



FACULTAD INGENIERIA Y CIENCIAS AGROPECUARIAS

**ANÁLISIS Y DISEÑO DE LA RED DE DATOS, PARA LA IMPLEMENTACIÓN
DE LA INFRAESTRUCTURA TECNOLÓGICA EN LA UNIDAD DE ANÁLISIS
FINANCIERO DEL ECUADOR**

**Trabajo de Titulación presentado en conformidad con los requisitos
establecidos para optar por el título de Ingeniera en Redes y
Telecomunicaciones**

Profesor guía

Ing. Ángel Jaramillo

Autora

Dalila Mirella Gaibor

Año

2013

DECLARACIÓN DEL PROFESOR GUÍA

Declaro haber dirigido este trabajo a través de reuniones periódicas con la Estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

Ángel Jaramillo

INGENIERO

1715891964

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Dalila Mirella Gaibor

0602670218

AGRADECIMIENTOS

A Dios

DEDICATORIA

A mi familia

RESUMEN

El presente trabajo tiene como finalidad analizar y diseñar la red de datos para la implementación de la infraestructura tecnológica en la Unidad de Análisis Financiero del Ecuador, para lo cual se ha utilizado conceptos de convergencia, movilidad, escalabilidad, interoperabilidad, seguridad, alta disponibilidad.

Se realiza un análisis de la situación actual de la infraestructura tecnológica de la Institución, lo cual permite plantear una solución para la red de datos que cubra los requerimientos de los servicios informáticos que se implementarán en la Institución, tales como VoIP, circuito de video vigilancia con cámaras IP, servicio de correo electrónico, sistema documental; y, se realiza un estimado del ancho de banda que se podría utilizar para estos servicios, así como también se estima el ancho de banda para el Internet de acuerdo a la realidad Institucional.

Adicional, se plantea un diseño de la red datos considerando los conceptos planteados en la presente tesis.

ABSTRACT

This paper aims to analyze and design the data network to implement the technology infrastructure in the Financial Analysis Unit of Ecuador, to which has been used concepts of convergence, mobility, scalability, interoperability, security, high availability.

An analysis of the current state of the technological infrastructure of the institution, which allows us to propose a solution to the data network that meets the requirements of the IT services to be implemented in the institution, such as VoIP, video surveillance circuit IP cameras, email service, documentation system, and an estimate is made of the bandwidth that could be used for these services, as well as estimating the bandwidth to the Internet according to Institutional reality.

Additional, it poses a data network design considering the concepts raised in this thesis.

INDICE

1. Capítulo I. Marco Teórico	2
1.1. Convergencia.....	2
1.2. Movilidad.....	5
1.3. Escalabilidad.....	7
1.4. Alta Disponibilidad.....	9
1.5. Interoperabilidad.....	12
1.5.1. Interoperabilidad de Redes.....	12
1.6. Seguridades.....	14
1.7. Redes.....	17
1.7.1. Redes LAN.....	17
1.7.2. Redes WAN.....	17
1.7.3. Protocolos de Red.....	17
1.7.4. Modelo jerárquico de 3 capas.....	18
1.8. Metodología de diseño.....	20
2. Capítulo II. Análisis y Definición de Requerimiento	22
2.1. Unidad de Análisis Financiero.....	22
2.1.1. De la Información.....	22
2.1.2. De las Funciones y Atribuciones.....	23
2.2. Análisis de la Situación Actual.....	25
2.2.1. Aplicaciones.....	28
2.2.2. Hardware.....	30
2.2.3. Red LAN.....	31
2.2.4. Políticas de Mantenimiento.....	32
2.2.5. Recurso Humano.....	33
2.3. Definición de Requerimientos.....	33
2.3.1. Aplicaciones Informáticas.....	34
2.3.2. Servicios Informáticos.....	34
2.3.3. Equipo Informático.....	35
2.3.4. Equipamiento de Red LAN y WAN.....	36
2.3.5. Cableado Estructurado.....	43
2.3.6. Sistema de Energía Eléctrica Regulada.....	44
3. Capítulo III. Diseño de la Solución	47

3.1.	Red LAN del Centro de Datos	52
3.1.1.	Criterios de diseño	52
3.1.2.	Protocolos de red	52
3.1.3.	Arquitectura de red	53
3.2.	Red LAN de las Oficinas Remotas	54
3.2.1.	Criterios de diseño	54
3.2.2.	Protocolos de red	55
3.2.3.	Cableado estructurado	55
3.2.4.	Arquitectura de red	57
3.3.	Diseño de la Red WAN	58
3.3.1.	Criterios de diseño	58
3.3.2.	Planteamiento de la solución.....	58
3.3.3.	Topología de red.....	59
3.3.4.	Capacidad de canales de telecomunicaciones	60
3.4.	Diseño de Seguridad Perimetral.....	61
3.4.1.	Criterios de diseño	61
3.4.2.	Técnicas a utilizar.....	61
3.4.3.	Topología de red.....	64
4.	Capítulo IV. Esquema de Servicios De Red	65
4.1.	Zona Web	65
4.2.	Zona de Aplicaciones.....	66
4.3.	Zona de Base de datos.....	68
5.	Capítulo V. Análisis de Costos	69
5.1.	Análisis de Costos / Beneficio.....	71
5.2.	Costos Fijos del Proyecto.....	74
6.	Capítulo VI. Conclusiones y Recomendaciones	76
6.1.	Conclusiones	76
6.2.	Recomendaciones.....	77
	REFERENCIAS	79
	ANEXOS	84

INTRODUCCIÓN

Este documento tiene por finalidad realizar un análisis de la situación actual de la red LAN de la Unidad de Análisis Financiero (UAF), determinar el crecimiento tecnológico y enmarcar conceptos de alta disponibilidad, convergencia, movilidad, escalabilidad, seguridad en un diseño que permita a la red LAN de la UAF tener la capacidad de explotar todos los beneficios de las nuevas tendencias tecnológicas, tal como voz, datos y video en un mismo medio físico; o tener la capacidad de crecimiento o expansión de la solución instalada sin que afecte la misma; o, disponer de una infraestructura de red que permita una capacidad de reacción en caso de posibles eventualidades ya sea por errores humanos, fallas técnicas, etc.

El documento se ha dividido en seis partes, intentando detallar de una manera comprensible cada uno de los capítulos, sin caer en la redundancia ni la confusión, es así que el primer capítulo describe el marco teórico que se utiliza en todo el documento.

En el capítulo dos se describe la situación actual en lo que a tecnología se refiere de la Unidad de Análisis Financiero.

En el capítulo tres se propone el diseño de la solución, considerando los conceptos de alta disponibilidad, convergencia, movilidad, interoperabilidad, escalabilidad.

En el capítulo cuarto se describe los servicios del área de negocio, considerando los conceptos objeto de este documento.

En el capítulo cinco se realiza una descripción de los costos más aproximados a la realidad de la implementación de la solución propuesta.

En el último capítulo se concluye y se realiza las correspondientes recomendaciones.

1. Capítulo I. Marco Teórico

1.1. Convergencia

Redes Convergentes: La convergencia de redes incorpora el tráfico de voz, vídeo y datos en una única red. Es algo más que Voz sobre IP; a más de soportar tráfico Multimedia sobre protocolo IP sobre una infraestructura de comunicaciones: es también un sistema que permite incorporar todos los sistemas de información y herramientas de productividad de una organización. El ahorro de costes es uno de los componentes principales impulsores de las Redes Convergentes; el soporte de aplicaciones altamente sofisticadas e integradas; y una mayor flexibilidad y funcionalidad de red.

Una red convergente además de ser apta para transmitir datos y voz también debe posibilitar un ambiente en el que coexistan servicios avanzados que integren estas capacidades, asegurando la utilidad de los mismos.

Existen y existirán inconvenientes técnicos que se debe superar en las redes de convergencia en virtud que los diversos servicios que se ofrecen tienen distintas particularidades y necesidades de red, por lo tanto es vital referir formas que aseguren calidad de servicio.

Normalmente, estos servicios se han prestado en forma separada sobre redes especializadas. La red de voz por ejemplo se fundamenta en uno o varios PBX (private Branche Xchange) enlazados a la PSTN (Public Switched Telephone Network) externa, entretanto la red de datos se fundamenta en Switches (conmutadores) y Router (enrutadores) IP (Internet Protocol) interconectando redes LAN (Local Area Network) y proporcionando el acceso a Internet.

Los elementos y protocolos de una red de convergencia son:

- Media gateways, mecanismo que permite la integración de distintos servicios de la red IP y otros como la red PSTN común o las redes inalámbricas.
- Gateways de señalización, es el responsable de traducir los protocolos de señalización de llamada dentro de las distintas redes.
- Controladores de media gateways es el responsable de coordinar a los media gateways en función de la señalización obtenida para el tráfico destino.

Protocolos:

- H.323: desarrollado por el ITU-T para normalizar el establecimiento de llamadas y la transmisión de multimedios en redes conmutadas por paquetes que no avalan ninguna QoS. H.323 se fundamenta en el RTP (Real Time Protocol) de IETF(Internet Engineering Task Force) y codecs estándares de la serie G. Pese a que este fue el primer protocolo usado en VoIP, el SIP (Session Initiation Protocol) de IETF ha obtenido aprobación porque tiene mecanismos más sencillos para el establecimiento de llamada.
- SIP: es un protocolo que logra establecer, cambiar y concluir sesiones o llamadas multimedios por medio de una red IP, incluyendo conferencias, aprendizaje a distancia, telefonía en Internet, etc., y pertenece al nivel de aplicación.
- MGCP: media gateway control protocol, se usa para controlar media gateways desde elementos externos mediante llamadas normales. Un protocolo alternativo que lo supera es MEGACO o H.248.
- SIGTRAN: es un conjunto de protocolos y niveles de adaptación usados para transportar información de señalización sobre redes IP

Asimismo por ejemplo, se consumen grandes volúmenes de ancho de banda cuando los datos se muestran en ráfagas durante cortos intervalos de tiempo, entretanto el tráfico de voz requiere un ancho de banda constante y un bajo retardo de transmisión.

La conmutación de circuitos basadas en multiplexación por división de tiempo (TDM) han satisfecho estas demandas del tráfico de voz, entretanto las redes de conmutación de paquetes han satisfecho el tráfico de datos. Bien que, la existencia de dos redes independientes compromete procesos de mantenimiento y administración independientes, con el debido incremento en costos y la dificultad para dar respuesta oportuna a los requerimientos de servicio de los clientes.

Adicionalmente, el tráfico de datos es mayor y crece exponencialmente en relación al tráfico de voz y este crece linealmente. Este hecho contrasta debido

a que el tráfico de voz genera las principales ganancias a las empresas de telecomunicaciones, realidad que se convierte en un atractivo especial en la integración de voz sobre la infraestructura ya existente, hecho que desembocaría en ofrecer mejores servicios a sus clientes y mayores ingresos para las empresas.

Normalmente se obtiene cargos elevados de telefonía (larga distancia) cuando se utiliza la red PSTN, lo que no sucede con Voz sobre IP, lo cual se considera como una de las mayores ventajas. Esto se debe a que la misma red sirve tanto para transportar voz y datos, principalmente cuando el usuario no utiliza el total de la capacidad de la red, misma que es utilizada por VoIP sin que esto signifique un costo adicional.

Esta realidad está presente en redes alambradas y en redes móviles inalámbricas, donde la llegada de la tercera generación supone la transición de la conmutación de circuitos a la conmutación de paquetes para convergencia de servicios. Y en este esfuerzo también se conduce al uso de voz (y video) empaquetada y a la aplicación de IP a través de toda la red.

En consecuencia, el vocablo VoIP define la transmisión de tráfico de voz digitalizada y empaquetada utilizando el protocolo IP. Los paquetes se exponen a sufrir retardos excesivos y, peor aún, variables en razón de que IP no fue esbozado para los requerimientos del tráfico de voz, para manipular inconvenientes relacionados con la calidad de voz como por ejemplo supresión de silencios y cancelación de ecos, VoIP se basa en procesos adicionales, implementados en los media gateways.

En aprovechamiento a la segregación de las funciones de enrutamiento y conmutación, la arquitectura MPLS que es un estándar del IETF, faculta ejecutar técnicas mejoradas de ingeniería de tráfico y funciones de calidad de servicio. Los paquetes IP son encapsulados en paquetes que contienen "labels" los cuales circulan en la red de conmutación de etiquetas dentro de lo que se conoce como conexión virtual denominada LSP (labels witched path) por MPLS.

La red telefónica tradicional (PSTN) no ha logrado un cambio significativo en el aspecto técnico a partir de su invención a fines del siglo XIX. Es claro que cada vez es menor el utilizar la red telefónica convencional (PTSN) para el envío de voz, ya que es mayor la tendencia de enviar señales de voz de manera digital, empaquetados por medio de la red. Por lo que se queda demostrado que la convergencia de la voz y los datos en una misma red, es una tecnología real.

Debido a la eficiencia los programas Open Source han obtenido gran aceptación tanto en el contexto empresarial, social y educativo, razón que los convirtió competitivos, en diversas áreas, en correspondencia a las aplicaciones propietarias existentes. Estos programas de código abierto han disminuido los problemas vinculados con los sistemas propietarios tradicionales logrando disminuir significativamente los costos, incrementar el mantenimiento y soporte técnico de equipos, así como también facultar el control del sistema de los equipos por parte de cada usuario.

Los costos bajos y el fácil acceso a los sistemas de comunicación VoIP (manuales, tutoriales, HowTo, URL oficiales, foros) son posible gracias al desarrollo de aplicaciones open source, lo cual facilita la implementación de estos sistemas.

1.2. Movilidad

Movilidad en Redes IP

Los servicios con independencia de terminales y redes pueden ser accedidos por los usuarios a través de la movilidad en redes IP. El usuario puede tener acceso al servicio desde cualquier red en cualquier lugar.

¿Por qué la movilidad de red?

El éxito de las tecnologías móviles ha generado que la movilidad cambie la manera de comunicarse de las personas. El servicio de acceso a Internet es cada vez más ubicuo, las peticiones de movilidad no se amurallan a una única terminal nunca más.

Es también necesario el soporte para la movilidad de una red completa que cambie este punto de unión de la infraestructura fija, manteniendo las sesiones

de cada dispositivo de la red; que es conocido como movilidad en red en redes IP. En este contexto, debe existir al menos un router (móvil) en la red de telefonía móvil que se conecta a la infraestructura fija, y este router móvil permite que los dispositivos de las redes móviles se conecten con el exterior.

El apoyo de la itinerancia o roaming de las redes que se mueven como un todo es requerido con el objetivo de posibilitar la prestación transparente de acceso a Internet en las plataformas móviles, como las que se detalla a continuación:

Los sistemas de transporte público.- Estos medios de tránsito posibilitan que viajeros en trenes, aviones, barcos, etc., logren acceder al servicio de Internet desde los terminales de a bordo (laptops, teléfonos celulares, asistentes digitales personales [PDA], y así sucesivamente) por medio de un router móvil emplazado en el vehículo de transporte que conecta a la infraestructura fija.

Las redes personales.- Las personas portan aparatos electrónicos, tales como PDAs, cámaras de fotos, etc., los cuales se conectan a través de un teléfono celular que actúa como router móvil de la red personal.

Escenarios Vehiculares.- Se augura que los autos del futuro se beneficiarán de tener conexión a la red de Internet, con varias finalidades tales como aumentar la seguridad (tal es el caso del uso de sensores que puede controlar múltiples aspectos de la operación del vehículo, la interacción con el medio ambiente y la comunicación con el Internet), así como también permitirán la comunicación personal, entretenimiento y servicios basados en los servicios de Internet.

