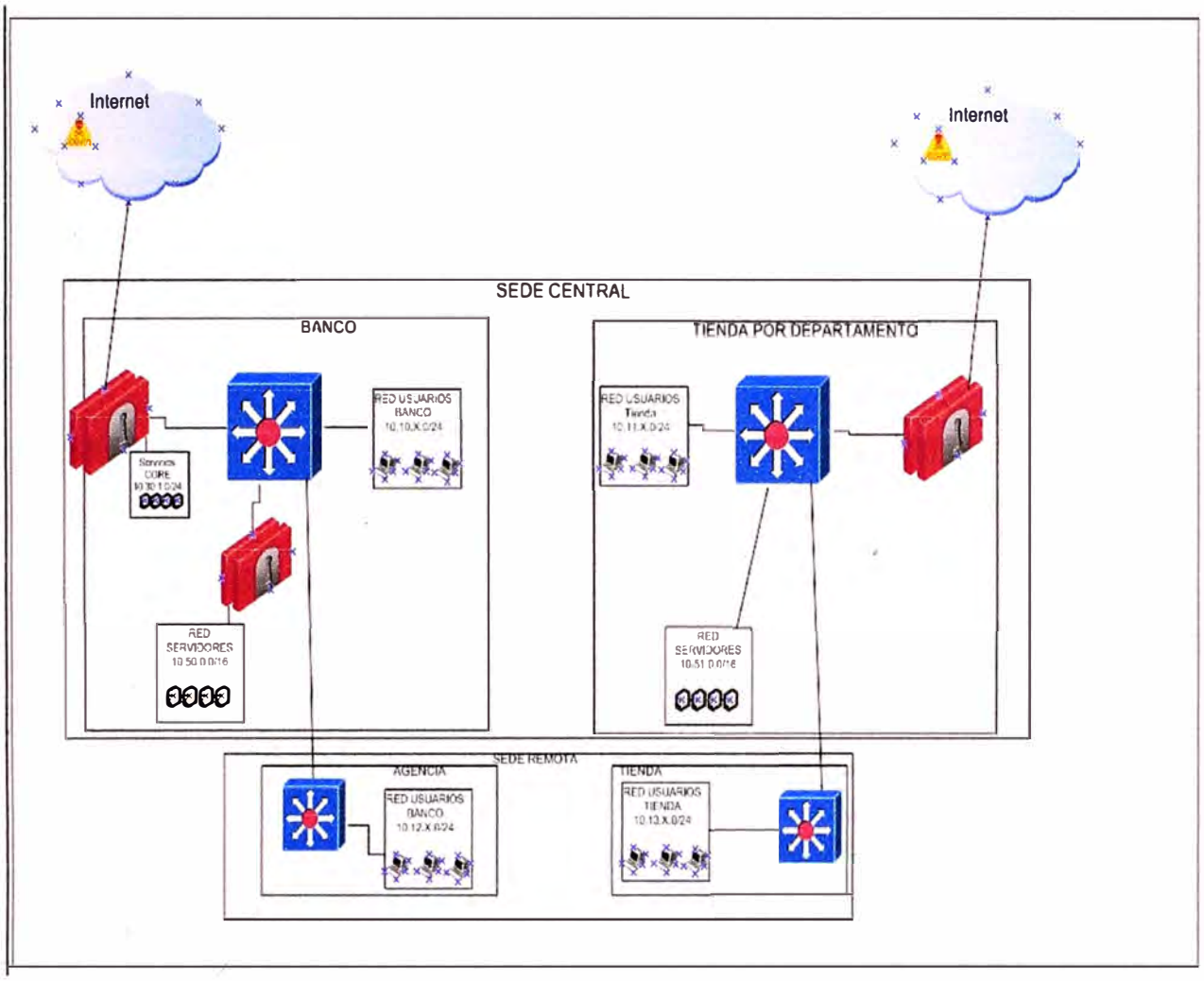

Figura2.1 Diagrama de la Arquitectura Actual

2.4 Limitaciones del informe

Para el desarrollo del presente trabajo se debe realizar el análisis de la situación actual de los servicios tanto de la Tienda por Departamento y el Banco, seguidamente formular una solución e implementarla.

2.4.1 Limitaciones en el diseño de red

El presente estudio se enfoca en el diseño y segmentación de la red que permita centralizar los principales servicios de la Tienda y el Banco en una capa superior; adicionalmente, se busca incrementar el nivel de protección perimetral del entorno de red que se obtenga como resultado de la segmentación de red con la implementación de Firewall, sistemas de detección de y protección contra intrusos y balanceadores de enlace.

2.4.2 Limitaciones en la gestión de seguridad de información

El presente estudio está focalizado en la implementación de una nueva zona de servicios, pero siguiendo las recomendaciones de los estándares de implementación de arquitecturas de Red seguras. No se consideran los requisitos que estén relacionados con:

- La gestión de la seguridad de la información, como lo son la elaboración de procedimientos, la implementación de políticas, la creación de estándares de seguridad y la implementación de metodologías de desarrollo seguro.
- La gestión de incidentes.
- Los planes de continuidad del negocio e interacción con proveedores.

CAPITULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

3.1 Introducción

Para el desarrollo del proyecto se usará la guía del xxxxxx PMBOK, que es el estándar para la administración de Proyectos, en la cual se define como Proyecto al esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único.

En primer lugar, todo proyecto debería estar alineado dentro del plan estratégico de la compañía; el segundo rango de jerarquía podría ser un portafolio que puede incluir distintos programas y/o proyectos, los cuales están enmarcados en el contexto de la dirección de proyectos tal como se muestra en la Figura 3.1

Figura3.1 Contexto de la Dirección de Proyectos
(Fuente DIRECTOR DE PROYECTOS)

Las principales características de los objetivos de un proyecto son los siguientes:

- Se establecen al Inicio.
- Se perfeccionan durante la planificación.
- Son responsabilidad del Director del Proyecto.
- Son claros y alcanzables.

3.2 Ciclo de Vida del Proyecto

En la Figura 3.2 se muestra el ciclo de vida de un proyecto estándar en el cual se muestra el uso de recursos y costos en cada una de sus fases.

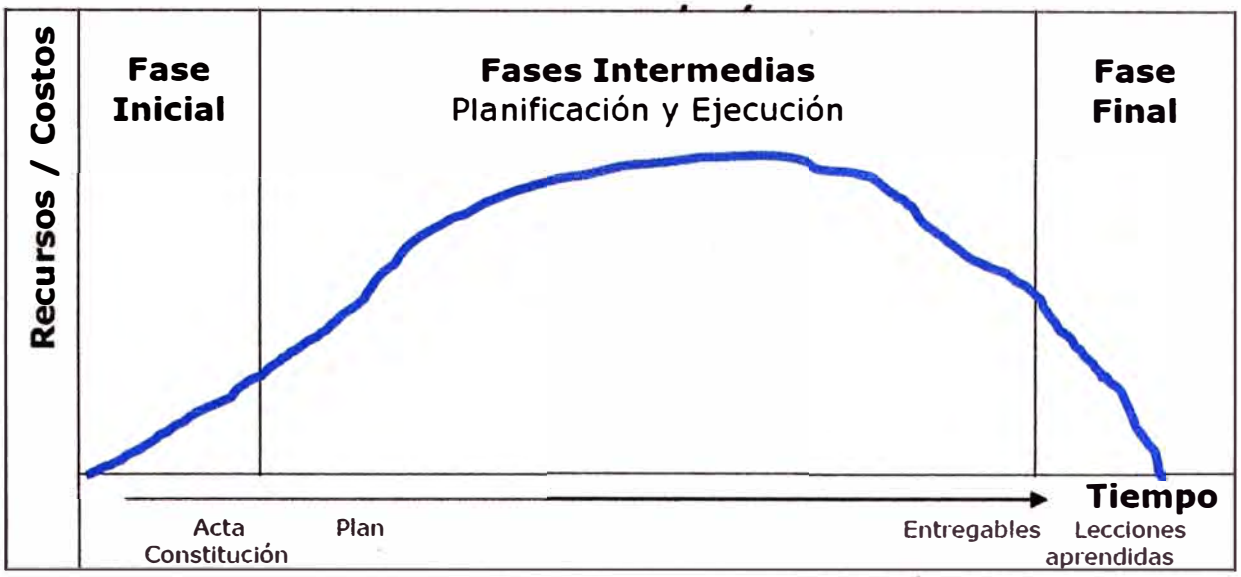

Figura 3.2 Ciclo de Vida del Proyecto

(Fuente DIRECTOR DE PROYECTOS)