Aunque, las redes IP no fueron diseñados para entornos móviles. Es así que las direcciones IP de IPv4 y Ipv6 ejercen roles distintos. Uno de ellos es que son localizadores que especifican, sobre la base de un sistema de enrutamiento, la manera de llegar al nodo que está utilizando esa dirección. El sistema de enrutamiento conserva la información de la forma cómo llegar a diferentes conjuntos de direcciones que tienen un prefijo de red común. Esta agregación de direcciones en el sistema de enrutamiento cumple con los requerimientos de escalabilidad. Otro rol es que, las direcciones IP son también parte de los identificadores de punto final de una comunicación, y las capas superiores el uso de los identificadores de los pares de una comunicación para

identificarlos. Es así que por ej., el Transmission Control Protocol (TCP), que es usado para ayudar la mayoría de las aplicaciones de Internet, usa la dirección IP como parte del identificador de la conexión TCP.

Es así también que se impone ciertas restricciones a la movilidad debido al rol desempeñado por las direcciones IP, en vista que cuando un terminal se moviliza de una red (subred IP) a otro, sería interesante mantener la dirección IP del nodo que se mueve (asociado a una de sus interfaces de red) con la finalidad de no cambiar el identificador que las capas superiores están usando en sus sesiones en curso. Aunque, también sería interesante modificar la dirección IP de manera que sea topológicamente correcta en la nueva ubicación de la terminal, admitiendo de esta manera el sistema de enrutamiento para llegar a la terminal.

La portabilidad de las terminales fue facilitada por protocolos como el Dynamic Host Configuration Protocol (DHCP), sin la intervención manual se permitió la adquisición dinámica de la información de configuración IP. Aunque, esta automatización no es suficiente para conseguir una movilidad real y transparente, ya que requiere el reinicio de sesiones en curso de transporte después cambia el punto de unión. El IETF ha estudiado el problema de la movilidad de terminales en las redes IP durante mucho tiempo, y la capa IP, las soluciones existe, tanto para IPv4 (IPv4 móvil) e IPv6 (IPv6 móvil) que permiten el movimiento de los terminales sin parar de sus sesiones en curso.

1.3. Escalabilidad

El dominio anhelado de una red, sistema o proceso, que enseña su habilidad para operar el continuo incremento de trabajo cuando se habla de telecomunicaciones o ingeniería informática se la conoce como escalabilidad. También es capaz de mostrar la disposición para crecer conservando la calidad en todos los servicios. La escalabilidad también se define como la idoneidad que puede llegar a tener un sistema informático de cambiar/alterar su tamaño y/o configuración para cumplir con los requerimientos del cambio.

Resulta un tanto complicado conceptualizar a la escalabilidad como un dominio de los sistemas, específicamente se hace necesario definir determinados

requisitos característicos de la escalabilidad en las medidas que se considere importante. Resulta una muestra muy significativa cuando se trata de sistemas electrónicos, equipos de red, bases de datos. Cuando se adiciona la capacidad del hardware y éste mejora en relación a la capacidad añadida es posible indicar que se ha aplicado el concepto de escalabilidad, el cual bien puede ser un sistema y/o equipos.

Escalabilidad en carga.- A través de un sistema distribuido se hace más fácil, en vista que se puede reducir e incrementar los recursos con mucha simplicidad de acuerdo a las necesidades de las cargas en función de que sean ligeras o pesadas.

Escalabilidad geográfica.- Cuando el uso de un sistema y todas sus características se conservan a pesar de la distancia de los usuarios se considera sistema escalable geográficamente.

Escalabilidad administrativa.- No debe importar que las organizaciones/empresas requieran distribuir un solo sistema distribuido, puesto que se debería manipular con mucha facilidad.

Escalada verticalmente.- Se define como vertical cuando se añaden recursos a un solo nodo del sistema, por ej., incrementar espacio de disco duro a un equipo.

Escalada horizontalmente.- Se define horizontal cuando se incrementan mas nodos al sistema, por ej., cuando se incrementan equipos a una aplicación para contingencia.

Red escalable

Se conoce como red escalable a una Red de Área Local que tiene la capacidad de ajustarse a un desarrollo posterior o futuro. Proyectar el número de tendidos y de derivaciones de cableado en el área de trabajo se convierte en un ítem de gran importancia a la hora de planificar. Es ventajoso instalar un número suficiente de cables adicionales a los requeridos a tener inconvenientes por la falta de ellos.

Se estima tender un cable extra para cada una de los puestos de trabajo con la finalidad de aceptar futuras ampliaciones y/o requerimientos, por lo que resulta necesario hacerlo también en el área de backbone. Resulta práctico mantener esta protección, ya que existe la posibilidad que fallen los cables de voz en el momento de la instalación. De forma similar es recomendable ubicar una cuerda de tracción en el momento de instalación lo que permitirá realizar un agregado de cables en cualquier momento.

Escalabilidad del backbone

Con el objetivo de conocer la proporción de cable adicional que requiere tender se debe en primera instancia determinar el número de tendidos que se requieren en ese instante y luego adicionar alrededor de un 20 por ciento más.

Utilizar cableado y equipamiento de fibra óptica en el edificio resulta ser otra manera diferente de lograr capacidad de reserva.

Escalabilidad del área de trabajo

Con el afán de adecuarse a las exigencias cambiantes de los usuarios en sus lugares de trabajo, se aconseja instalar mínimo un cable extra conectado a la toma en el área de trabajo. Las oficinas son capaces de convertirse de ser de un único usuario a una con múltiples usuarios. Esta realidad podría convertir al área de trabajo en un lugar poco eficiente si es que en un inicio solo se tuvo previsto cables para comunicaciones. Se estima una realidad que cada área tendrá múltiples usuarios.

1.4. Alta Disponibilidad

Técnicamente hablando fiabilidad es la probabilidad de que un servicio informático sea de cualquier índole funcione o se encuentre operativo en un período de tiempo establecido.

Alta disponibilidad, significa que determinado servicio informático y/o equipos informáticos cuenten con los mecanismos adecuados para que no dejen de operar; es decir; bajo circunstancias no adecuadas sigan funcionando.

Cuando determinado servicio informático deja de funcionar o presenta inconvenientes que no permiten un normal funcionamiento, se le conoce como falla, siendo ésta de dos tipos:

Servicio apropiado.- el sistema cumple a cabalidad con lo requerido.

Servicio inapropiado.- el sistema no cumple a cabalidad con lo requerido.

No siempre un error es sinónimo de falla en el sistema, pero siempre una falla es consecuencia de un error. Las formas de minimizar las fallas en el servicio son:

Prevención de errores.-, anticipar los errores para evitarlos.

Tolerancia a errores.-, tener a disposición un servicio de acuerdo con los requerimientos a pesar de los errores, presentando redundancias.

Eliminación de errores.-, tomar acciones correctivas con la finalidad de reducir la cantidad de errores.

Predicción de errores.- determinar el impacto en el servicio anticipando errores.

El índice de disponibilidad es un porcentaje que se encuentra dividiendo el tiempo en el cual el servicio está disponible por el tiempo total.

Tabla 1. Índice de disponibilidad de un servicio

Índice de disponibilidad	Duración del tiempo de inactividad
97%	11 días
98%	7 días
99%	3 días y 15 horas
99,9%	8 horas y 48 minutos
99,99%	53 minutos
99,999%	5 minutos
99,9999%	32 segundos

Evaluación de riesgos

Con la finalidad de restablecer los servicios informáticos dentro de un período de tiempo aceptable, es importante hacer una evaluación de los riesgos de los

eventos que se están asociados a las fallas de determinados componentes de un servicio informático, de forma que sea posible preparar los mecanismos y/o controles para evitar incidentes.

Se puede clasificar las fallas de la siguiente manera:

- Fallas por causas físicas (de origen natural o delictivo)
- Fallas por causa de desastres naturales (inundaciones, terremotos, incendios)
- Fallas por causa del medio ambiente (condiciones climáticas adversas, humedad, temperatura)
- Fallas por causas materiales
- Fallas por causa de la red
- Fallas por causa de cortes de energía
- Fallas por causas humanas (intencionales o accidentales):
 - ❖ Errores en el diseño (errores de software, aprovisionamiento de red insuficiente)
 - ❖ Fallas por causas operativas (vinculadas al estado del sistema en un momento dado):
 - Errores de software
 - Falla del software

Tolerancia a errores

Con la finalidad de ofrecer tolerancia a errores, existe un mecanismo que consiste en duplicar los recursos críticos, la cual se la conoce como redundancia.

Es así que se logra una tolerancia a errores cuando un componente falla, pero el sistema continúa operando.

Servicio de protección contra Fallas (FOS) es cuando uno de los recursos de un sistema falla, y los otros recursos siguen funcionando al tiempo que los administradores del sistema generan una solución al problema.

En el caso de que un dispositivo sufre un daño o avería el equipo o sistema debería permitir que la posibilidad de intercambiar en caliente el dispositivo; es decir reemplazar el daño sin interrumpir el servicio.

1.5. Interoperabilidad

El término interoperabilidad es la característica que admite que productos distintos puedan relacionarse entre sí, sin que esto signifique ambigüedad, para coordinar procesos o intercambiar datos. Se establece que las informaciones exactas para ejecutar la interoperabilidad se encuentren disponibles como Normas o Estándares.

Para un funcionamiento adecuado de las redes telefónicas e Internet es necesario cumplir con el concepto de interoperabilidad, en vista que faculta que las redes formadas por equipos heterogéneos junto con una amplia gama de productos informáticos y software. Cuando se habla de interoperabilidad en telecomunicaciones se hace referencia a la capacidad de las diferentes redes de comunicaciones de conectar usuarios de otras redes, de forma que los cambios en las aplicaciones y en los servicios prestados sobre las mismas sean completamente soportables o en su caso no se perciban las diferencias. Además, se conoce que la interoperabilidad entre productos se refiere a la característica de que un producto pueda ser sustituido por el de otro fabricante sin que esto sea motivo de que varíen las características funcionales. Por ej., en telecomunicaciones se podría mencionar a las redes de telefonía, que admiten realizar llamadas desde la red móvil a la red telefónica normal o a una red de telefonía IP.

La interoperabilidad para un usuario es transparente, puesto que es la capacidad de usar dispositivos o software sin la preocupación por la parte técnica.

1.5.1. Interoperabilidad de Redes

SNMP (Single Network Management Protocol)

El protocolo simple de administración de redes (SNMP) tiene la capacidad de observar e informar el estado entre una gran variedad de hosts.

El protocolo SNMP suministra una forma de administrar hosts de redes a través de un equipo centralizado que ejecuta un programa de administración de redes. Este protocolo permite ejecutar servicios de administración a través de una arquitectura distribuida de sistemas de administración y agentes.

Sistema de Administración: Es el host que se encuentra activo dentro de la red y que permite operar una aplicación de administración de Protocolo simple de administración de redes (SNMP). Dicha aplicación requiere datos de los agentes del protocolo SNMP. Se conoce como consola de administración al sistema de administración.

Agentes: Se conoce como agente al equipo que opera la aplicación agente de SNMP.

Usos de SNMP:

Configurar dispositivos remotos. Los datos de configuración de los host conectados a la red se los puede enviar desde el sistema de administración.

Supervisar el rendimiento de la red. La velocidad de procesamiento y el rendimiento de la red son parámetros que se pueden administrar, así como también se puede recabar información acerca de las transmisiones de datos.

Detectar errores en la red o accesos no autorizados. Cuando se produzcan determinados sucesos es posible configurar alarmas en los dispositivos de red. El sistema de administración recibirá un mensaje de suceso del dispositivo cuando se haya disparado una alarma. Una alarma se dispara frecuentemente por diversos motivos: accesos no autorizados, reinicio no programado de un dispositivo, errores en dispositivos, etc.

Auditar el uso de la red. Se vuelve necesario determinar ciertos parámetros para el uso de una red, por lo que también es posible controlar estos parámetros. El uso que se pueda dar a esta información varía dependiendo el contexto y la necesidad de cada lugar que se aplique.

Control de admisión QoS

El Control de admisión QoS muestra la forma centralizada con que se puede destinar el uso de los recursos de una red. (Cómo, cuándo quién). La

administración eficiente del uso del ancho de banda es un parámetro importante que no deben descuidar los administradores de redes, en especial porque los usuarios tienden a ejecutar multimedia (películas, videos, etc.) online. El Control de admisión QoS permite controlar este inconveniente puesto que no permite la utilización de un ancho de banda más que el asignado.

Interoperabilidad entre redes

La interoperabilidad entre redes es un problema con solución. Desde el punto de vista técnico actualmente nos enfrentamos a la interoperabilidad entre redes inalámbricas distintas por completo. Un claro ejemplo son los Smartphones, o teléfonos inteligentes, que admiten al usuario acceder a una gran variedad de servicios a través de Internet, utilizando distintas tecnologías para admitir la conexión a Internet. Mucho tiene que ver la distancia y el momento, el Smartphone se conecta por medio ciertas tecnologías disponibles, ya sea Wi-Fi, 3G, GPRS... sin embargo en cuanto nos trasladamos de ubicación o zona de cobertura, es muy probable que la tecnología que nos brinda el servicio de red puede cambiar, sin que esto afecte los servicios que estamos utilizando. Es deseable que el cambio de tecnología para proporcionar el servicio sea imperceptible para el usuario. La interoperabilidad entre redes es apreciable cuando se desea que un servicio provisto por una tecnología continúe sin alteraciones para el usuario cuando se cambia de tecnología. Ej., en zona Wi-Fi un video en Youtube y entramos en zona de cobertura 3G, es deseable que el servicio continúe sin que el usuario lo note, es decir sin alteraciones en el servicio.

Para permitir la interoperabilidad entre todo tipo de redes el IEEE ha creado el Grupo de Trabajo b (TGb) IEEE 802.21, que se encarga de estandarizar los traspasos entre redes de distintas tecnologías.

1.6. Seguridades

Hablar de seguridad redes, involucra varios contextos tanto interno como externo, los mismos que si llegan a tener algún tipo de intromisión no autorizada podrían comprometer de manera significativa la continuidad de las operaciones informáticas en una empresa.

La seguridad en las redes es un continuo riesgo al que se exponen todas las empresas por el mismo crecimiento de la tecnología lo cual lo vuelve vulnerable a cada instante por las habilidades que adquieren los atacantes, por lo que no se debe subestimar en lo más mínimo ninguna falla o vulnerabilidad existente.

Con la finalidad de evitar cierta complejidad en la detección y corrección de problemas de seguridad en la red, es necesario que en los criterios de diseño se prevea disponer de equipos y recurso humano responsable que permitan realizar una protección sistemática y continua para la protección de los sistemas, así como también evitar el crecimiento desordenado de equipos de red. Para conseguir este objetivo es necesario realizar un adecuado dimensionamiento de los puntos de datos requeridos para el personal con un crecimiento estimado que se encuentre entre el 25 al 50 % del total requerido.

Ejemplo: disponer de dos appliance de seguridad (firewall), el cual permita mantener un control de acceso a la red; en un esquema activo-pasivo o activo-activo con replicación simultánea, lo cual permitirá mantener un esquema de alta disponibilidad.

En la seguridad perimetral es recomendable disponer de un IDS (Intrusion Detection System) con la finalidad de detectar posibles ataques gracias a los sensores virtuales con los que cuenta, por ejemplo, un sniffer de red, este será un filtro de seguridad importante

Seguridad en la comunicación

Las tendencias tecnológicas modernas están dando lugar a un enfrentamiento en el ciberespacio entre hackers y profesionales de seguridad. Día a día se libra una batalla contra datos maliciosos que navegan en el Internet y las redes. Cada vez es más intenso este conflicto debido a que la globalización ha dado lugar a una sola red mundial lo cual convierte a múltiples redes en blancos más susceptibles.

En relación a la seguridad orientada a redes multiservicios se puede mencionar que los factores que se encuentran directamente ligados en las tendencias de las redes corporativas:

Convergencia.- Debido al tipo de aplicaciones como voz IP y multimedia las redes están adquiriendo esta característica, adicionalmente es de relevancia mencionar la considerable reducción de costos, aumento de la productividad, confiabilidad y alta disponibilidad. Cada vez es más evidente que la red se está tornando inteligente, al generar prioridades a las diversas aplicaciones según sea la necesidad de la empresa en un determinado momento.

Seguridad.- La seguridad tiene que ver de acuerdo al tipo, intensidad y frecuencia de los ataques. Hasta hace poco se debía proteger el perímetro de la red con la finalidad de evitar ataques desde fuera, hoy en día es un requisito proteger la red desde adentro; de los propios usuarios de la red que sin tener la intención podrían dañar la red.

Movilidad.- En la actualidad es cada vez más frecuente que el usuario tenga que acceder a la red empresarial remotamente, por lo que resulta necesario garantizar el servicio operativo como si estuviese en el lugar de trabajo.

Confiabilidad y recuperación.- Intenta mantener el concepto de niveles de servicio altos “cinco nueves”, lo que significa que cuando se presenten fallas la tecnología adoptada permita que la recuperación se dé en menos de un segundo; es decir, fallas de minutos en el año.

Firewall

Es idóneo poder mantener conectado un computador desde cualquier lugar de la red interna hacia cualquier lugar de la red externa, lo cual no siempre es una utilidad completa, porque desde el punto de vista de conexiones domésticas este hecho significaría navegación en Internet con mucha diversión; sin embargo para oficiales de seguridad de TI esto se torna en un ambiente gris. Existen un elevado número de compañías que mantienen en la red global grandes cantidades de información reservada y confidencial, lo cual constituye un alto riesgo si es que no se toman las debidas precauciones y esta información llega a caer en manos erróneas tendría consecuencias adversas.

Igualmente siempre se mantiene latente el peligro de fuga de información así como también persiste la amenaza de infiltración de información. Es muy conocido el tema de los comúnmente denominados virus informáticos, gusanos

y otros programas informáticos que se pueden infiltrar en la red y destruir información valiosa. Esto ocurre generalmente por el descuido de usuarios internos de la red. Estas son unas de las razones por las que se requiere mecanismos de seguridad para lograr mantener segmentados la información relevante así como también los programas o accesos que podrían causar daño intencional.

Es necesario entonces hablar de los firewalls (servidores de seguridad), el mismo que es un mecanismo que controla todas las E/S desde y hacia la red.

Los equipos de seguridad denominados firewalls constituyen una puerta de entrada por la cual están obligados a ingresar todos con el permiso respectivo (puertos); es decir que en una LAN todas las E/S pasarán por este filtro sin que exista alguna omisión involuntaria.

1.7. Redes

1.7.1. Redes LAN

Red de datos (LAN) sin backbone: Cuando las actividades de una empresa se centran en una sola planta, o en caso de que la cantidad de usuarios es mínima y tiene relación con la distancia física existente entre ellos, la solución de una red LAN no amerita la implementación de un backbone.

El switch que establece la conectividad en esta red, debe tener configurado VLANS para realizar un control de tráfico de broadcast, a la vez que se incorpora un elemento de seguridad interno de la red local.

1.7.2. Redes WAN

Las redes de Área Amplia (Wide Area Network) cubren grandes extensiones geográficas que bien pueden ser ciudades, países inclusive continentes, conectando múltiples equipos denominados hosts. El mejor ejemplo de una red WAN es el Internet.

1.7.3. Protocolos de Red

Los protocolos de red que se espera utilizar en el diseño de la LAN son:

802.1ad QinQ y QinQ selectivo: aumentan la escalabilidad de la red Ethernet a través de una estructura jerárquica; que permite enlazar diversas LAN en redes metropolitanas y de complejos de edificios de alta velocidad.

Rapid SpanningTreeProtocol (RSTP) es un protocolo de red ubicado en la capa dos del modelo OSI, (nivel de enlace de datos), que permite dirigir enlaces redundantes.

El **protocolo IEEE 802.1Q** es un protocolo que permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). El protocolo 802.1Q es el estándar utilizado para comunicar VLANS de distintos fabricantes. Esta comunicación es regularmente entre hosts de la misma VLAN ubicados en distintos switches.

El estándar IEEE 802.1p es un método para la asignación de prioridad a los paquetes que pasan por una red. Funciona con el MAC (Media Access Control) en la cabecera de capa dos (enlace de datos- modelo OSI).

QoS o Calidad de Servicio (Quality of Service) la calidad de servicio permite transmitir determinada cantidad de datos dentro de un tiempo dado (throughput). También se puede decir que es capacidad de brindar un servicio adecuado. Este es un parámetro muy apreciado en determinados servicios como transmisión de voz e imagen.

Gigabit Ethernet: soporta las nuevas innovaciones en tecnologías de networking y adhiere los conceptos de integración sobre IP, velocidades altas, QoS, escalabilidad, servicios administrados y costo eficiente.

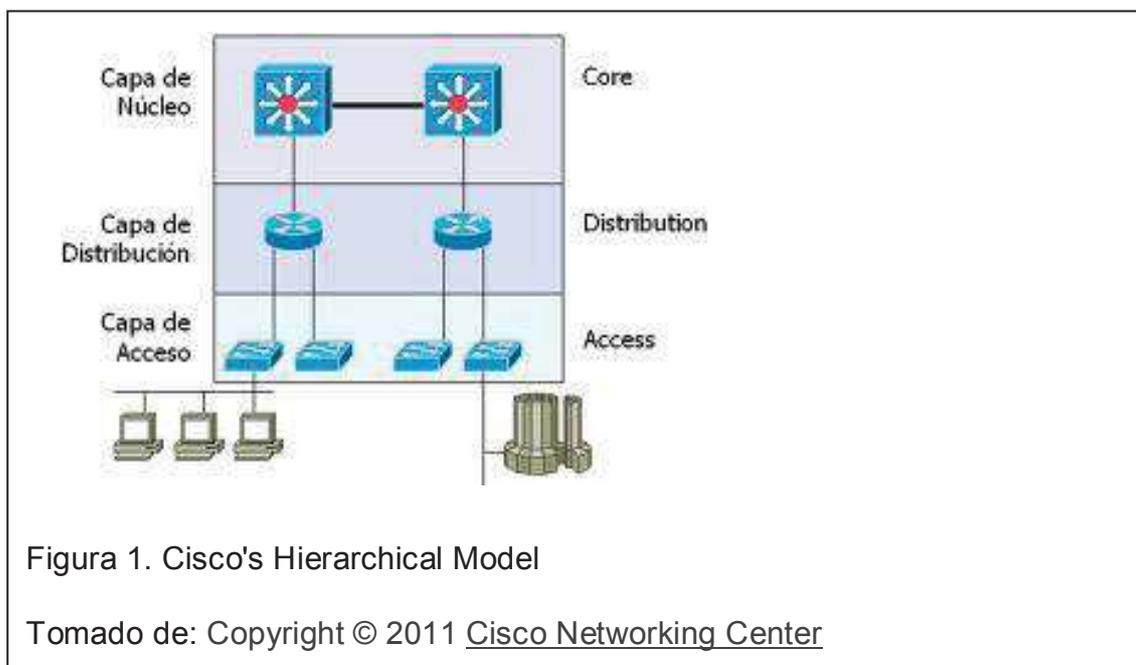
1.7.4. Modelo jerárquico de 3 capas

La construcción de una red de área local que cumpla con los requerimientos de clientes pequeños o medianos tiene posibilidades de éxito si se utiliza un modelo de diseño jerárquico. Es posible comparar con distintos modelos de diseños de redes, y se determina que una red jerárquica tiene la característica

de fácil administración y se expande con más facilidad de forma que los inconvenientes son resueltos rápidamente.

Se recomienda utilizar la metodología de diseño de CISCO (Cisco Press, 2008) para efectuar el diseño de la red LAN del centro de datos, ya que se define un modelo por capas, en virtud que se puede llegar a tener una alta complejidad en las redes e incluir múltiples protocolos; por lo que este diseño permite un modelo de red fácil de entender:

- Capa de Acceso o borde (Access Layer)
- Capa de Distribución (Distribution Layer)
- Capa de Núcleo (Core Layer)



Dentro de este modelo los dispositivos finales como las PC's, impresoras y teléfonos estarán ubicados en la capa de acceso o capa de borde en cada piso.

El objetivo fundamental de esta capa es permitir un medio de conexión entre los dispositivos a la red, y poder inspeccionar qué dispositivos pueden conectarse o no con la red. El equipamiento que se utilizará son los switches.

La capa de distribución es el medio de comunicación entre la capa de borde y la capa de núcleo. Esta capa tiene como finalidad proveer ruteo de tráfico entre diferentes grupos gracias a las VLAN-s, realiza el filtro de paquetes. La capa de

distribución verifica el tráfico de la red, traza los dominios de broadcast al efectuar el enrutamiento de las funciones entre las VLAN-s. El equipamiento que se utilizará son los routers.

La capa de núcleo es de vital importancia para la interconectividad entre los dispositivos de la capa de distribución. Literalmente es el núcleo de la red; en esta capa se concentra el equipamiento principal de los servicios informáticos y de aplicaciones de la Institución. Su función es conmutar tráfico de manera rápida ya que lleva cantidades de tráfico considerables de forma confiable y veloz. El diseño debe ser sumamente disponible y redundante. Se dispondrá de dos switches de core con la finalidad de dar alta disponibilidad.

1.8. Metodología de diseño

Como marco referencial se ha tomado en consideración a la metodología Top-Down Network Design. Por lo que se ha considerado en la metodología de diseño de la red como primer paso a la identificación de las necesidades y metas del cliente, segundo paso al análisis de los objetivos técnicos y compensaciones, tercero análisis de la red actual, luego el diseño de la red lógica y diseño del modelo.

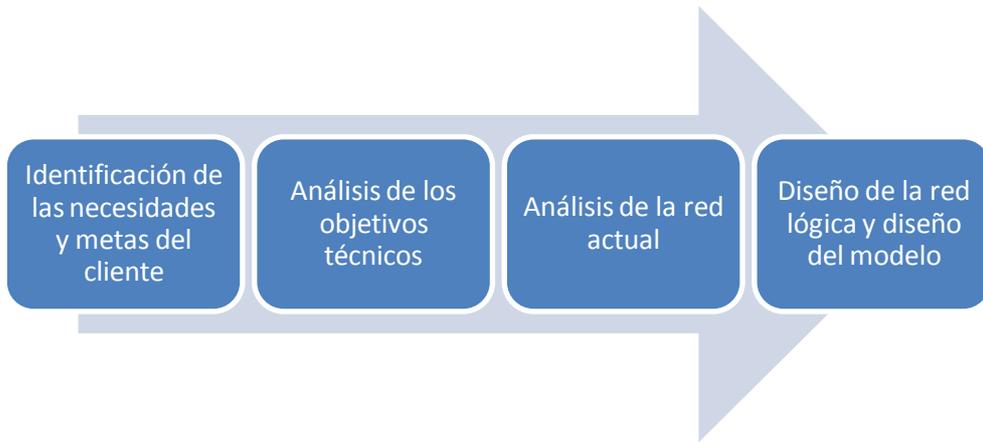
En la identificación del problema se ha realizado el levantamiento de los antecedentes que ha permitido determinar el problema actual de la red de datos de la Unidad de Análisis Financiero; además, se ha comprendido las metas a largo plazo de la Institución.

En el análisis de los objetivos técnicos se ha propuesto como meta realizable los cambios a nivel de red de datos que requiere la Institución.

En el análisis de la red de datos actual se ha identificado los requerimientos y alcances a nivel de red de datos que tiene la Institución, así como también las necesidades en cuanto a servicios informáticos.

En el diseño de la red lógica se ha logrado plasmar los objetivos propuestos sobre las necesidades identificadas y metas planteadas.

Pasos de la metodología utilizada:



2. Capítulo II. Análisis y Definición de Requerimiento

2.1. Unidad de Análisis Financiero

La LEY DE PREVENCIÓN, DETECCIÓN Y ERRADICACIÓN DEL DELITO DE LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DE DELITOS tiene por finalidad prevenir, detectar oportunamente, sancionar y erradicar el lavado de activos y el financiamiento de delitos, en sus diferentes modalidades. Para el efecto, son objetivos de esta Ley los siguientes: (Registro Oficial Suplemento 352, 2010, Tít.I, Cap.I, Art.1)

- 1) Detectar la propiedad, posesión, utilización, oferta, venta, corretaje, comercio interno o externo, transferencia gratuita u onerosa, conversión y tráfico de activos, que fueren resultado o producto de delitos, o constituyan instrumentos de ellos, para la aplicación de las sanciones correspondientes; (Registro Oficial Suplemento 352, 2010, Tít.I, Cap.I, Art.1, Lit.a.)
- 2) Detectar la asociación para ejecutar cualesquiera de las actividades mencionadas en el literal anterior, o su tentativa; la organización de sociedades o empresas que tengan ese propósito; y, la gestión, financiamiento o asistencia técnica encaminados a hacerlas posibles, para la aplicación de las sanciones correspondientes; (Registro Oficial Suplemento 352, 2010, Tít.I, Cap.I, Art.1, Lit.b.)
- 3) Decomisar, en beneficio del Estado, los activos de origen ilícito; y, (Registro Oficial Suplemento 352, 2010, Tít.I, Cap.I, Art.1, Lit.c.)
- 4) Realizar las acciones y gestiones necesarias para recuperar los activos que sean producto de los delitos mencionados en esta Ley, que fueren cometidas en territorio ecuatoriano y que se encuentren en el exterior. (Registro Oficial Suplemento 352, 2010, Tít.I, Cap.I, Art.1, Lit.d.)

2.1.1. De la Información

Además de las y los sujetos obligados a informar, quienes conocieren de hechos relacionados con los delitos mencionados en esta Ley los informarán a las autoridades competentes y, en el caso de que conozcan de la existencia de

operaciones o transacciones económicas inusuales e injustificadas, informarán de ello a la Unidad de Análisis Financiero (UAF). Se entenderá por operaciones o transacciones económicas inusuales e injustificadas los movimientos económicos, realizados por personas naturales o jurídicas, que no guarden correspondencia con el perfil que éstas han mantenido en la entidad reportante y que no puedan sustentarse. (Registro Oficial Suplemento 352, 2010, Tít.I, Cap.I, Art.2.)

La Unidad de Análisis Financiero (UAF) es la dependencia competente para receptor toda clase de información y reportes relacionados con los delitos de lavado de activos y el financiamiento de delitos. (Registro Oficial Suplemento 352, 2010, Tít.I, Cap.I, Art.2., párr.2.)

La Unidad de Análisis Financiero (UAF) es el órgano operativo del Consejo Nacional Contra el Lavado de Activos. Está conformada por la Dirección General, la Subdirección y los departamentos técnicos especializados, cuyas funciones y atribuciones estarán determinadas en el Estatuto Orgánico por Procesos de la Unidad de Análisis Financiero (UAF). (Registro Oficial Suplemento 352, 2010, Tít.III, Cap.I, Art.9.)

La Unidad de Análisis Financiero (UAF) solicitará y recibirá, bajo reserva, información sobre operaciones o transacciones económicas inusuales e injustificadas para procesarla, analizarla y de ser el caso remitir un reporte a la Fiscalía General del Estado, con carácter reservado y con los debidos soportes. (Registro Oficial Suplemento 352, 2010, Tít.III, Cap.I, Art.9.párr. 2.)

De ser el caso, la Unidad de Análisis Financiero (UAF) atenderá requerimientos de información de la Secretaría Nacional de Inteligencia, conservando la misma reserva o sigilo que pese sobre ella. (Registro Oficial Suplemento 352, 2010, Tít.III, Cap.I, Art.9.párr. 3.)

2.1.2. De las Funciones y Atribuciones

La Unidad de Análisis Financiero (UAF) deberá cumplir las siguientes funciones: (Registro Oficial Suplemento 352, 2010, Tít.III, Cap.II, Art.10.)