Por lo general, en la fase inicial del proyecto se utilizan pocos recursos, lo que implica bajos costos, en las etapas intermedias se consume la mayor parte del presupuesto y en la fase final el costo es relativamente bajo.

Al inicio de un proyecto existe una mayor incertidumbre, la certeza de alcanzar un proyecto exitoso aumenta a medida que se va desarrollando y ejecutando el proyecto.

3.3 Procesos del Proyecto

Se mencionan 5 grupos de procesos de la dirección de proyectos tal como se muestran en la Figura 3.3:

- Procesos de inicio: En los cuales se definen los objetivos del proyecto, se identifican a los principales interesados y se autoriza formalmente el inicio del proyecto.
- Procesos de planificación: en el cual se define el alcance del proyecto, se refinan los objetivos y se desarrolla el plan para la dirección del proyecto, que será el curso de acción para un proyecto exitoso.
- Procesos de ejecución: en el cual se integran todos los recursos a los fines de implementar el plan para la dirección del proyecto.
- Procesos de monitoreo y control: en el cual se supervisa el avance del proyecto y se aplican acciones correctivas.
- Procesos de cierre: en el cual se formaliza la aceptación de los entregables del proyecto.

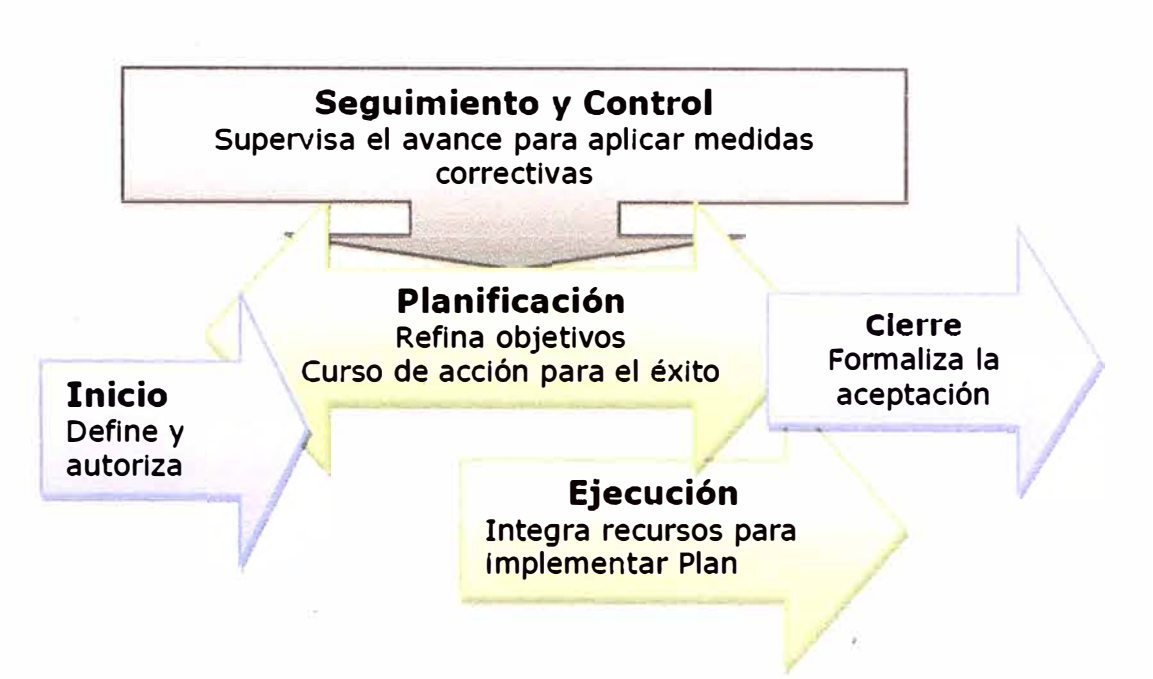

Figura 3.3 Ciclo de vida del proyecto

(Fuente DIRECTOR DE PROYECTOS)

3.3.1 Inicio

Las entradas de los procesos de inicio son:

- Activos de los procesos de la organización: políticas, procesos, normas, información histórica y lecciones aprendidas.
- Enunciado del trabajo.
- Requisitos de negocio.
- Plan estratégico.
- Disparadores del proyecto: problema, oportunidad de mercado, requisito de negocio, cambio tecnológico, legislación, etc.

Al procesar las entradas según corresponda se obtendrá:

- Acta de constitución del Proyecto.

3.3.2 Planificación

En los procesos de planificación se determinará si es factible o no llevar a cabo lo anunciado en el alcance. En caso que sea posible, la planificación deberá detallar cómo se desarrollará el proyecto para cumplir con los objetivos. Esta planificación es gradual, siendo este grupo de procesos repetitivo e iterativo.

3.3.3 Ejecución

En el grupo de procesos de ejecución se invierte la mayor parte del presupuesto desarrollándose las siguientes actividades:

- Implementar el plan para la dirección del proyecto.
- Coordinar todos los procesos.
- Asegurar que se cumpla con la calidad pre-establecida.

- Distribuir la información con los avances del proyecto.
- Gestionar las expectativas de los interesados.

3.3.4 Monitoreo y Control

En este grupo de procesos se debe controlar que solo se implementen los cambios aprobados, esta es una etapa de retroalimentación continua que permite detectar acciones preventivas y recomendar acciones correctivas.

3.3.5 Finalización

Todo proyecto que comienza debe cerrarse, los cierres principales son:

- Cierre de proyecto.
- Cierre de contrato.

CAPITULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

4.1 Introducción

El análisis y presentación de resultados se enfoca en el diseño de la arquitectura de red de una de nube de servicios corporativa, así como el aprovisionamiento del direccionamiento de las Redes.

4.2 Solución de la arquitectura de red

Evaluando las necesidades de la corporación se identifican los servicios y se realiza una grafico inicial de lo solicitado tal como se muestra en el anexo A y en el anexo B. Adicionalmente, en la TABLA Nº 4.1 se muestra el direccionamiento de red utilizado en la implementación.