- 1) Elaborar programas y ejecutar acciones para detectar, de conformidad con esta Ley, operaciones o transacciones económicas inusuales e injustificadas, con la finalidad de promover, de ser el caso, su sanción y recuperar sus recursos; (Registro Oficial Suplemento 352, 2010, Tít.III, Cap.II, Art.10, lit.a)
- 2) Solicitar de los sujetos obligados a informar, de conformidad con lo previsto en esta Ley, la información que considere necesaria para el cumplimiento de sus funciones, con la finalidad de procesarla, analizarla y custodiarla; y, de ser el caso, respecto de la información que le haya sido entregada, solicitar aclaraciones o ampliaciones; (Registro Oficial Suplemento 352, 2010, Tít.III, Cap.II, Art.10, lit.b)
- 3) Coordinar, promover y ejecutar programas de cooperación con organismos análogos internacionales y unidades nacionales relacionadas para, dentro del marco de sus competencias, intercambiar información general o específica relativa al lavado de activos y financiamiento de delitos; así como ejecutar acciones conjuntas, rápidas y eficientes a través de convenios de cooperación en todo el territorio nacional incluidas las zonas de frontera; (Registro Oficial Suplemento 352, 2010, Tít.III, Cap.II, Art.10, lit.c)
- 4) Remitir exclusivamente a la Fiscalía General del Estado el reporte de operaciones inusuales e injustificadas que contendrá el análisis correspondiente con los sustentos del caso, así como las ampliaciones e información que fueren solicitadas por la Fiscalía; en consecuencia, la Unidad de Análisis Financiero queda prohibida de entregar información reservada, bajo su custodia, a terceros con la excepción prevista en el último inciso del artículo anterior; (Registro Oficial Suplemento 352, 2010, Tít.III, Cap.II, Art.10, lit.d)
- 5) Crear, mantener y actualizar, con carácter reservado, una base de datos con toda la información obtenida como producto de sus actividades, de conformidad con el reglamento correspondiente;(Registro Oficial Suplemento 352, 2010, Tít.III, Cap.II, Art.10, lit.e)

- 6) Organizar programas periódicos de capacitación en prevención de lavado de activos y del financiamiento de delitos; (Registro Oficial Suplemento 352, 2010, Tít.III, Cap.II, Art.10, lit.f)
- 7) Contratar, cuando sea del caso, empresas especializadas en ubicación de fondos y activos ilícitos, con la finalidad de gestionar su recuperación; y,(Registro Oficial Suplemento 352, 2010, Tít.III, Cap.II, Art.10, lit.g)
- 8) Las demás que le correspondan, de acuerdo con esta Ley y su reglamento general. (Registro Oficial Suplemento 352, 2010, Tít.III, Cap.II, Art.10, lit.h)

2.2. Análisis de la Situación Actual

La información acerca de la situación actual, se la obtuvo al realizar un levantamiento de información con reuniones realizadas con el Director de Gestión Tecnológica de la UAF y con las personas responsables de los sub-procesos en la mencionada Área, en la que se recopiló la siguiente información:

Tabla 2. Situación actual de la UAF

Levantamiento de información de la Situación Actual de la UAF	
Redes de Datos	
Cableado estructurado	
Categoría:	5e
Certificación	Panduit
Conector	RJ45
Tipo de cable	UTP(Par trenzado no blindado)
Vel. Máx.	1 Gbps
Estándares de instalación de cableado	568A, 568B
Centro de Datos	

Área de construcción	El Centro de Datos es una oficina de 16m ² adecuada para el efecto y no cumple con el área mínima para los armarios y equipos actuales.
Centro de Datos	No cuenta con un área para almacenamiento de equipos y medios libre de circulación de tuberías de gas natural o propano
Puerta del Centro de Datos	No cumple ningún estándar de Centro de Datos
Piso falso	Medidas 60x60 Instalado sobre gatos y cumple con las características de ser antiestático, aislante, no inflamable y no combustible
Accesos directo al perímetro del predio	El Centro de Datos cuenta con ventanas de acceso directo
Sistema de Control de Acceso	No cuenta con un sistema de control de acceso
Cuarto de UPS's	El cuarto de Centro de Datos no cuenta con un área adicional para los equipos UPS's
Sistema de Enfriamiento	El cuarto de Centro de Datos cuenta con un sistema de aire acondicionado a presión de 24000 BTU's, sin redundancia, el mismo que ha presentado inconvenientes técnicos, tiene 5 años de vida útil cumplidos.
Estándares	No cumple
Equipos de red	
Switch	3COM 24 puertos
Switch	3COM 48 puertos
Switch	CISCO 24 puertos
Apliance	Check point UTM 270
Equipos servidores	
(4) HP DL 360 G5	
(6) HP DL 380 G5	

(1) HP ML 350 G5	
Aplicaciones	
Misional	Sistema de carga de reportes en línea JAVA 2EE Servidor a Aplicaciones JBOSS v5.0
Contabilidad	Spyral Oracle 10g
Documentación	SISDOC Lotus Domino v.8
Correo	Sendmail
Página Web	Apache/2.2.3 PHP 5.1.6 Mysql v.5.0.22 Joomla v.
Servicios de Red	Sendmail 8.13.8
S.O.	Linux RedHat Enterprise v.5.5
Equipos de escritorio	
Computadores/Laptops	HP Processor RAM 2GB Windows XP/VISTA
Equipos de oficina	
Impresoras Laser	11
Copiadoras	4
Plotter	2
Scanner	5
Equipos de telecomunicaciones	
	No existe
Políticas de seguridad	

	No existe
Políticas de mantenimiento	
	No existe

En referencia al levantamiento de información realizado se puede mencionar que:

La Unidad de Análisis Financiero, antiguamente llamada Unidad de Inteligencia Financiera (UIF) entró en operación en el año 2008 con una infraestructura básica de acuerdo al siguiente detalle:

Tabla 3. Servicios iniciales UAF

Equipamiento	Servicios
Servidor HP ML350	Conexión con el MEF
Servidores HP DL360 G5	Web, Correo Electrónico, Proxy, DNS Sistema de Gestión Documental

Estos servicios informáticos básicos dieron inicio a las operaciones de la Unidad de Análisis Financiero.

2.2.1. Aplicaciones

La Unidad de Análisis Financiero con el objetivo de cumplir su misión inició sus operaciones de recepción de reportes de transacciones que superan el umbral y reportes de operaciones inusuales e injustificadas desde el Sistema Financiero Nacional de manera física, es decir; recibiendo la información a través de medios magnéticos físicos (CD's).

En el año 2010 se automatizó el proceso de recepción de reportes con el desarrollo de un sistema web denominado Sistema de Reportes, que permitiría recibir las transacciones que superan el umbral y los reportes de operaciones inusuales e injustificadas.

Con la reforma de la Ley para Reprimir el Lavado de Activos actualmente denominada LEY DE PREVENCIÓN, DETECCIÓN Y ERRADICACIÓN DEL DELITO DE LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DE DELITOS, se incrementó el número de sujetos obligados a reportar:

A más de las instituciones del sistema financiero y de seguros, serán sujetos obligados a informar a la Unidad de Análisis Financiero (UAF) a través de la entrega de los reportes previstos en el artículo 3 de esta Ley, de acuerdo a la normativa que en cada caso se dicte: las filiales extranjeras bajo control de las instituciones del sistema financiero ecuatoriano; las bolsas y casas de valores; las administradoras de fondos y fideicomisos; las cooperativas, fundaciones y organismos no gubernamentales; las personas naturales y jurídicas que se dediquen en forma habitual a la comercialización de vehículos, embarcaciones, naves y aeronaves; las empresas dedicadas al servicio de transferencia nacional o internacional de dinero o valores, transporte nacional e internacional de encomiendas o paquetes postales, correos y correos paralelos, incluyendo sus operadores, agentes y agencias; las agencias de turismo y operadores turísticos; las personas naturales y jurídicas que se dediquen en forma habitual a la inversión e intermediación inmobiliaria y a la construcción; los casinos y casas de juego, bingos, máquinas tragamonedas e hipódromos; los montes de piedad y las casas de empeño; los negociadores de joyas, metales y piedras preciosas; los comerciantes de antigüedades y obras de arte; los notarios; y, los registradores de la propiedad y mercantiles. (Registro Oficial Suplemento 352, 2010, Tít.I, Cap.II, Art. ...)

Este hecho impacta directamente en la prestación del servicio que provee el sistema de reportes, puesto que afecta a los recursos del equipo en el que se encuentra alojado el software mencionado y provoca que el servicio no sea eficiente eficaz y oportuno.

Además, este hecho también impacta en el número de concurrencias que tiene equipo servidor Web, puesto que el diseño actual de los equipos no cuenta con un balanceador de carga; es decir no cuenta con un esquema de alta disponibilidad; además esta situación exige mayor calidad y cantidad de

respuesta por parte de los funcionarios en cuanto a gestión interna se refiere, es decir, se requerirá mayor performance en comunicaciones a nivel LAN por el incremento de demanda de peticiones de servicios tales como respuesta a oficios, respuesta a solicitudes de soporte técnico (call center) a sujetos obligados.

La información existente es confiable, sin embargo por el incremento de sujetos obligados a reportar, el sistema de almacenamiento requiere un upgrade urgente, así como también un sistema de respaldos adecuado, puesto que el actual es un sumamente básico y no permite realizar respaldos incrementales.

El Sistema de Gestión Documental fue desarrollado en LOTUS DOMINO en el año 2008, el mismo que persiste hasta la actualidad; sin embargo no cuenta con personal técnico capacitado que pueda dar soporte y mantenimiento al mismo.

2.2.2. Hardware

La ausencia de una gestión tecnológica apropiada, ha generado que el crecimiento de la infraestructura tecnológica marque una obsolescencia tecnológica, lo cual genera dificultades para un crecimiento apropiado.

Como equipos para impresión se utiliza dos tipos de impresoras láser y de red.

Todas las áreas cuentan con computadoras y sistemas de impresión que no se encuentran integrados a través de la red de datos, sino que prestan servicios exclusivamente a los usuarios que las operan.

Los computadores personales y equipos de impresión tienen un tiempo de vida útil de alrededor de 4 años, los mismos que no han sido adquiridos ni puesto en operación respondiendo a un plan de equipamiento, es producto de iniciativas de los funcionarios en base a las necesidades de proporcionar soluciones a requerimientos puntuales de los usuarios.

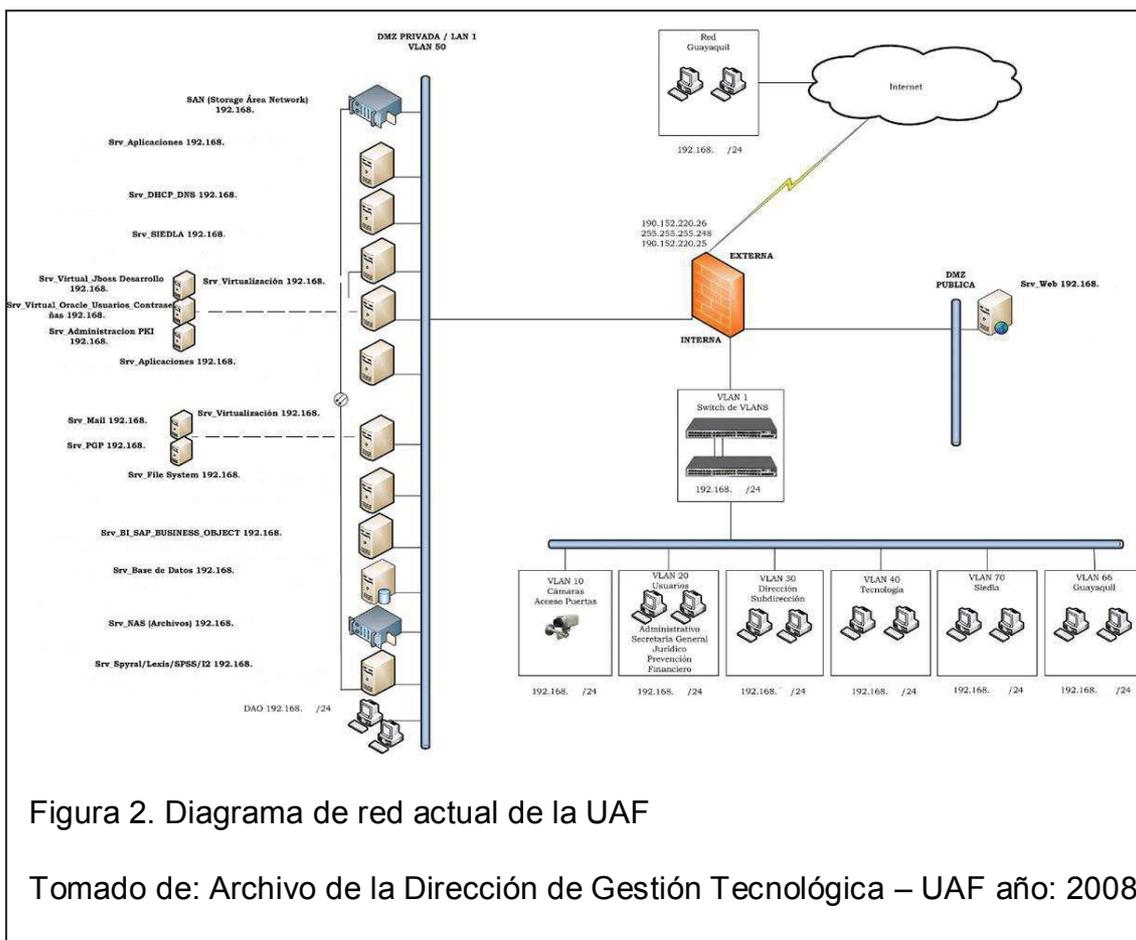
En el siguiente detalle se muestra la distribución, cantidad y tipo de equipos con que cuenta actualmente la Institución:

Tabla 4. Detalle de equipamiento Institucional

Área	Computador Personal	Impresoras Láser
Administrativo-Financiero	6	1
Talento Humano	2	1
Tecnología	10	1
Secretaría General	4	1
Análisis	16	2
Jurídico	8	2
Dirección General	7	3

2.2.3. Red LAN

La Institución cuenta con una red LAN que tiene configuradas VLAN's con un cableado categoría 5e, Switches capa 2 y capa 3, con un firewall que permite administración de red y permite segmentar la zona militarizada y desmilitarizada.



La Institución cuenta con 3 Switches marca 3COM modelo 5500G de 24 Ptos, actuando en modo de stacking, virtualizando los switch como una sola unidad, interconectados entre sí a través de enlaces de 10Gb. Esta configuración provee redundancia en los caminos de interconexión entre el grupo de switches y conectividad hacia un switch Cisco que posee la entidad. No existe redundancia o alta disponibilidad entre switches, por ello ante la falla de un switch dentro del stacking se pierde la conectividad.

2.2.4. Políticas de Mantenimiento

Tanto el hardware, el software y telecomunicaciones no cuentan con políticas de mantenimiento.

Las aplicaciones no cuentan con políticas de control de calidad de las versiones generadas cuando se realiza mantenimiento. Los programadores asignados tienen el dominio total de las aplicaciones a su cargo, no se lleva

adecuadamente un procedimiento de manejo de versiones ni de control de cambios. Los programadores realizan las modificaciones, prueban y ponen en producción los cambios realizados.

El área de infraestructura realiza tres mantenimientos anuales del equipamiento del Centro de Datos con soporte técnico externo, en vista que no cuenta con personal ni capacitación adecuada para el efecto.

2.2.5. Recurso Humano

El Recurso Humano de la Dirección de Gestión Tecnológica se encuentra en proceso de renovación de conocimientos con la finalidad de contar con una idea clara de conceptualización de tecnología orientada a alta disponibilidad, movilidad, interoperabilidad, escalabilidad, y de esta manera estar en la capacidad de solventar los requerimientos de la plataforma tecnológica que requiere la Institución, y así lograr altos índices de rendimiento y disponibilidad.

2.3. Definición de Requerimientos

La Unidad de Análisis Financiero, actualmente ejecuta sus actividades en una casa adecuada para oficinas, propiedad que se encuentra dentro de un proceso judicial que todavía no se halla ejecutoriado, por lo que es necesario realizar la adquisición o arrendamiento de un espacio adecuado para el funcionamiento de la Institución.

La misión del presente documento basado en las directrices dictadas en el Plan Estratégico de la Dirección de Gestión Tecnológica tiene como finalidad plantear la referencia a partir del cual se diseñará las redes y servicios informáticos para las nuevas oficinas de la Unidad de Análisis Financiero.

El número de equipos que se requerirá por Área se lo ha definido en base a las proyecciones que tiene la Institución considerando el incremento de sujetos obligados a reportar y el esfuerzo que ese hecho conlleva.

Se estima que el nuevo espacio físico donde funcionarán las oficinas de la Unidad de Análisis Financiero se encuentren repartidas en cinco pisos de un edificio alquilado para este fin.

2.3.1. Aplicaciones Informáticas

El sistema de reportes con el que cuenta la Unidad de Análisis Financiero, requiere ser adecuado para que permita que todos los sujetos obligados a reportar de los diferentes sectores económicos puedan enviar el reporte de las transacciones que superan el umbral y el reporte de operaciones inusuales e injustificadas.

El diseño de la infraestructura requiere que la referida aplicación sea puesta en producción de acuerdo a criterios como:

El acceso a las aplicaciones deberá encontrarse operativa vía web tanto desde el Internet como también desde cualquier sucursal, misma que se encuentra dentro de los objetivos Institucionales.

Los módulos que permiten el acceso a los funcionarios analistas deben ser accedidos exclusivamente por personal autorizado, en un horario establecido.

La red de datos debe permitir tráfico de voz, datos y video dentro de un mismo medio, considerando un ancho de banda que permita que los servicios de telefonía IP, circuito de seguridad por cámaras IP, etc., cumplan con las necesidades de los usuarios

2.3.2. Servicios Informáticos

Es necesaria la implementación de servicios informáticos que permitan la agilidad de los procesos administrativos, considerando la operación diaria enmarcada en las necesidades de los usuarios.

Servicio de:

- a) Correo electrónico,
- b) Internet,
- c) Intranet,
- d) Servicios de red (DNS, DHCP, NFS, PROXY, NTP)

2.3.3. Equipo Informático

Las computadoras de escritorio deberán tener instalado un software que permita encriptar el disco duro y bloquear todos los puertos E/S excepto teclado y mouse. Además deberá contener software regido por licencias GPL del Software Libre. Es necesario mantener un estándar en el software instalado en todos los equipos con que cuenta la Institución.

Los equipos servidores destinados a servicios web y de red deben permitir alta velocidad de respuesta, contar con una tecnología diseñada para soportar cargas de trabajo elevadas sujetas a alta disponibilidad. Tanto los discos duros como las fuentes de alimentación deben tener una capacidad Hot Swap. Sistema Operativo base Linux.

Todos los equipos servidores deberán tener un sistema de almacenamiento centralizado en red (Storage Area Network) en alta disponibilidad.

La solución de impresión debe permitir trabajo en red con alta capacidad de rendimiento, tomando en consideración el número de clientes.

Para obtener un dimensionamiento aproximado de los requerimientos de equipos informáticos de cada departamento de acuerdo a los objetivos institucionales y de acuerdo a un sondeo de opinión se estima que aproximadamente en dieciocho meses la Institución tendrá un incremento significativo de funcionarios tanto técnicos de análisis, informáticos, personal administrativo y funcionarios de nivel jerárquico superior, por lo que se cree conveniente considerar el siguiente requerimiento:

Tabla 5. Requerimiento de equipamiento informático Institucional

UNIDAD DE ANÁLISIS FINANCIERO			
EQUIPAMIENTO INFORMÁTICO INSTITUCIONAL			
Área	Computadores de escritorio	Impresoras	Computador portátil

Dirección General	31	6	5
Asistentes			
Secretario			
Asesorías			
Subdirección			
Asistentes			
Secretario			
Asesorías			
Secretaría General	4	2	0
Recepción – Call Center	9	2	0
Prevención	20	3	3
Tecnología	21	1	3
Administrativa Financiera	12	2	1
Recursos Humanos	4	1	1
Análisis	24	3	1
Jurídico	8	1	1
Relaciones Internacionales	4	2	3
Guayaquil	5	1	1
Cuenca	5	1	1
TOTAL:	147	25	20

2.3.4. Equipamiento de Red LAN y WAN

La infraestructura debe soportar voz, datos, video para lo cual el diseño de red de telecomunicaciones debe permitir criterios de convergencia, movilidad, escalabilidad, interoperabilidad y alta disponibilidad a través de la integración de protocolos de calidad de servicio, priorización y clasificación de paquetes.

Los equipos que destinados a ser eje de LAN deben estar diseñados a trabajar con la premisa de alta disponibilidad.

La Institución mantiene la idea de estandarizar tanto el hardware como el software con el objetivo de facilitar la administración, mantenimiento y operación.

Es conveniente que el cableado estructurado esté de acuerdo a los estándares del TIA/EIA, con la finalidad de que la red de datos sea capaz de tener un control de la seguridad y que los datos que circulan por la misma sean confiables, y por ende se pueda certificar el cableado.

Se estima que el requerimiento del cableado estructurado sea de categoría 6a, con la finalidad de que permita la transmisión de datos, voz y video a una velocidad estándar a las herramientas existentes en el mercado. La Institución como ente ejecutor de la Ley de Prevención Detección y Erradicación de Lavado de Activos y Financiamiento de Delitos, tiene por finalidad analizar los reportes de todos los diversos sectores económicos del país y debido a la alta transaccionalidad en días pico y la premisa de entregar los reportes de incumplimiento en días posteriores a los días 15 o fin de mes, se vuelve estrictamente necesario un ancho de banda que permita el envío y recepción de paquetes de distintos tamaños a nivel de la red LAN a tasas de velocidad aceptables.

La Institución mantiene una aplicación para el manejo de documentos denominada Sistema Documental (SISDOC), a través de la cual se despachan diariamente documentos. Los usuarios internos requieren enviar paquetes de datos desde 25KB hasta 2MB aproximadamente. Para realizar el cálculo de ancho de banda requerido se realiza en base a la siguiente fórmula:

$$AB = G \times C$$

G = Tamaño del archivo a enviarse dividido para el tiempo estimado de carga

C= Número de usuarios concurrentes

Tamaño archivo máximo = 2MB

Tiempo estimado= 1 minuto

$$G=2MB / (1 \times 60\text{seg})$$

$$G=0,034\text{Mbps}$$

$$C=80$$

$$AB=80 \times 0.034\text{Mbps} = 2,72 \approx AB= 3\text{Mbps}$$

Adicionalmente, el servicio de correo electrónico requiere un estimado de 25KB hasta 8MB de envío de paquetes por usuario, lo que significa un incremento del consumo de ancho de banda. Para conocer la capacidad de ancho de banda requerida se debe utilizar la misma fórmula anterior:

$$AB = G \times C$$

G = Tamaño del archivo a enviarse dividido para el tiempo estimado de carga

C= Número de usuarios concurrentes

Tamaño archivo máximo = 8MB

Tiempo estimado= 1 minuto

$$G=8\text{MB} / (1 \times 60\text{seg})$$

$$G=0,134\text{Mbps}$$

$$C=80$$

$$AB=80 \times 0.134\text{Mbps} = 10,72 \approx AB= 11\text{Mbps}$$

La Institución como parte de su seguridad física interna tiene previsto implementar un sistema de video vigilancia a través de cámaras IP, lo cual significa que el tráfico de video en la red LAN ocuparía un ancho de banda considerable. Para tener una idea clara del ancho de banda necesario para este servicio se debe tener en cuenta ciertos aspectos como: número de cámaras, tiempo en el día que la cámara estará grabando, resolución de la imagen, frames por segundo, tipo de compresión de video. Por la naturaleza de la Institución se prevé que la configuración de las cámaras será para imágenes de alta calidad y alta frecuencia lo que significa que se tendría un uso de ancho de banda aproximado de 2 a 3Mbit/s. Para la transmisión de datos generalmente existen dos tipos de velocidades: efectiva que es la cantidad real de datos que el canal transmite y la velocidad nominal que es más grande que la efectiva, la cual asocia caracteres de control, maneja pérdidas, fallas, colisiones, etc. Se asume que la velocidad efectiva es un cuarenta por ciento

(40%) de la nominal. Para calcular el ancho de banda necesario para este requerimiento es posible utilizar la siguiente fórmula:

$$AB = \text{Velocidad} \times \text{Promedio del tamaño de cada imagen} \times \% \text{ de actividad} \times 8$$

La velocidad es el número de cuadros de la imagen y se expresa en (fps). De acuerdo al estándar NTSC (*National Television System Committee*) se considera la velocidad en 30fps. El tamaño de la imagen en promedio depende del dispositivo y del tipo de algoritmo de compresión (*MPEG4 Layer 2 más usado*) que se utilice, se expresa en Bytes, el fabricante proporciona este dato, por lo que regularmente se puede considerar que usa 12KBytes en el día y el doble en la noche; el tipo de escena también influye en el tamaño de la imagen en promedio, Ej.: más color, más tamaño. El porcentaje de la actividad de la escena es un parámetro importante, para lo cual es necesario considerar las horas de alto, medio y bajo tráfico. Por la naturaleza de la Institución se tomaría tráfico alto de 8 horas, y tráfico bajo de 16 horas, con muestras de tiempo simuladas quedaría así:

Muestra del porcentaje de actividad de la escena a las 8:p.m.:

Tiempo de muestra 5 min.=300s, tiempo de actividad=15s

$$15 \times 100 / 300 = 5,34\%$$

Muestra del porcentaje de actividad de la escena a las 10:a.m.:

Tiempo de muestra 5 min.=300s, tiempo de actividad=215s

$$215 \times 100 / 300 = 71,67\%$$

Ahora, bien para el cálculo del ancho de banda se aplica la fórmula expresada, quedando de la siguiente manera:

$$\text{Para el día } AB = 30 \text{fps} \times 12 \text{kBytes} \times 71,67\% \times 8 = 30 \times 12 \times 0,7167 \times 8 = 2064,096 \text{Kbps}$$

$$\text{Para la noche } AB = 30 \text{fps} \times 24 \text{KBytes} \times 5,43\% \times 8 = 30 \times 24 \times 0,0543 \times 8 = 312,768 \text{Kbps}$$

Estos valores son para una sola cámara, se debe multiplicar cada resultado por el número total de cámaras y se tendría un número estimado de ancho de banda requerido.

Se tiene previsto también la incorporación del servicio de telefonía IP, por lo que el tráfico de envío y recepción de paquetes de voz incrementaría notablemente en el ancho de banda de la red. Para el cálculo de este parámetro se debe considerar dos factores: número de llamadas concurrentes así como también, CODEC, opciones de compresión, etc. Para este cálculo se debe considerar el tamaño de la trama, suponiendo que se utilizará un algoritmo de compresión común (G.729a,) que tiene una longitud de 50Bytes, más los encabezados de la capa 2, capa 3, y capa 4 que son aproximadamente 40Bytes, y considerando que se utilizará la trama del protocolo punto a punto se adicionará 6Bytes. Los encabezados de las capas 2,3,4 deben ser comprimidos por lo que se tendría 2Bytes; el resultante sería:

tamaño de la trama: Payload + Enc. 4 + Enc. 3 + Enc. 2

tamaño de la trama: 50B + 2B + 6B = 58B

58bytes x 8bits/byte = 464bits/trama

Ahora para calcular el ancho de banda por llamada se tendría que calcular multiplicando el tamaño de la trama por la cantidad de tramas que se envían por segundo, considerando que el tamaño del CODEC (G.711, G.728, G.728) generan 50 tramas por segundo, se tendría:

AB/llamada = tamaño de la trama x tramas por segundo

AB/llamada = 464bits/trama x 50 tramas/seg. = 23200 bps/llamada

El ancho de banda es la cantidad de información que se puede transmitir por un canal de transmisión en un segundo. Para determinar la cantidad de información que se requeriría para transmitir por la red es necesario considerar parámetros aproximados de acuerdo al siguiente detalle:

Tabla 6. Detalle de requerimiento de ancho de banda para la LAN

TIPO SERVICIO	CANTIDAD	TAMAÑO MÍNIMO	TAMAÑO MÁXIMO	FORMULA	CALCULO
MAIL	80 USUARIOS	5KB	8MB	$AB=G \times C$	$AB=80 \times 0.134Mbps=10,72 \approx AB=11Mbps$ $AB=10Mbps$
SISTEMA DOCUMENTAL	80 USUARIOS	5KB	8MB	$AB=G \times C$	$AB=80 \times 0.034Mbps=2,72 \approx AB=3Mbps$ $AB=3Mbps$
CIRCUITO DE VIDEO-VIGILANCIA CAMARAS -IP	# DE CAMARAS=16	24Kbps	2Mbps	$AB= \text{Tamaño de la Imagen} \times \text{Promedio del tamaño de cada imagen} \times \% \text{ de actividad} \times 8$	Para el día $AB=30fps \times 24KB \times 71,67\% \times 8 = 30 \times 24 \times 0,7167 \times 8 = 4128,192Kbps$ $4Mbps \times 16 = 64Mbps$ Para la noche $AB=30fps \times 2MB \times 5,43\% \times 8 = 30 \times 2 \times 0,0543 \times 8 = 25,44Mbps$ $25,44Mbps \times 16=407Mbps$
TELEFONIA IP	# LINEAS= 20		22300 bps/llamada	$AB = AB/llamada \times \text{llamadas concuerrentes}$	$AB = 22,300 kbps/llamada \times 20 = 446Kbps$
INTERNET (up)	80 usuarios		40 usuarios	$AB=n \times Pap \times \emptyset(n)$	$AB=40(\text{usuarios} \times \text{seg.}) \times 8MB \times 50\% = 160Mbps$
INTERNET (down)	5500 usuarios		4 usuarios x segundo	$AB=n \times Pap \times \emptyset(n)$	$AB=4(\text{usuarios} \times \text{seg.}) \times 30MB \times 100\% = 120Mbps$

Nota:* Lo normal para video en tiempo real en CCTV es de 25-30fps - Frames Por Segundo (Securamente,s.f.)

En los cálculos expuestos en el cuadro que antecede se ha considerado los valores máximos estimados con la finalidad de tener un margen de error mínimo.

De igual manera se espera recibir alrededor de 5.500 usuarios externos en días de alta transaccionalidad los cuales deben conectarse al sistema misional a

través de la página web. El tamaño de archivos que se deben cargar a través de la página web tienen como tamaño mínimo 25k y como tamaño máximo 30MB. Para calcular el ancho de banda se cree conveniente utilizar la siguiente fórmula:

$$AB=n \times Pap \times \emptyset(n)$$

Donde n es el número de usuario, Pap es el peso de la aplicación/tamaño estimado del paquete de datos y $\emptyset(n)$ es la tasa de ocupación que representa la cantidad de usuarios que estarían usando la aplicación de forma simultánea, reemplazando datos quedaría:

$$n=5500$$

$$Pap=30MB$$

$$\emptyset(n)=100\% \text{ (porcentaje estimado de usuarios concurrentes)}$$

Los 5500 usuarios no se conectarán en el mismo instante pero si lo harán durante todo el día, lo cual implicaría considerar el número total de usuarios dividido para las 24 horas que tiene el día, quedando de la siguiente manera:

$$n= 5500 \text{ (usuarios)}/24(\text{horas día})\times(60\text{seg}) = 4 \text{ usuarios x seg}$$

$$AB = 4(\text{usuarios x seg.}) \times 30MB \times 50\% = 60Mbps$$

El resultado es aproximadamente 60Mbps

Para los usuarios internos se estima que se conecten hacia la red de Internet 40 usuarios concurrentes. Es importante tomar en cuenta también el número total de usuarios que son 80. Un cálculo más exacto del requerimiento de ancho de banda se espera utilizar la siguiente fórmula:

$$AB=n \times Pap \times \emptyset(n)$$

$$\text{Donde } n= 40$$

$$Pap=8MB$$

$$\emptyset(n)=50\%$$

$$AB = 40(\text{usuarios} \times \text{seg.}) \times 8\text{MB} \times 50\% = 160\text{Mbps}$$

Este resultado corresponde aprox., a 160Mbps

Adicional se debe considerar también que la Institución tiene previsto ofrecer el servicio de capacitación online para usuarios externos, lo cual generará un tráfico de datos aproximado de 5GB. Por el tamaño del archivo se prevé asignar un ancho de banda de 3MB exclusivo para este servicio.