TABLA Nº 4.1 Direccionamiento nube de servicios

VLAN ID	Nombre de la VLAN	Descripción	Número de Direcciones IP necesarias	Segmento de red asignado
10	Vlan 10	Servicio de Internet proveedor 1	No mayor a 14 hosts	200.44.30.0/28
20	Vlan 20	Servicio de Internet proveedor 2	No mayor a 14 hosts	190.33.30.0/28
30	Vlan 30	Servicios compartidos de la empresa	No mayor a 14 hosts	192.168.10.0/28
40	Vlan 40	Red de gestión	No mayor a 30 hosts	192.168.200.0/27

4.2.1 Cifrado e Intercambio de información

Cifrado e intercambio de información segura, es una tecnología que proporciona la transferencia de información de manera confiable y eficiente. Las herramientas tradicionales de transferencia de información, como el *File Transfer Protocol* (FTP) son inseguras, pero con el uso de un sistema de intercambio de información en el cual se incluyan el cifrado cuente con un log de auditoría es lo que la diferencian son las principales funciones que la diferencian. En la Figura 4.1 se muestra la arquitectura asociada al servicio de intercambio de información.

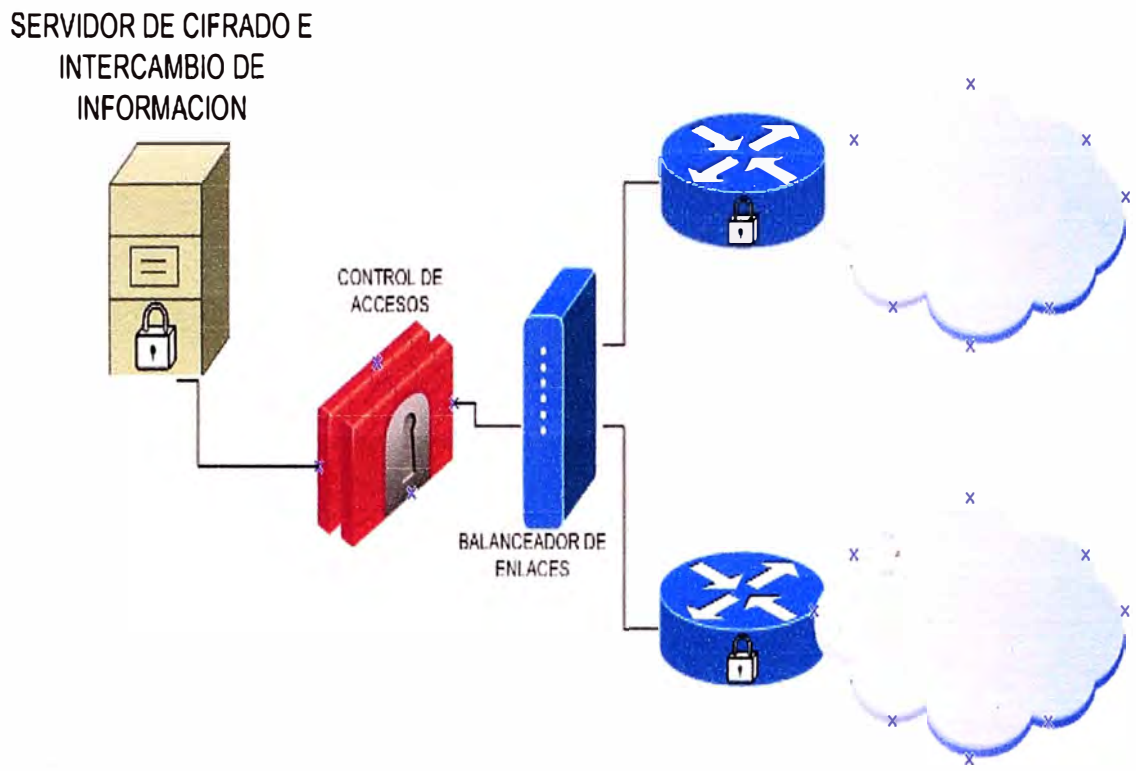

Figura 4.1 Arquitectura servicio de intercambio de información

4.2.2 Correo Seguro

El Servidor de Gestión de correo seguro cuenta con:

- Filtro de reputación para realizar una evaluación en tiempo real de las amenazas e identificar a los remitentes de e-mail sospechosos a nivel de conexión TCP.
- Motor Anti-Spam basado en contenido el cual analiza 4 criterios para cada mensaje ¿Qué contiene el mensaje?, ¿Cómo ha sido construido el mensaje?, ¿Quién ha enviado el mensaje? y ¿A dónde llevan los enlaces *Uniform Resource Locator* (URL) incluidos en el correo?.
- Defensa anti-virus el cual identifica y bloquea los virus horas antes de que estén las firmas tradicionales y se integran con Motores de Antivirus de terceros.

Tratamiento de contenido el cual se realiza según la dirección IP de origen, el encabezado, palabras clave en el cuerpo del mensaje, el tamaño o el tipo de archivos adjuntos, palabras clave u objetos insertados en los archivos adjuntos o la reputación del remitente. Lo cual permite a los administradores proteger los datos sensibles. En la Figura 4.2 se muestra la arquitectura asociada al servicio de correo seguro.

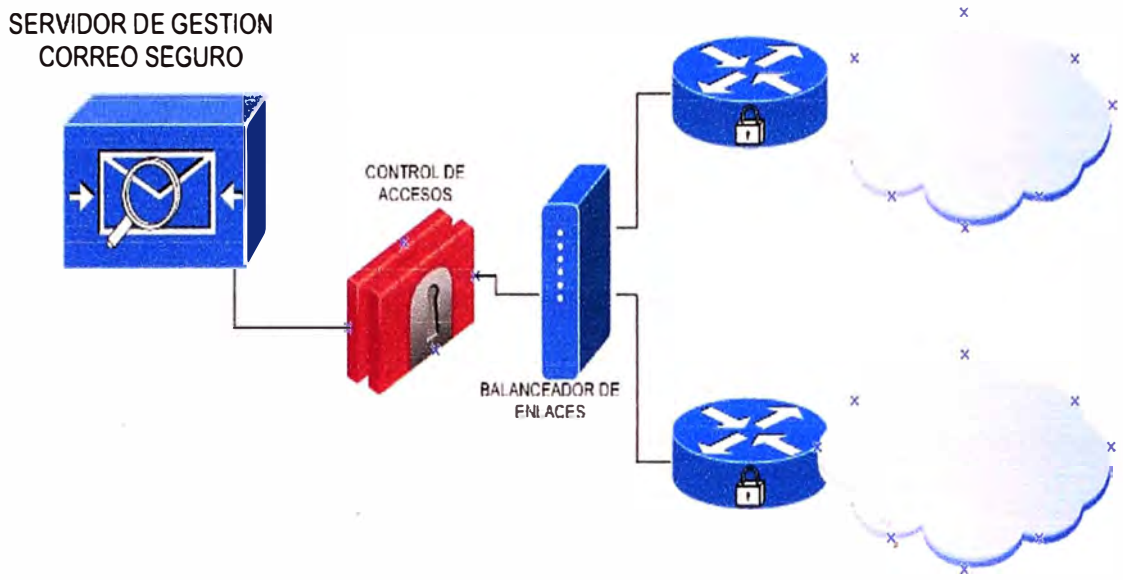

Figura 4.2 Arquitectura servicio de correo seguro

4.2.3Red Privada Virtual (VPN)

El servicio de la Red Privada Virtual, se usa para extender redes privadas por medio de redes públicas como el internet, por el cual se habilita conexiones virtuales punto a punto encriptados. En la Figura 4.3 se muestra la arquitectura asociada al servicio de VPN.