2.3.5. Cableado Estructurado

El sistema de cableado estructurado debe permitir alta tasas de transferencias de datos, puesto que deberán permitir que los servicios de voz, datos y video cumplan el objetivo adecuadamente, además deberán proporcionar el medio para que los uploads de archivos de todos los sujetos obligados a reportar puedan llegar a su destino. Por lo que deberán cumplir con las siguientes especificaciones técnicas mínimas:

- 1) Sistema de cableado estructurado categoría 6A
- 2) Estándares a ser cumplidos EIA/TIA 568, 569, 606, 607.
- 3) El cuarto de equipos debe estar bien ventilado y ambientalmente controlados 24 horas al día, siete días por semana. Se debe mantener una razón de disipación de calor de 225 BTU por pie cuadrado y mantener una temperatura entre 18 y 24 grados centígrados con una humedad relativa entre 30 y 55 por ciento.
- 4) En el cableado horizontal:
- 5) La distancia cross-connect (panel de parcheo) al toma de telecomunicaciones no excederá 90 metros.
- 6) Ningún segmento tendrá más de dos curvas entre cajas de paso. Estas cajas de paso de colocarse cada 30 m.
- 7) Las canalizaciones horizontales se seleccionarán de forma que el radio de curvatura mínimo sea de 50 mm.

- 8) Evitar colocar los cables sobre el techo falso, se puede utilizar conduits o bandeja portacable tipo escalera, sin sobrepasar el 40 % de llenado.

A continuación se muestra un detalle de los puntos requeridos por Área:

Tabla 7. Estimado de puntos de cableado estructurado requerido

UNIDAD DE ANALISIS FINANCIERO		
CABLEADO ESTRUCTURADO		
Área	Puntos de Red	Distribución
Dirección General	40	Dirección General
Secretaría General	6	Secretaría General
Prevención	12	Prevención
Recepción – Call Center	11	Recepción – Call Center
Tecnología	23	Tecnología
Administrativa Financiera	14	Administrativa Financiera
Recursos Humanos	6	Recursos Humanos
Análisis	27	Análisis
Jurídico	9	Jurídico
Relaciones Internacionales	7	Comunicación
Guayaquil	10	Guayaquil
Cuenca	10	Cuenca
Centro de Datos	73	Centro de Datos
Sala de Capacitación	40	Sala de Capacitación
TOTAL:	288	

Tomado de: Archivo de la Dirección de Gestión Tecnológica UAF

2.3.6. Sistema de Energía Eléctrica Regulada

La Unidad de Análisis Financiero por su naturaleza requiere mantener activos todos los servicios y aplicaciones, por lo que la energía eléctrica requiere que

las redes de energía eléctrica incorporen sistemas de protección indispensables para que garanticen el funcionamiento de energía regulada en la red.

Los sistemas de respaldos de energía eléctrica UPS (Uninterruptible Power Supply) debe permitir la administración a través del protocolo SNMP (Simple Network Management Protocol).

A continuación se muestra un detalle de los puntos de energía eléctrica regulada y puntos de energía normal que se requiere:

Tabla 8. Distribución de puntos normales y regulados

UNIDAD DE ANÁLISIS FINANCIERO		
DISTRIBUCIÓN DE PUNTOS DE ENERGÍA ELÉCTRICA		
AREA	Puntos Energía eléctrica normal	Puntos Energía eléctrica regulada
Dirección General	4	40
Secretaría General	2	9
Prevención	3	12
Recepción - CC	4	12
Tecnología	4	23
Administrativa Financiera	3	14
Recursos Humanos	3	6
Análisis	5	27
Jurídico	4	10
Comunicación	3	7
Guayaquil	8	15
Cuenca	6	15
Sala de Capacitación	4	40
TOTAL:	30	230

Los puntos de energía regulada para el Centro de Datos estarán dispuestos de acuerdo al requerimiento y cantidad de armarios.

Cabe mencionar que para cubrir la carga eléctrica regulada requerida tanto para las PC's así como para el Centro de Datos, es conveniente utilizar los dos equipos UPS de 15kva con los que inicialmente cuenta la Institución, así como también con los que se indica en el requerimiento del diseño de la solución.

Es preciso indicar que una vez que la Unidad de Análisis Financiero cuente con instalaciones en el nuevo edificio tomará este análisis como punto de partida para realizar futuras ampliaciones, en las cuales demande infraestructura de cableado estructurado.

3. Capítulo III. Diseño de la Solución

La Unidad de Análisis Financiero se encuentra en un momento de crecimiento tecnológico en vista que la Ley de Prevención Detección y Erradicación de Lavado de Activos y Financiamiento de Delitos aprobó la incorporación de diversos sectores económicos como sujetos obligados a reportar, lo que significa un incremento de reportes online que la Institución recibirá a través del sistema web, incrementándose el número de concurrencias al segundo e incrementándose significativamente la cantidad de información.

Se ha definido para este diseño conceptos de alta disponibilidad, interoperabilidad, escalabilidad, movilidad, convergencia, y seguridad como componentes que requieren sean ejecutadas tanto en el equipamiento y tecnología empleados, como también en los procesos y lineamientos con los que se ejecutan e implementan.

En virtud de lo expresado y en función a lo establecido en el ítem 2.3 Definición de Requerimientos del capítulo anterior se detalla a continuación los requerimientos técnicos mínimos para el diseño de la solución tanto para la red LAN como para la red WAN.

Tabla 9. Solución Propuesta para la Red de Datos de la UAF

Requerimientos de la solución propuesta para la Red de Datos de la Unidad de Análisis Financiero	
Cableado estructurado	
Categoría:	6a
Certificación	Panduit
Conector	RJ45
Tipo de cable	F/UTP(Par trenzado blindado)
Vel. Máx.	10 Gbps
Puntos de red	290 puntos de red

Estándares de instalación	EIA/TIA 568, 569, 606, 607
Centro de Datos	
Área de Construcción	El área de construcción debe ser mínimo de 25m ² ., y debe ser una construcción diseñada exclusivamente para ese fin, ser sismo resistente.
Centro de Datos	Debe contar con un área para almacenamiento de equipos y medios libre de circulación de tuberías de gas natural o propano.
Puerta del Centro de Datos	La puerta blindada de seguridad debe ser construida en material antinflamable y vidrios templados para evitar su caída en caso de rompimiento por movimiento sísmico o explosión ya sea por incendio o atentado.
Piso falso	El piso falso del Centro de Datos deberá estar instalado sobre gatos y cumplir con las características de ser antiestático, aislante, no inflamable y no combustible; bajo él deberá alojarse la escalerilla que permitirá el paso de cableado estructurado
Sistema de Control de Acceso	Sistema de control de acceso por medio de biométrico con huella para el acceso al centro de datos.
Cuarto de UPS's	Cuarto para UPS's con sistema de ventilación redundante. Piso de vinil antiestático Puerta de seguridad Control de accesos Iluminación de la sala de equipos
Sistema de enfriamiento	El cuarto de Centro de Datos deberá tener como mínimo dos equipos de aire acondicionado de configurados 49000 BTU's en un esquema activo-pasivo
Detección y extinción de incendios	Deberá tener un sistema automático de detección y extinción de incendios con gas ecológico.

Estándares	TIA 942
Equipos de protección eléctrica	
UPS	(high availability) (2)UPS de 15 KVA trifásico con un tiempo de respaldo de alrededor de 10 minutos
Equipos de red	
Switch de core	(high availability) (2) Switch de core con puertos de fibra SFP+10G, 48 puertos
Switch de acceso	(high availability) (10) Switch de acceso de 48 puertos
Equipos servidores	
Servidores	(4) Blades Intel 2 procesadores de 8c, 128 GB
Servidores base de datos	(high availability) (2) Rackeables RISC 32 cores, procesador 64 bits, 256GB RAM, 1066Mhz,
Sistema de almacenamiento	(high availability) (2) Almacenamientos 7Gb Raid 1 para BDD y 6Gb Raid 5 para Aplicaciones. Configuración StandBy
Aplicaciones	
Misional	Ambiente Producción: high availability cluster Sistema de carga de reportes en línea: JAVA 2EE Servidor a Aplicaciones JBOSS v5.0 Ambiente Desarrollo: Sistema de carga de reportes en línea: JAVA 2EE Servidor a Aplicaciones JBOSS v5.0 Ambiente Pre-Producción Sistema de carga de reportes en línea: JAVA 2EE Servidor a Aplicaciones JBOSS v5.0

Contabilidad	<p>Ambiente de Producción: high availability cluster</p> <p>Syral: Oracle 10g</p> <p>Ambiente Desarrollo</p> <p>Syral: Oracle 10g</p> <p>Ambiente Pre-Producción</p> <p>Syral: Oracle 10g</p>
Documentación	<p>Ambiente Producción high availability cluster</p> <p>SISDOC : Lotus Domino v.8</p> <p>Ambiente Desarrollo</p> <p>SISDOC : Lotus Domino v.8</p> <p>Ambiente Pre-Producción</p> <p>SISDOC : Lotus Domino v.8</p>
Correo	<p>Ambiente Producción high availability cluster</p> <p>Sendmail 8.13.8</p> <p>Ambiente Desarrollo</p> <p>Sendmail 8.13.8</p> <p>Ambiente Pre-Producción</p> <p>Sendmail 8.13.8</p>
Página Web	<p>Ambiente Producción high availability cluster</p> <p>Apache/2.2.3 - PHP 5.1.6 - Mysql v.5.0.22 - Liferay v.</p> <p>Ambiente Desarrollo</p> <p>Apache/2.2.3 - PHP 5.1.6 - Mysql v.5.0.22 - Liferay.</p> <p>Ambiente Pre-Producción</p> <p>Apache/2.2.3 - PHP 5.1.6 - Mysql v.5.0.22 - Liferay v.</p>

Servicios de Red	<p>Ambiente Producción high availability cluster</p> <p>Domain Name Server - DNS</p> <p>Samba</p> <p>Lightweight Directory Access Protocol - LDAP</p> <p>Network Time Protocol – NTP</p> <p>Ambiente Desarrollo</p> <p>Domain Name Server - DNS</p> <p>Samba</p> <p>Lightweight Directory Access Protocol - LDAP</p> <p>Network Time Protocol – NTP</p> <p>Ambiente Pre-Producción</p> <p>Domain Name Server - DNS</p> <p>Samba</p> <p>Lightweight Directory Access Protocol - LDAP</p> <p>Network Time Protocol – NTP</p>
S.O.	Linux RedHat Enterprise v.5.5
Equipos de oficina	
Impresoras, copiadoras, escáners,	Se sugiere se centralice el servicio de equipos de oficina con la finalidad de mejorar la administración y disminuir los costos de suministros
Equipos de telecomunicaciones	
	Se utilizará enlaces dedicados contratados con un proveedor, por lo que no se requiere equipos de telecomunicaciones

3.1. Red LAN del Centro de Datos

3.1.1. Criterios de diseño

Es necesario que el diseño de la red LAN del centro de datos tenga en cuenta los siguientes requerimientos:

- Debe tener la propiedad de aumentar la capacidad de trabajo sin comprometer su funcionamiento; es decir debe ser escalable.
- Incorporación de equipamiento con criterio de alta disponibilidad.
- Sistema de seguridad en la red LAN.
- Red de datos convergente que soporte voz, datos y video.

El diseño propone considerar el concepto de arquitectura de CISCO.

La capa de borde o acceso estará distribuido en los cinco pisos del edificio al 100% de redundancia; igualmente la capa de core tendrá una redundancia al 100% en el centro de datos.

El concepto balanceo de carga se toma en cuenta con el objetivo de dividir las tareas que tendría que soportar un solo equipo, con el fin de maximizar las capacidades de proceso de datos así como de ejecución de tareas. De esta manera ningún equipo será parte vital del servicio que se desea ofrecer, evitando así una parada del servicio debido a un evento inesperado de uno de los equipos. Se incorpora este concepto para balancear carga entre los servidores Web.

3.1.2. Protocolos de red

Se plantea que los protocolos de red que se utilizarán en esta solución propuesta son:

Tabla 10. Protocolos de red

Protocolos	Descripción
802.1ad QinQ y QinQ selectivo	Este protocolo permitirá aumentará la escalabilidad en la red, este protocolo

	permitirá conectividad con la red de Guayaquil y Cuenca.
Rapid SpanningTreeProtocol (RSTP)	Este protocolo gestionará enlaces redundantes en la capa de enlace de datos.
Protocolo IEEE 802.1Q	Este protocolo dará la posibilidad de comunicación de manera transparente entre VLAN's
QoS (Quality of Service)	Este protocolo garantizará la transmisión de la información, además de dar calidad en el servicio.

3.1.3. Arquitectura de red

Para el diseño de la arquitectura de red, es necesario considerar los distintos niveles de seguridad perimetral, lo cual permitirá definir niveles de confianza, admitiendo el acceso a determinados usuarios internos o externos a ciertos servicios y denegando otro tipo de acceso a otros. En tal razón se ha previsto los siguientes niveles:

Zona desmilitarizada (DMZ demilitarized zone) o también conocida como red perimetral, que es la red que estará ubicada entre la red interna y la red externa que generalmente es Internet.

Zona militarizada: Es un área protegida donde se encuentran los componentes que requieren un nivel de seguridad, es decir que no tiene acceso desde la red externa o Internet.

Por motivos de seguridad la red LAN contendrá un segmento exclusivo para los equipos de base de datos y sistema de almacenamiento SAN (Storage Area Network), esto garantizará que solamente ciertos equipos se conecten al almacenamiento.

Con la finalidad de garantizar la seguridad a este nivel se implementará la técnica de firewall de filtrado de paquetes a través de listas de acceso (ACL) en los enrutadores. Adicional a esto se utilizará un firewall tipo proxy para el servicio http.

El direccionamiento que se utilizará en el centro de datos es el siguiente:

Tabla 11. Direccionamiento de red del Centro de Datos

SUBRED	DIRECCIONAMIENTO
Servidores WEB	Dirección IP: 192.168.2.0 Mascara: 255.255.255.0
Servidores de Aplicaciones	Dirección IP: 192.168.3.0 Mascara: 255.255.255.0
Servidores de Bases de Datos	Dirección IP: 192.168.4.0 Mascara: 255.255.255.0

3.2. Red LAN de las Oficinas Remotas

3.2.1. Criterios de diseño

Es indispensable que se considere los siguientes requerimientos:

- Diseño escalable, sin que su crecimiento interfiera en la operación de la infraestructura
- Diseño con incorporación de equipamiento con criterio de alta disponibilidad
- Diseño del sistema de seguridad en la red LAN
- Diseño de una red de datos convergente que soporte voz, datos y video

Es imprescindible que se considere seguridades en las redes LAN remotas, de manera que se pueda acceder a ellas de acuerdo a lo que estipule las políticas de seguridad de la Institución, además el tráfico broadcast debe ser controlado porque afecta directamente en el rendimiento de la red.

Estos elementos indicados pueden ser manejados a través de la configuración de VLANS. La implementación de VLANS deben ser realizados por departamentos de forma que se contribuye a fortalecer la seguridad de la red.