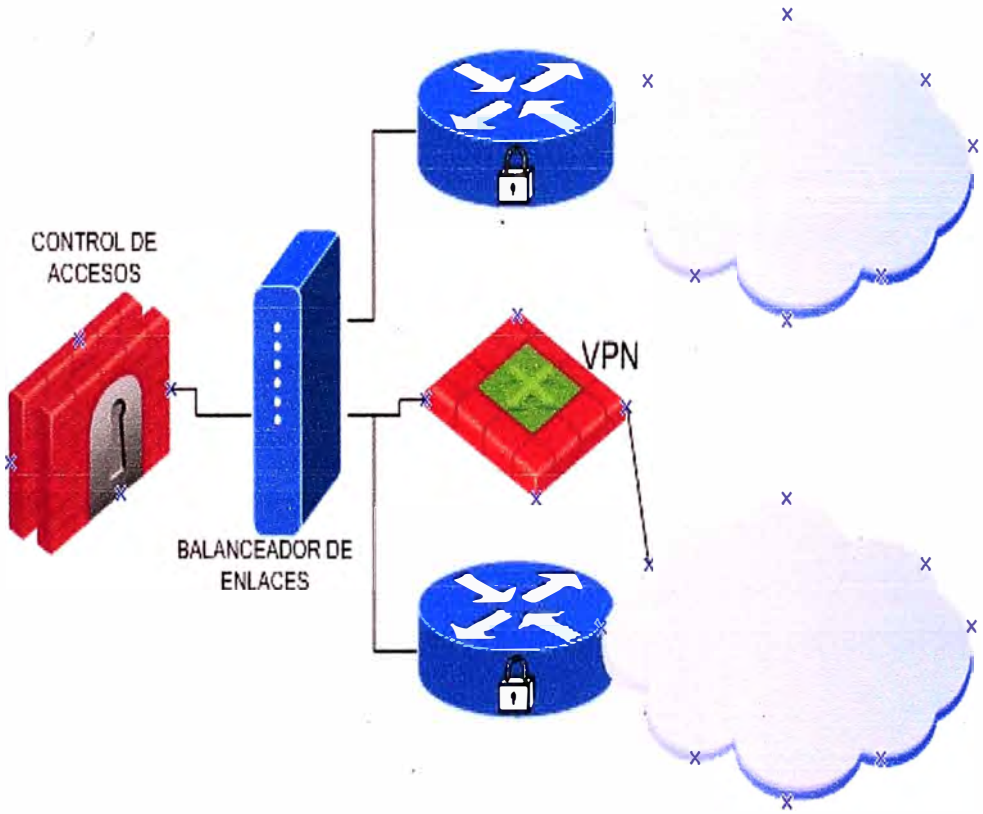

Figura 4.3 Arquitectura servicio de VPN

4.2.4 Navegación Segura

El servicio de navegación segura presta una solución integral de protección y control sobre el tráfico de Internet. Cuenta con las siguientes funciones:

- Autenticación fuerte de usuarios, filtrado web, inspección profunda de contenido para los datos.
- Inspección y validación de tráfico SSL, el contenido de la memoria caché y optimización del tráfico, gestión de ancho de banda.
- Filtrar, quitar o reemplazar contenido Web malicioso.

En la Figura 4.4 se muestra la arquitectura asociada al servicio de navegación segura.

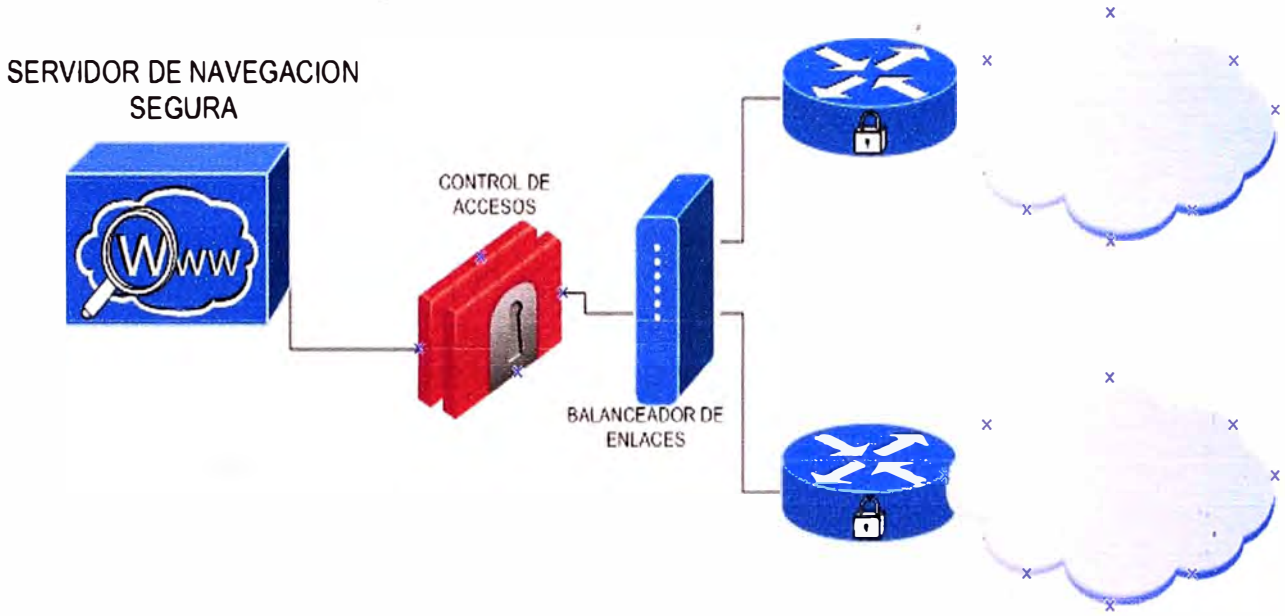

Figura 4.4 Arquitectura servicio de navegación segura

4.2.5 Gestión de Identidades

El servicio de gestión de identidades proporciona una gestión del ciclo de vida de los usuarios automatizada y basada en políticas, así como controles de acceso en toda la empresa.

El servicio proporciona:

- Gestión del ciclo de vida de los usuarios automatizada, optimizando la productividad y reduciendo los costes de gestión y rechazo de perfiles de usuario, credenciales y derechos de acceso en todo el ciclo de vida del usuario.
- Conformidad de seguridad, ofrece la colección de seguimiento de auditoría, correlación y creación de informes. En la Figura 4.5 se muestra la arquitectura asociada al servicio de gestión de identidades.

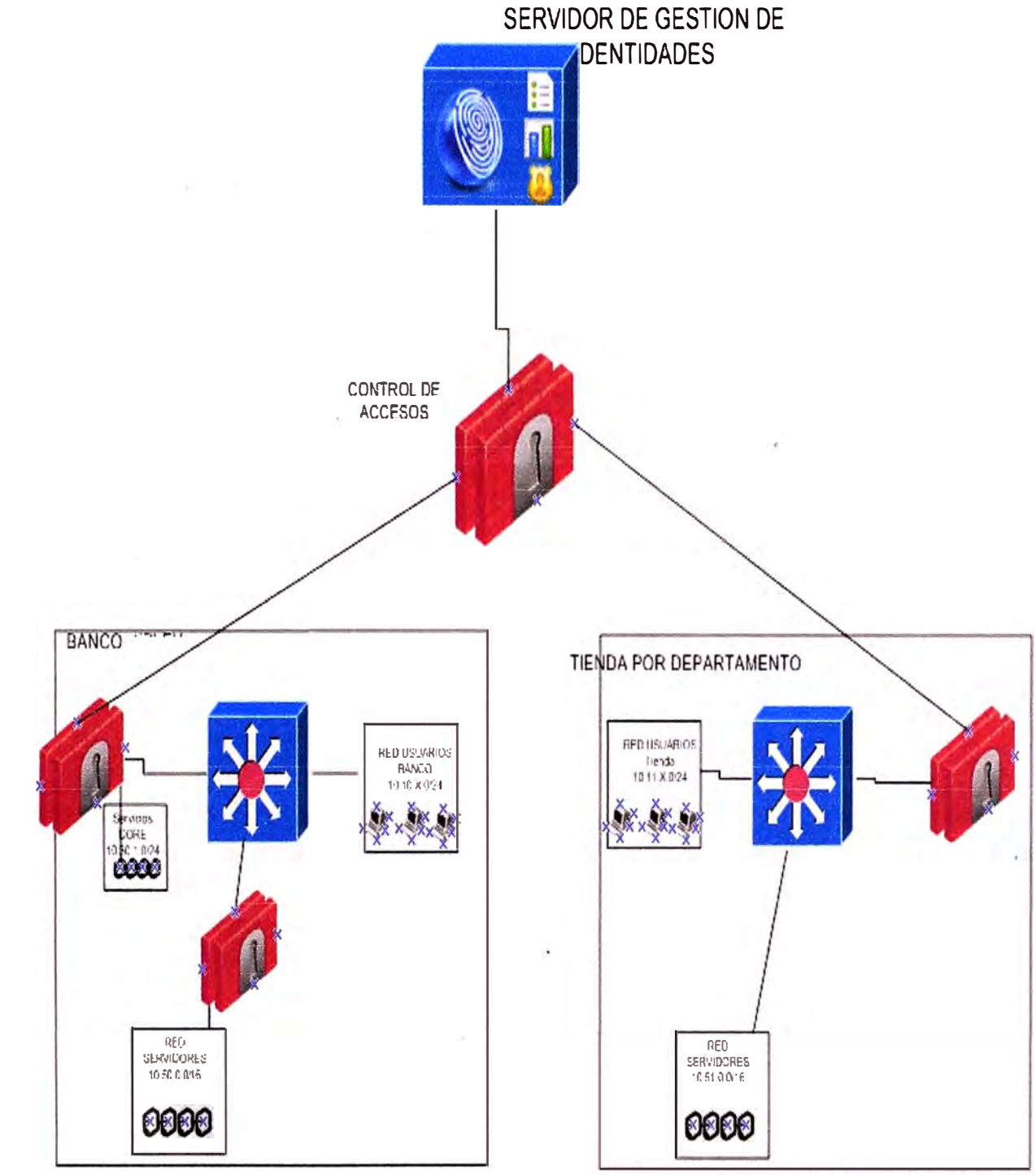

Figura 4.5 Arquitectura servicio de gestión de identidades

4.2.6 Concentrador de Accesos de Red

Es una plataforma de administración de accesos a los recursos de Red proporcionando la administración y soporte a una gran variedad de escenarios que incluyen redes inalámbricas, 802.1x wired, y acceso remoto mediante AAA (Autenticación, Autorización y Contabilización). En la Figura 4.6 se muestra la arquitectura asociada al servicio de concentrador de Accesos de Red.

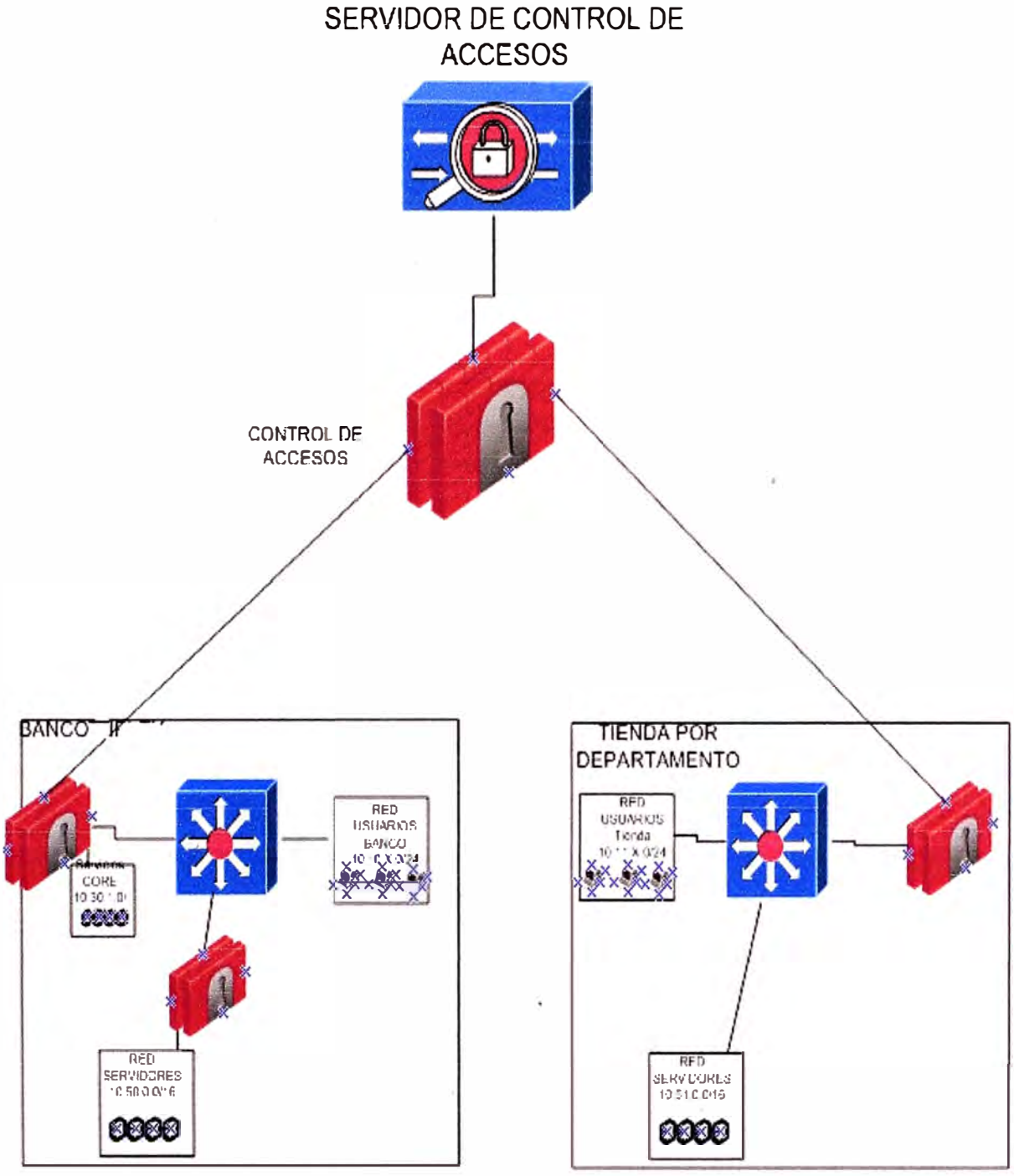

Figura 4.6 Arquitectura servicio de control de accesos de red

4.3 Recursos humanos y equipamiento

Con la finalidad de garantizar resultados óptimos se conto con el apoyo de empresas con experiencia en implementación de soluciones *Cloud* así como en cada uno de los servicios que se brindaran, conformándose un equipo de trabajo mixto tal como se muestra en la Figura 4.7