3.2.2. Protocolos de red

Los protocolos de red que se estima utilizar para el diseño de la red WAN son los mismos que los utilizados para el diseño de la red LAN.

Se plantea que los protocolos de red que se utilizarán en esta solución propuesta son:

Tabla 12. Protocolos de red

Protocolos	Descripción
802.1ad QinQ y QinQ selectivo	Este protocolo permitirá aumentará la escalabilidad en la red, este protocolo permitirá conectividad con la red de Guayaquil y Cuenca.
Rapid Spanning Tree Protocol (RSTP)	Este protocolo gestionará enlaces redundantes en la capa de enlace de datos.
Protocolo IEEE 802.1Q	Este protocolo dará la posibilidad de comunicación de manera transparente entre VLAN's
QoS (Quality of Service)	Este protocolo garantizará la transmisión de la información, además de dar calidad en el servicio.

3.2.3. Cableado estructurado

De acuerdo a la tendencia tecnológica actual el sistema de cableado estructurado que se implemente en la oficina de Guayaquil y Cuenca debe permitir un nivel alto de flujo de información, por lo que es necesario

implementar el sistema de cableado con categoría 6A, la cual es la que se ha implementado en las oficinas de la UAF en la ciudad de Quito u oficina principal. Además es importante que cumpla con los estándares requeridos para la correspondiente certificación:

EIA/TIA:

569 Diseño y Administración de la Red

568 Control de calidad de la instalación

606 Administración

TSB-67 Pruebas de Cableado Estructurado

607 Tierras y aterramientos para sistemas de telecomunicaciones

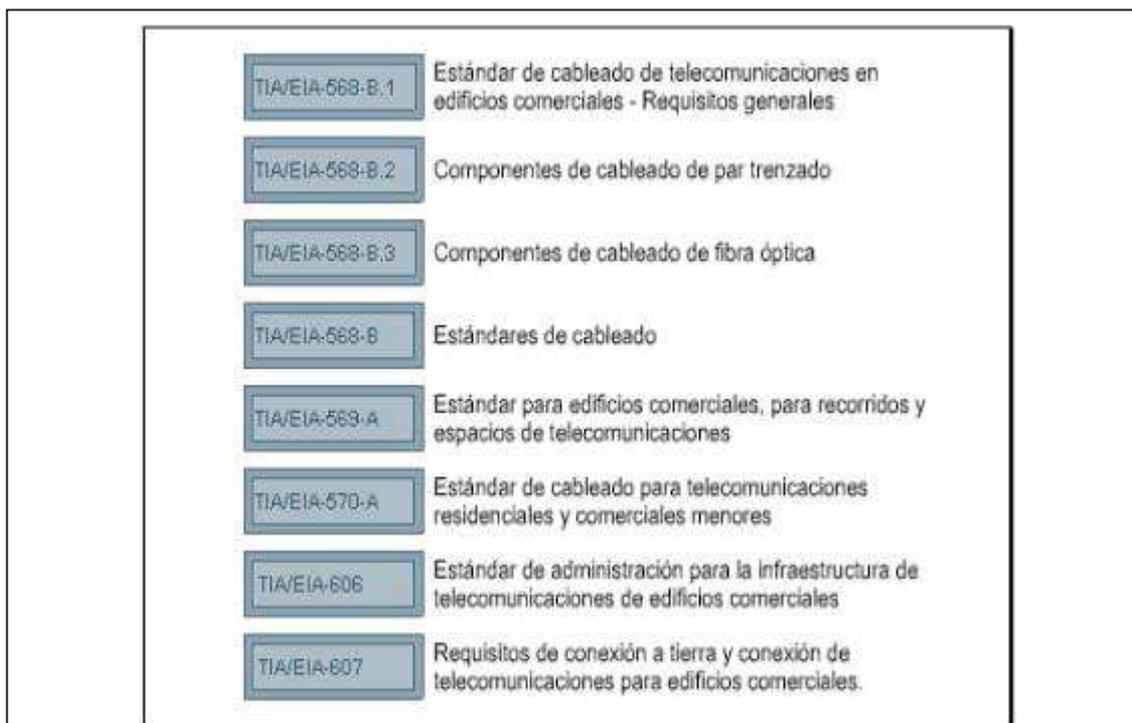


Figura 3. Estándares TIA/EIA para cableado estructurado

Tomado de: CCNA 1 Suplemento sobre cableado estructurado –V3.1

Con el afán de cumplir con el objetivo de tener redes convergentes el sistema de cableado estructurado debe tener un solo punto en cada una de las áreas de trabajo, a través del cual fluirá tráfico de voz, datos y video.

3.2.4. Arquitectura de red

Considerando que el nuevo espacio de trabajo de la Unidad de Análisis Financiero estará distribuido en varios pisos se plantea la opción de diseño con una implementación de un backbone de datos. El backbone se implementará con fibra óptica multimodo de 6 hilos; dos pares de hilos se encontrarán operativos y los otros restantes estarán de respaldo en caso de averías y/o daños en uno de los enlaces principales.

Cada piso tendrá dos switch de acceso redundante, y el número de puertos configurados se encontrará de acuerdo a los requerimientos definidos.

El switch de core estará integrado por los switch de acceso de cada piso a través de canales de fibra óptica, cuyos puertos en los switch deben tener configuración de agregación de enlace (802.1ad). Con la finalidad de aumentar la capacidad del canal que enlazará los switch de acceso con el switch de core se utilizará balanceo de carga y alta disponibilidad.

La capa de core o núcleo deberá estar implementada con dos switches con la finalidad de minimizar los puntos de error y mantener operativa la red.

En el siguiente detalle se muestra la estructura de VLAN's como debe estar configurados los switch:

Tabla 13. Asignación de ID de las diferentes VLANS

# VLAN	NOMBRE VLAN	DESCRIPCION
1	VLAN-DAO	Análisis
2	VLAN-DGT	Tecnología
3	VLAN-FIN	Financiero
4	VLAN-PRE	Prevención

5	VLAN-SER	Servidores
6	VLAN-MON	Monitoreo
7	VLAN-APP	Aplicaciones
8	VLAN-WEB	Servidores WEB
9	VLAN-GEN	Dirección General
10	VLAN-BDD	Base de Datos
11	VLAN-VID	Cámaras de video

La estructura de red que se define en la oficina principal de la UAF será la misma con la que se trabajará en cada subred de cada LAN adicional. Es necesario contar con una VLAN para se pueda realizar la administración respectiva.

En el momento de configurar los protocolos de calidad de servicio, priorización y clasificación de paquetes en los switch de acceso así como también en los switch de core el tráfico de voz toma mucha importancia.

3.3. Diseño de la Red WAN

WAN (Wide Area Network) es una red de área geográfica amplia que permite una transmisión a larga distancia de datos, voz, imágenes, videos con un acceso rápido y eficaz. Es la unión de dos o más redes LAN.

3.3.1. Criterios de diseño

Con la finalidad de considerar los criterios de diseño de la red WAN es importante la incorporación de calidad de servicio para que la infraestructura soporte voz datos y video. Sin dejar de lado los conceptos de alta disponibilidad, interoperabilidad y convergencia.

3.3.2. Planteamiento de la solución

La solución debe considerar la implementación de calidad de servicio fin a fin, para lo cual es necesario que tanto los equipos de red WAN como los de la

infraestructura de servicios de telecomunicaciones soporten estos protocolos. Lo cual permitirá manejar distinto tipo de tráfico entre la sucursal de Guayaquil, la sucursal de Cuenca y la oficina principal de la ciudad de Quito.

Dentro de los criterios de diseño de los enlaces de telecomunicaciones, se prevé utilizar MPLS (Multiprotocol Label Switching) con la finalidad de garantizar calidad de servicio y escalabilidad por su característica de agregación ya sea en las capacidades del canal y en el empleo de distinto tipo de tráfico.

Con la finalidad de garantizar la seguridad y mantener disponibilidad y rendimiento al máximo en la red WAN de la Unidad de Análisis Financiero, deberá utilizar un enlace dedicado por medio físico.

3.3.3. Topología de red

Se requiere que la implementación cuente con una solución de alta disponibilidad, por lo que se plantea una arquitectura de red redundante con switchs de core y switchs de acceso redundantes en cada piso, conexión de fibra redundantes.

Adicional se plantea un enlace dedicado para una oficina sucursal en la ciudad de Guayaquil, y una oficina en la ciudad de Cuenca así:

Tabla 14. Distribución de los enlaces de Telecomunicaciones

NODO	SITIOS REMOTOS
Nodo Quito	Matriz
Nodo Guayaquil	Sucursal Guayaquil
Nodo Cuenca	Sucursal Cuenca

Es necesario anotar que el nodo de la ciudad de Guayaquil estará ubicado en el centro de datos correspondiente de la sucursal, así como también el nodo de

la ciudad de Cuenca en su centro de Datos respectivo, en tanto que el de Quito se encontrará en las instalaciones del edificio principal.

3.3.4. Capacidad de canales de telecomunicaciones

Para determinar el ancho de banda para el enlace de comunicaciones entre la oficina principal y las sucursales WAN, se cree conveniente considerar el número de usuarios que se encontrarán inicialmente en las oficinas remotas y por lo tanto los servicios informáticos que la oficina principal va a ofrecer. Tomando en cuenta el análisis de ancho de banda del ítem 2.3.4 Equipamiento de Red LAN y WAN capítulo 2, se estima un ancho de banda para el enlace de comunicaciones de 5MB.

En cuanto al tipo del canal este es un dato que se sujeta al Proveedor del servicio dependiendo de la tecnología y disponibilidad del mismo, en este caso se sugiere MPLS con la finalidad de aprovechar sus características de priorización de tráfico, las aplicaciones de voz y datos y la flexibilidad de las comunicaciones punto a punto.

Tabla 15. Definición de capacidad de canal para la red WAN

ORIGEN	DESTINO	CAPACIDAD DE CANAL	TIPO DE CANAL
ENLACES			
QUITO	MATRIZ	60 Mbps	MPLS
GUAYAQUIL	SUCURSAL	5 Mbps	MPLS
CUENCA	SUCURSAL	5 Mbps	MPLS

El cálculo de los enlaces de telecomunicaciones se realizó en base a la cantidad de usuarios que se conectarían con los diferentes servicios informáticos que ofrece la matriz. Es decir, se estima que alrededor de 10 usuarios de cada sucursal accedan a los servicios que provee la oficina principal de la ciudad de Quito; para lo cual se considera los mismos servicios informáticos previstos en el ítem 2.3.4 Equipamiento de Red LAN y WAN

capítulo 2; además, se evalúa que podría existir un tráfico de archivos de reportes con un tamaño entre 25KB y 30MB.

En virtud de lo expresado:

$$AB = G \times C$$

G = Tamaño del archivo a enviarse dividido para el tiempo estimado de carga

C= Número de usuarios concurrentes

Tamaño archivo máximo = 30MB

Tiempo estimado= 1 minuto

C=10 (para cada enlace)

G=30MB / (1 x 60seg)

G=0,5Mbps

C=80

AB=10 x 0.5Mbps= 5 ≈ AB= 5Mbps

Las especificaciones técnicas del equipamiento de red se encuentran en el anexo.

3.4. Diseño de Seguridad Perimetral

3.4.1. Criterios de diseño

Para el diseño de la seguridad perimetral de la red LAN de la Institución se plantea que se debe considerar la tendencia tecnológica actual enfrentándose diariamente a los múltiples riesgos de posibles intromisiones desde y hacia el Internet.

3.4.2. Técnicas a utilizar

Para el diseño de seguridad perimetral, es importante considerar algunos aspectos tales como:

Red de borde en el que constarán el o los equipos enrutadores provistos por el proveedor del servicio de Internet (ISP). Este será el primer filtro de red básico.

Red perimetral en el que se considerarán los equipos web que se encuentran expuestos a la red de Internet, a esta zona comúnmente se le conoce como zona desmilitarizada (DMZ). La seguridad para la DMZ estará provista por el firewall de seguridad el cual permite los criterios de acceso desde esta zona hacia la red interna.

En la DMZ es prioritario estimar criterios de seguridad los mismos que deben estar establecidos en un documento de políticas de seguridad de la red de datos tales como: qué tipo de conexiones se debe rechazar por poner en riesgo a servicios críticos; qué tipo de tráfico se debe permitir; mecanismos que se debe considerar para proteger servicios vulnerables y/o críticos; de igual manera la forma de ocultar información de red de carácter relevante que bien puede ser topología de red, nombres de cuentas de usuario, nombres y tipos de equipos, etc. entre otros.

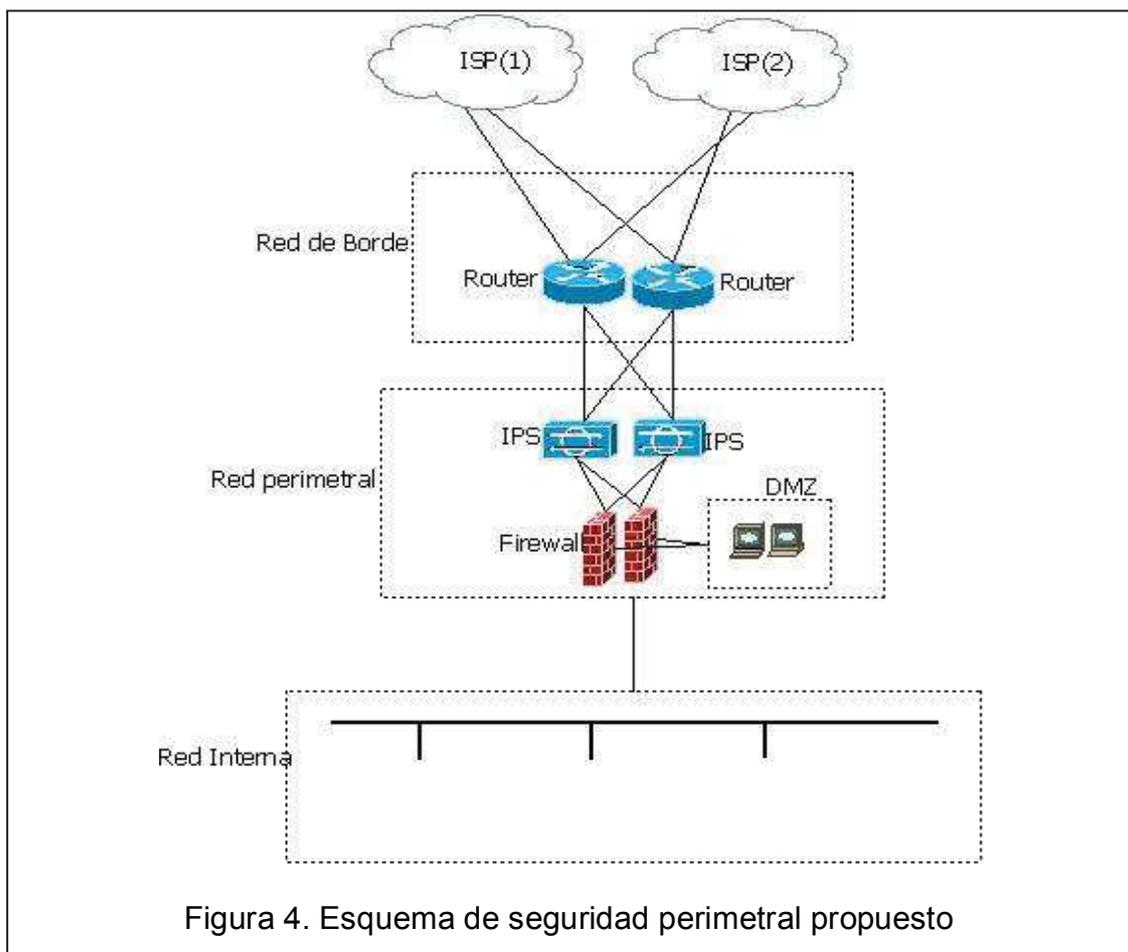
Red interna es la red que permite unir a los equipos servidores con sus distintos servicios informáticos y el resto de la red interna propiamente dicha.