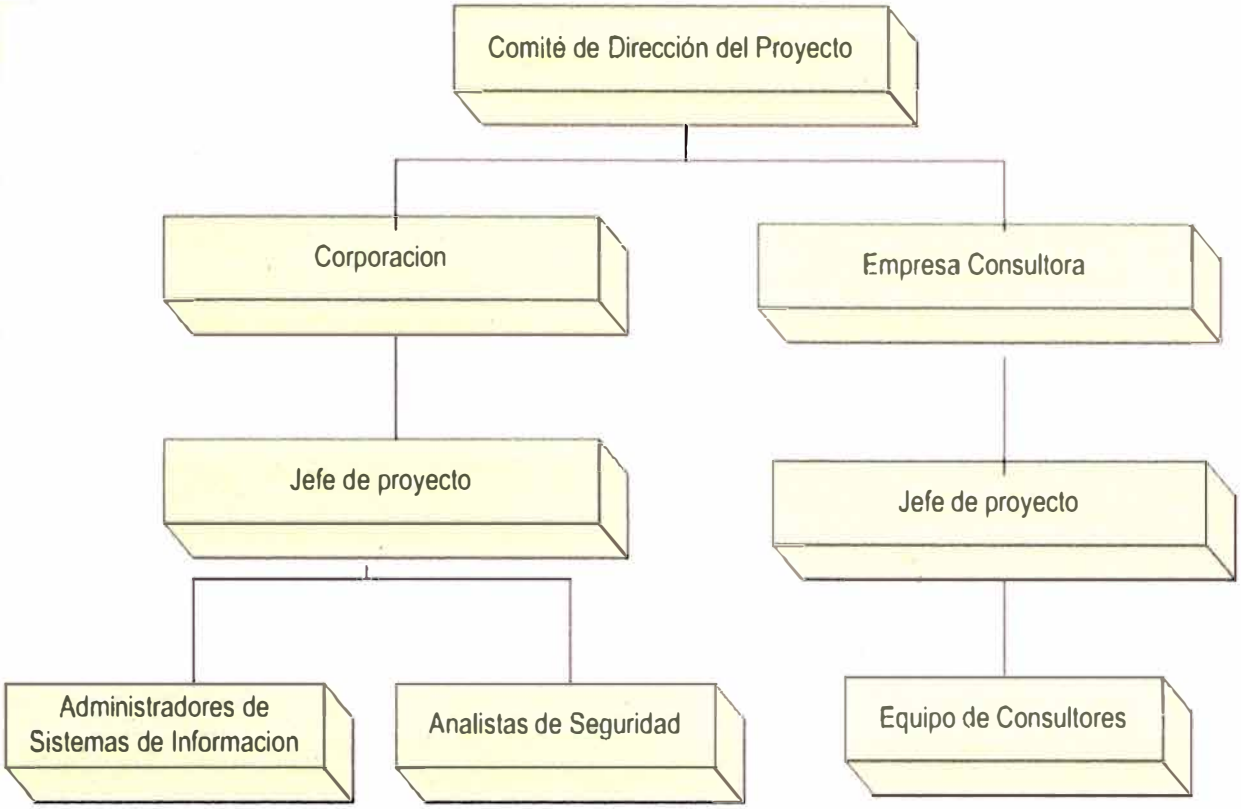

Figura 4.7 Equipo de trabajo

CONCLUSIONES

Del presente informe se concluye:

1. Las utilidades que se implementan en la nube de servicios corporativa son correctamente identificados, con la finalidad de poder dimensionar de manera eficaz el aprovisionamiento de recursos.
2. Como factor principal para lograr el éxito de la implementación de la nube de servicios corporativa es necesario contar con la asesoría externa de empresas que cuenten con personal especializado.
3. Para lograr el éxito del desarrollo del proyecto es fundamental contar con el respaldo de la "Alta Gerencia".
4. La implementación de la nube de servicios es el primer paso para el cumplimiento de la regulación de la Superintendencia de Banca y Seguros (SBS) circular G-140-2009, se debe tener presente que para reforzar los controles se requiere además de la elaboración de políticas, procedimientos y normas de seguridad para el desarrollo de aplicaciones y configuración de dispositivos.
5. Si la corporación requiere certificar y mantener el cumplimiento de la regulación, debe tener en cuenta que es necesario desarrollar un proceso de mantenimiento y control de cambios. Se debe contar con un procedimiento de monitoreo y documentación ante cambios en la infraestructura, con lo cual se tendrá un registro de cambios autorizados como evidencia ante el regulador.

RECOMENDACIONES

Del presente informe se recomienda:

1. Elaborar e implementar estándares de seguridad para la configuración de los routers, firewalls alineados a los requerimientos de aseguramiento de las redes.
2. Implementar un correlacionador de eventos en el cual se pueda mostrar el estado de los servicios en línea.
3. Revisar la familia de normas ISO 27000 actualizados para poder alinear la implementación de la nube de servicios corporativa.

ANEXOS

ANEXO A
RELACIÓN DE SERVICIOS COMPARTIDOS DE LA CORPORACIÓN

La relación de servicios que serán compartidos por la corporación se muestran en la TABLA A. 1

TABLA A.1

SERVICIO	DESCRIPCIÓN
Cifrado e intercambio de información	Servicio utilizado para concentrar y asegurar el intercambio de información con los distintos proveedores vía SFTP, HTTPS.
Correo seguro	Servicio utilizado para contener las posibles amenazas relacionadas al servicio de correo tales como SPAM, archivos con software malicioso adjunto, etc.
Red privada virtual	Servicio utilizado para el acceso remoto seguro a los servicios de la empresa
Navegación segura	Servicio utilizado para contener las posibles amenazas relacionadas al servicio de navegación de internet de los usuarios de la empresa, mediante un filtro de contenidos evitando el acceso a páginas que contengan contenido malicioso.
Gestión de identidades	Servicio utilizado para gestionar el ciclo de vida de los usuarios que tienen accesos a los diversos sistemas de la empresa.
Concentrador de accesos de red	Servicio utilizado para tener centralizada la gestión de accesos a los servicios de red, así como tener un registro de auditoría.

ANEXO B
DEFINICIÓN DE REQUERIMIENTOS

En la Figura B.1 se detallan los requerimientos para realizar la implementación de la nube de servicios corporativa.

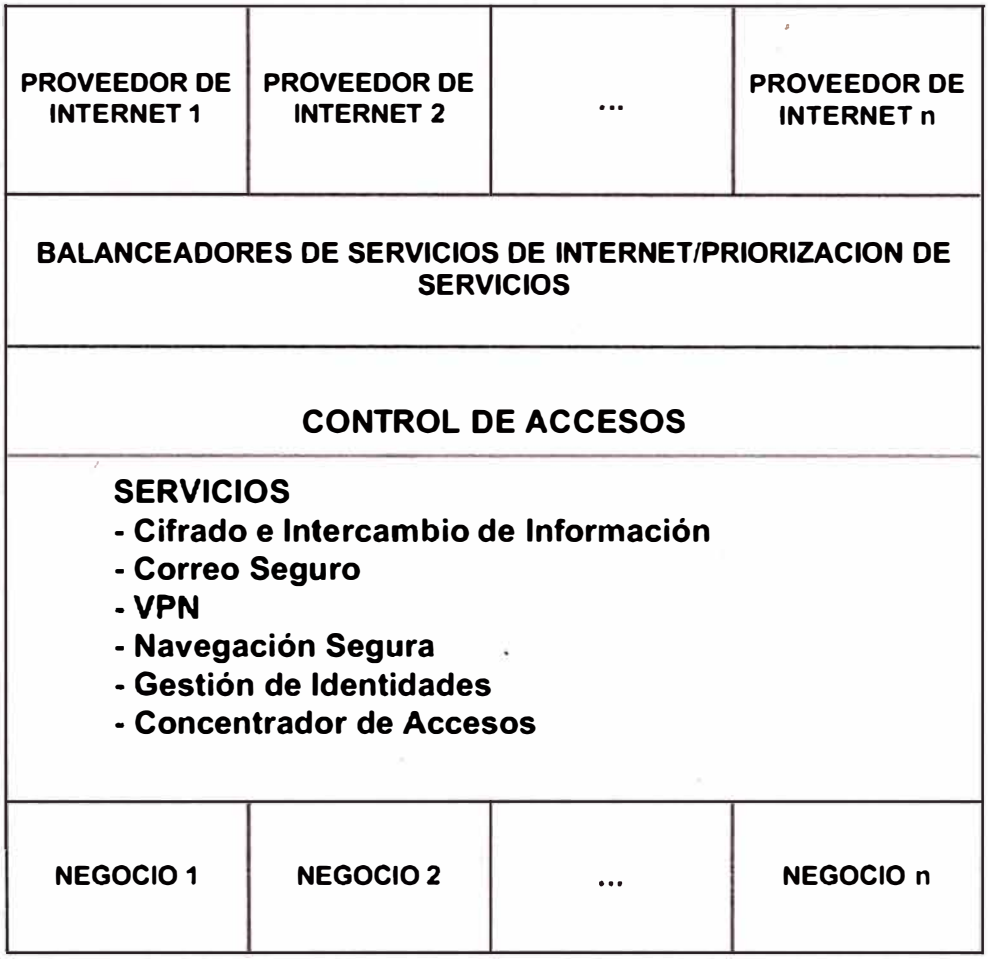

Figura B.1 Requerimientos para la implementación de la nube de servicios corporativa.

ANEXO C
DISEÑO LÓGICO DE LA SOLUCIÓN

En la Figura C.1 se muestra el diseño lógico correspondiente a la implementación de la nube de servicios corporativa.

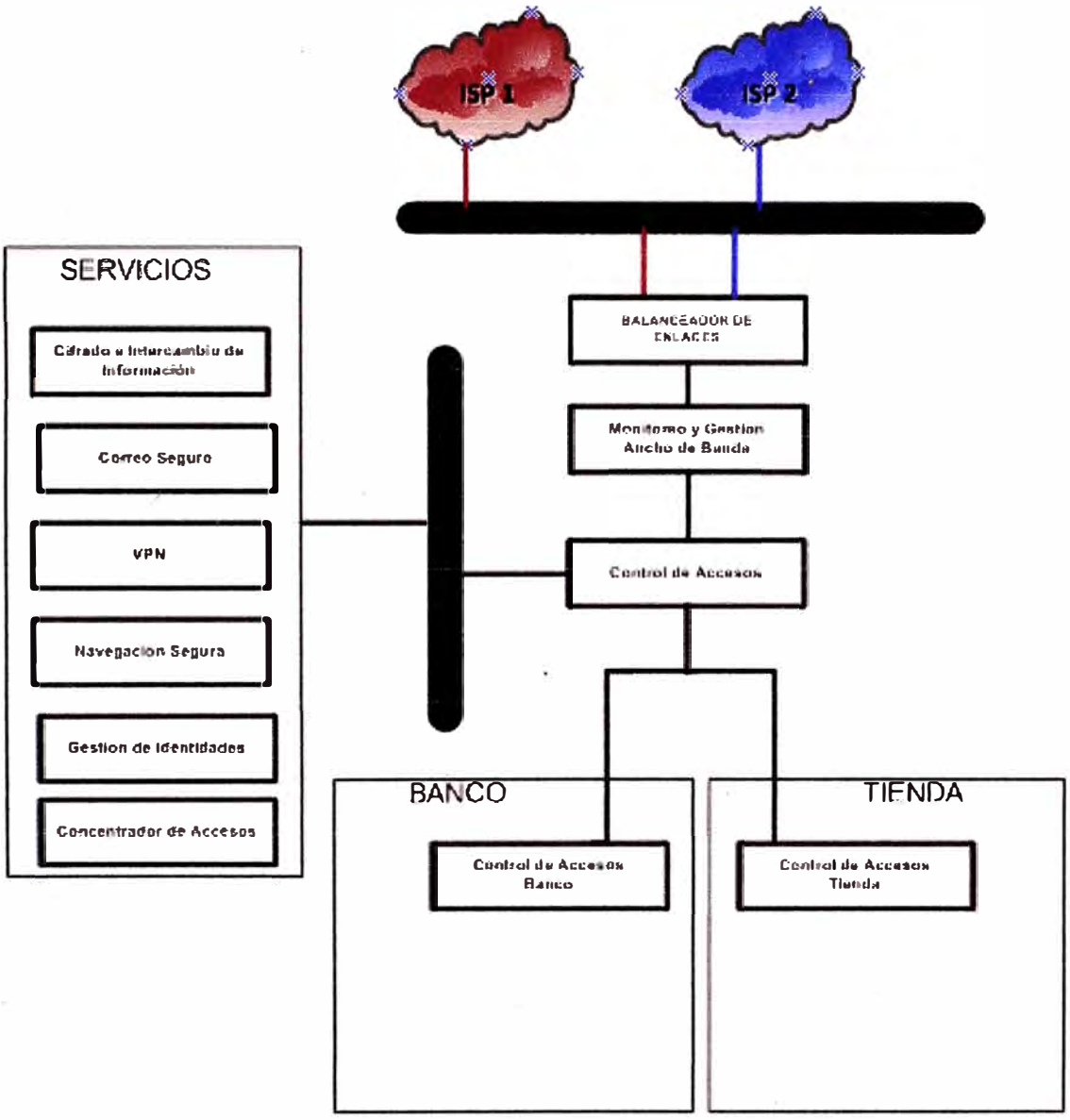

Figura C.1 Diseño lógico de la arquitectura de nube de servicios corporativa.

ANEXO D
DIAGRAMA ACTUAL DE RED

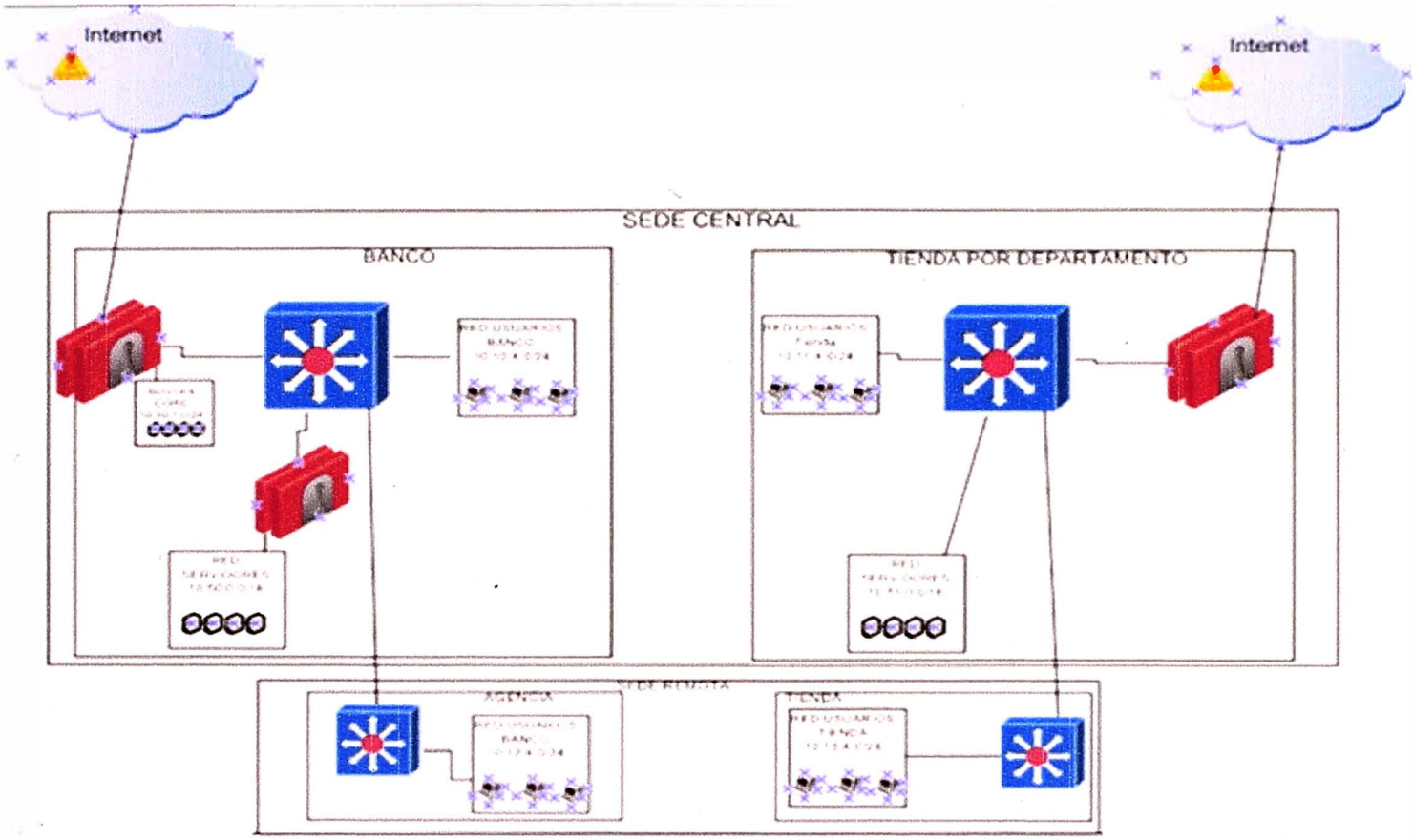

Figura D.1 Diagrama actual de red

ANEXO E
DIAGRAMA FINAL DE RED

En la Figura E.1 se muestra el diagrama final de la implementación de la nube de servicios corporativa.

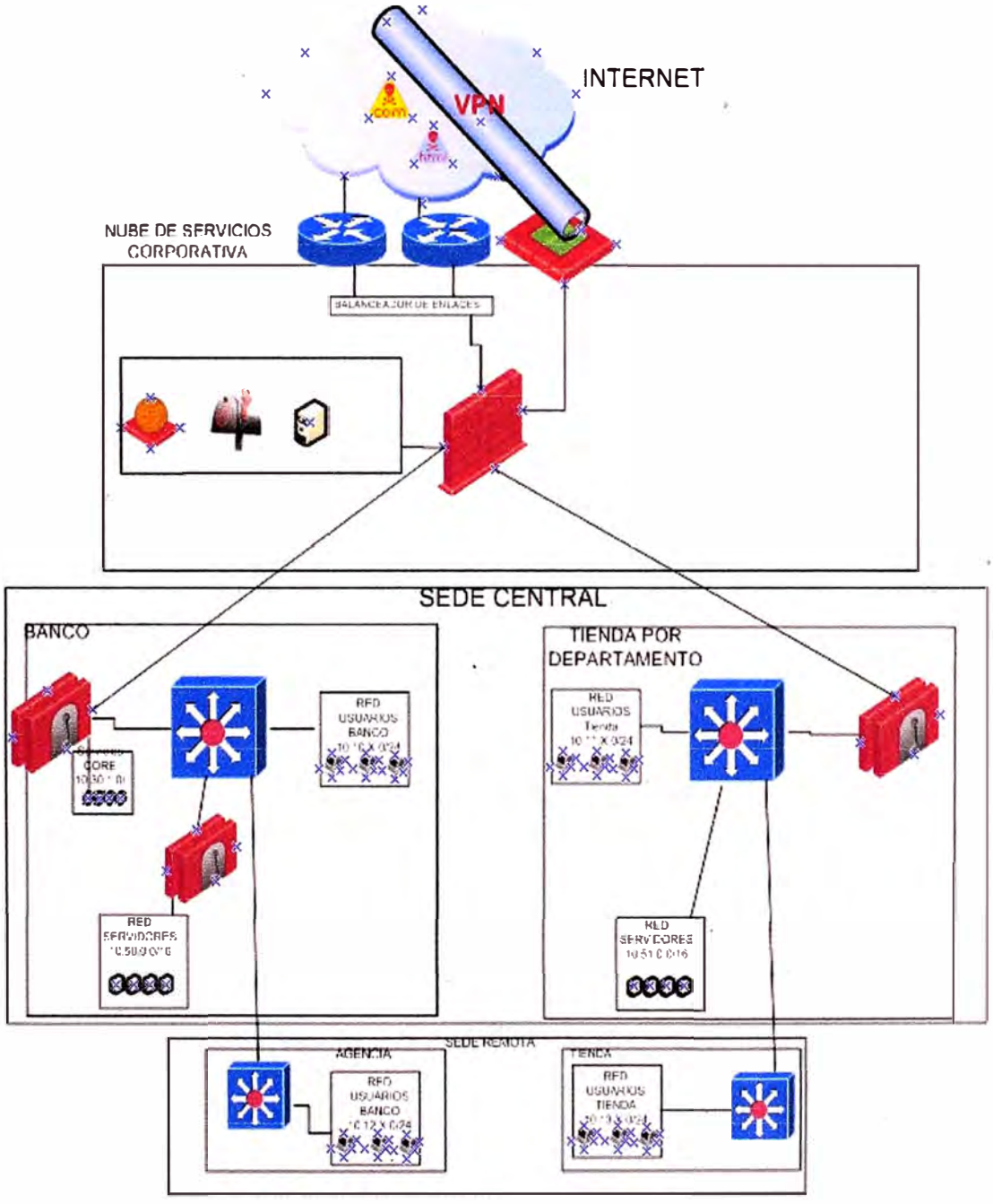

Figura E.1 Diagrama final de la implementación de la nube de servicios corporativa.

ANEXO F
GLOSARIO DE TÉRMINOS

SBS: Súper Intendencia de Banca y Seguros.

Backdoor: Es el método que se usa para pasar la autenticación normal, asegurando de esta manera un acceso remoto ilegal a los sistemas afectados.

IP: Protocolo de internet el cual contiene información sobre direcciones y algunos datos de control, permitiendo el ruteo de paquetes.

Servidor Web: Computadora con un programa capaz de aceptar pedidos HTTP de clientes web y brindar respuestas HTTP.

Navegador Web: Software que permite el acceso a Internet.

Base de Datos: Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Sistema Operativo: Es un programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación.

VPN: Es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como internet.

OSI: Open System Interconexión (Interconexión de sistemas abiertos) usado para estandarizar los Sistemas.

Protocolo: Es un método estándar que permite la comunicación entre Sistemas.

Throughput: Es la tasa promedio de la entrega de mensajes de éxito a través de una vía de comunicación.

BIBLIOGRAFÍA

[1] Eric Conrad/Seth Misenar/Joshua Feldam, CISSP STUDY GUIDE, Segunda Edición, 2012.

[2] W. Hord Tipton, OFFICIAL GUIDE TO THE CISSP CBK, Tercera Edición, 2013.

[3] ONTSI, Cloud Computing Retos y Oportunidades, 2012.

[4] Pablo Lledo, DIRECTOR DE PROYECTOS, Segunda Edición, 2013

[5] PMI, A GUIDE TO THE PROJECT MANAGEMENT BODY OF KNOWLEDGE, Quinta Edition, 2013