El perímetro de la red involucra a los ruteadores, los equipos firewalls, los IPS, y la zona desmilitarizada.

La Institución tiene previsto actualizar la infraestructura tecnológica con equipos servidores tipo blade y ofrecer ambientes al 100% virtualizados y por ende ofrecer alta disponibilidad, por lo que se vuelve indispensable prever esta situación considerando que la Institución debe manejar altos estándares de seguridad porque el tipo de información que manipula es de carácter reservado y confidencial.

Es así que con la finalidad de garantizar que la información que atraviesa por la red disponga de un nivel de seguridad alto, además que sea válida y autorizada, se plantea la utilización de equipos IPS (Intrusion Prevention System) en la zona perimetral desmilitarizada, con la finalidad de mantener a salvo a la red interna de cualquier eventualidad. El equipo debe ser redundante; es decir, proporcionar una alta disponibilidad en este segmento.

En la siguiente figura podemos tener un esquema de seguridad propuesto:



Las características del equipo instalado debe permitir mecanismos de manejo de paquetes de forma que asegure la integridad del mismo al viajar por la red; además debe permitir el filtrado de contenido validando la información que cada paquete lleve consigo. También debe tener la capacidad de limitar el ancho de banda, de manera que se garantice la disponibilidad de los recursos de la red para el tráfico que tenga una mayor prioridad.

Además para la zona semi-militarizada es necesario realizar un cambio del appliance de seguridad (firewall) actual por uno más robusto que permita un mejor performance, además que incluya una administración gráfica idónea para que el administrador de la red cuente con las interfaces gráficas necesarias de reportes de la transaccionalidad de la red.

Se debe poner énfasis en el hecho que hay un notable aumento en la transaccionalidad en la red tanto por el incremento de usuarios internos así como también por el crecimiento de usuarios externos. Se plantea que todos los equipos tengan redundancia, con la finalidad de ofrecer alta disponibilidad en el firewall.

3.4.3. Topología de red

En la figura 5 se observa el esquema de la red LAN propuesto.

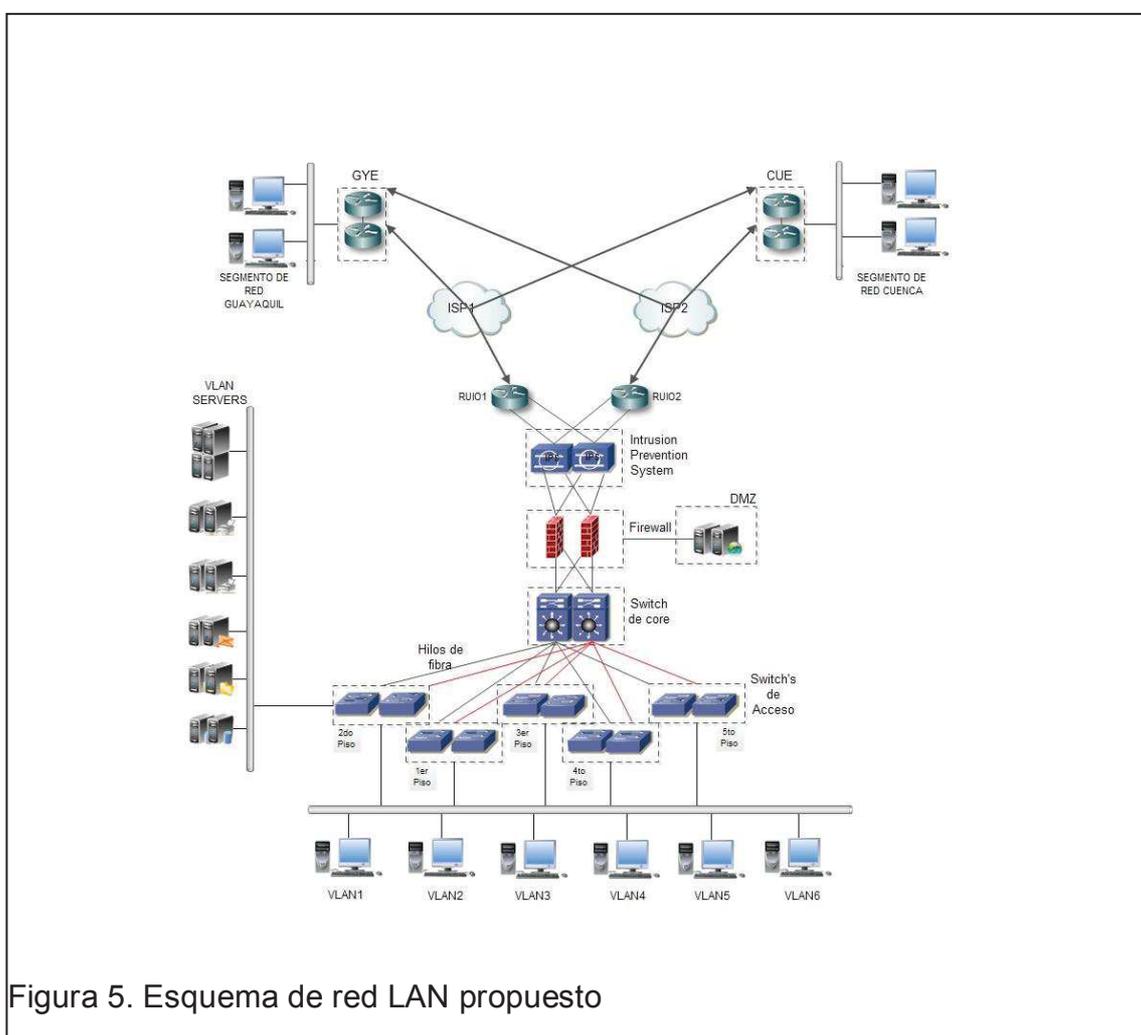


Figura 5. Esquema de red LAN propuesto

4. Capítulo IV. Esquema de Servicios De Red

Dentro de la implementación de los servicios de red, se deberá considerar los servicios de DNS (Domain Name Server), DHCP (*Dynamic Host Configuration Protocol*), los mismos que deberán ser configurados en un equipo que cuente como sistema operativo base LINUX.

El DNS (Domain Name Service) es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y vice-versa, el mismo que se configurará ejecutando named. Este servicio estará configurado en el servidor principal, el mismo que deberá ser replicado en cada uno de los nodos tanto de Guayaquil como de Cuenca (respectivamente).

EL servicio DHCP que significa Protocolo de configuración de host dinámico, permite que un host que se encuentra conectado a una red pueda obtener su configuración de red de manera dinámica. Para lo cual se utilizará un equipo con sistema operativo LINUX y se configurará el demonio dhcp, en la configuración se determinará los rangos de direcciones de red de cada segmento, para la asignación automática de direcciones IP a cada equipo de cada área.

4.1. Zona Web

El sistema misional Institucional es de gran relevancia para el cumplimiento de las funciones de la Unidad de Análisis Financiero, por lo que resulta de gran importancia mantener altos estándares de servicio, debido a que es un sistema vía web que proporciona el medio de acceso de los reportes de todos los sectores económicos del país hacia la Institución.

El servicio web apache + php estará implementado en servidores blades sobre un ambiente virtual lo cual permitirá disponer de mínimo dos equipos virtuales en un esquema de alta disponibilidad. La base de datos para este servicio: mysql estará implementado en otros equipos virtuales dentro de otra Vlan, lo que garantizará la seguridad de la información publicada en caso de un posible hackeo a la página web.

Adicionalmente se dispondrá de dos equipos balanceadores de carga con la finalidad de balancear las peticiones cuando el nivel de concurrencia en el sistema web sea alto, cubriendo de esta manera con la disponibilidad del servicio web en cualquier momento.

Se garantizará la veracidad y la seguridad de la página web con certificado SSL con una encriptación de 256 bits y una longitud de clave de 2048 bits. En la figura 6 se puede esquematizar la zona web en alta disponibilidad.

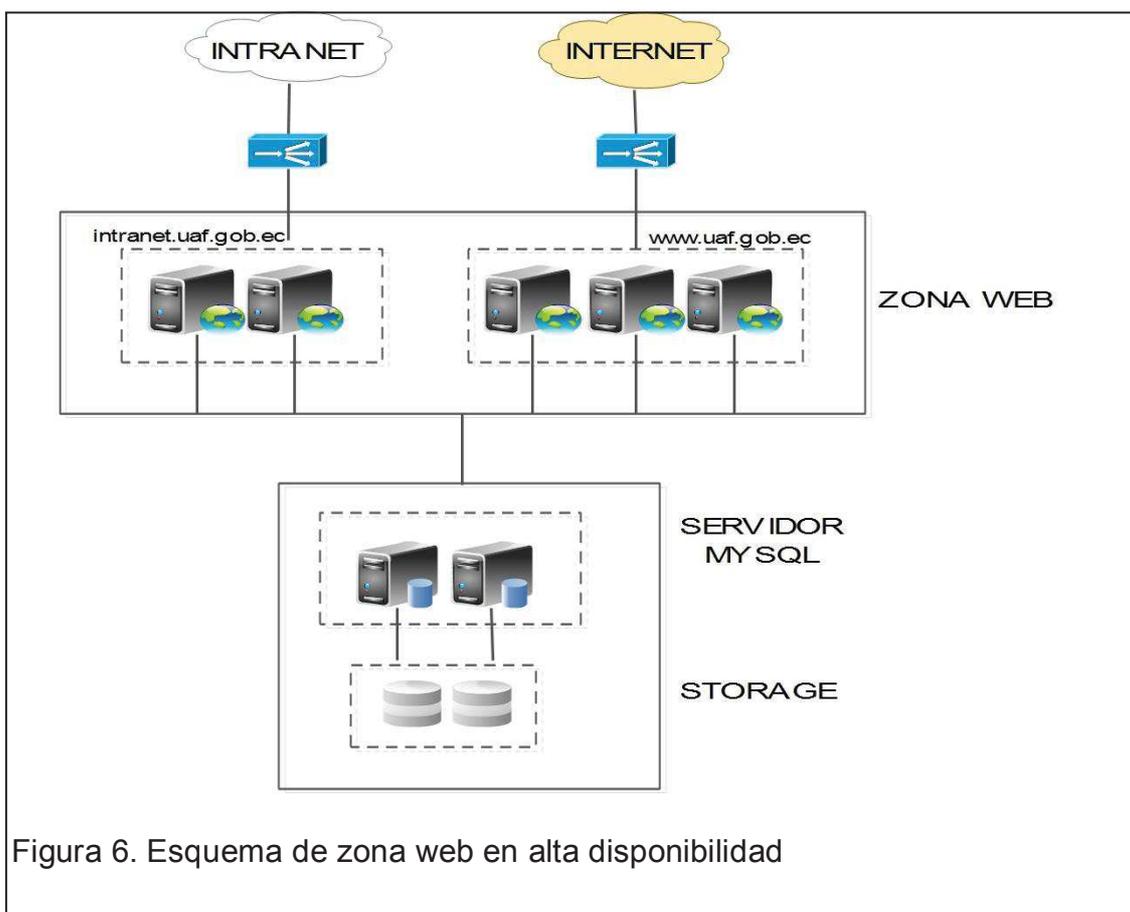


Figura 6. Esquema de zona web en alta disponibilidad

4.2. Zona de Aplicaciones

En esta capa estarán los servidores que contendrán las reglas del negocio de la aplicación de reportes de la Unidad de Análisis Financiero que proporcionará servicio a los sujetos obligados a reportar. Esta capa es de vital importancia razón por lo que se ha previsto mantener un esquema de alta disponibilidad configurado a través de máquinas virtuales sobre equipos blades.

Al igual que a la página web, el sistema de reportes garantizará su veracidad y seguridad con un certificado SSL con una encriptación de 256 bits y una longitud de clave de 2048 bits; y, el acceso al sistema tendrá una autenticación de doble vía a través de un token de seguridad, conocido también como token de autenticación o token criptográfico el cual permite al usuario acceder al servicio, y autenticación de usuario.

Los equipos servidores que contengan las aplicaciones de negocio, deberán estar en un ambiente virtual en un esquema de alta disponibilidad de manera que se garantice el servicio, para lo cual se sugiere la adquisición de un software de virtualización que permita reiniciar las aplicaciones automáticamente en cuestión de minutos tanto en el caso de que ocurra alguna falla a nivel de equipo o de sistema operativo, como también que sea tolerante a fallos sin que se interrumpa el servicio, etc. En la figura 7 se puede esquematizar la zona web en alta disponibilidad

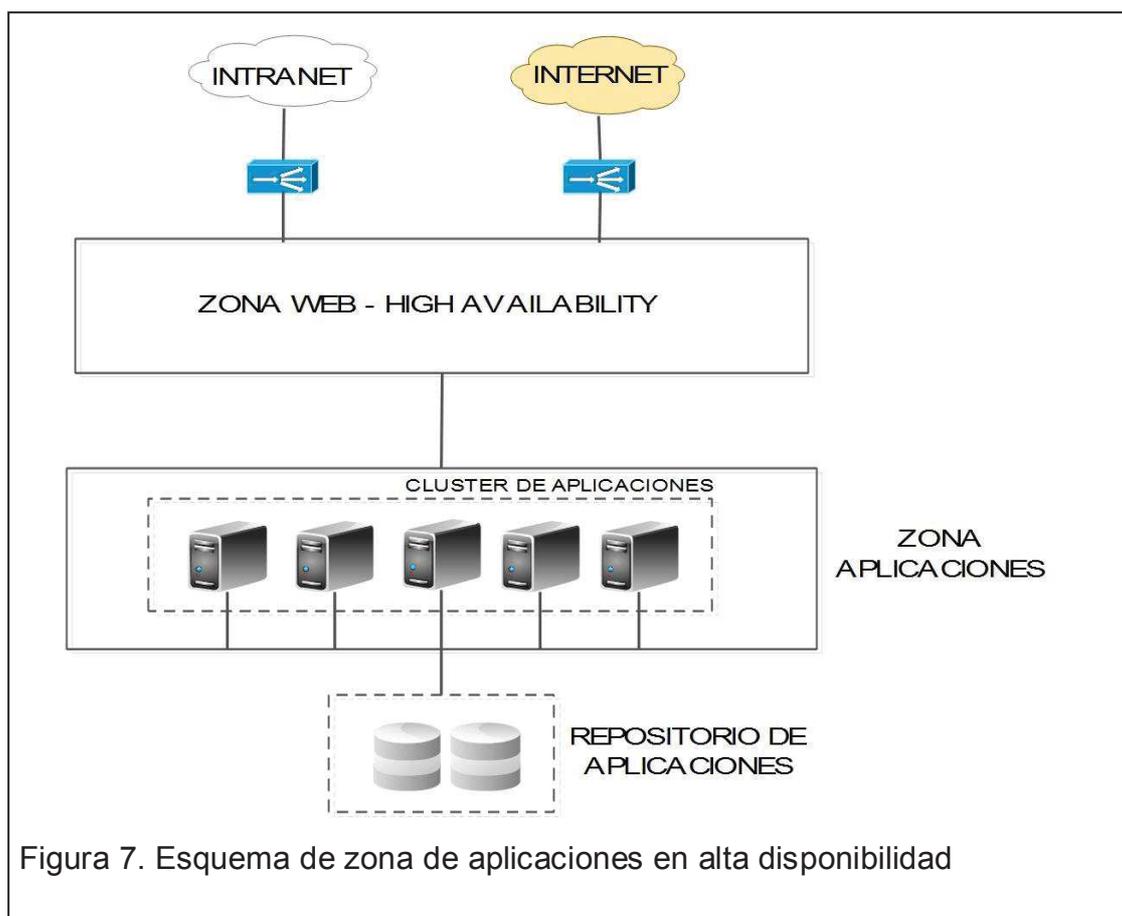
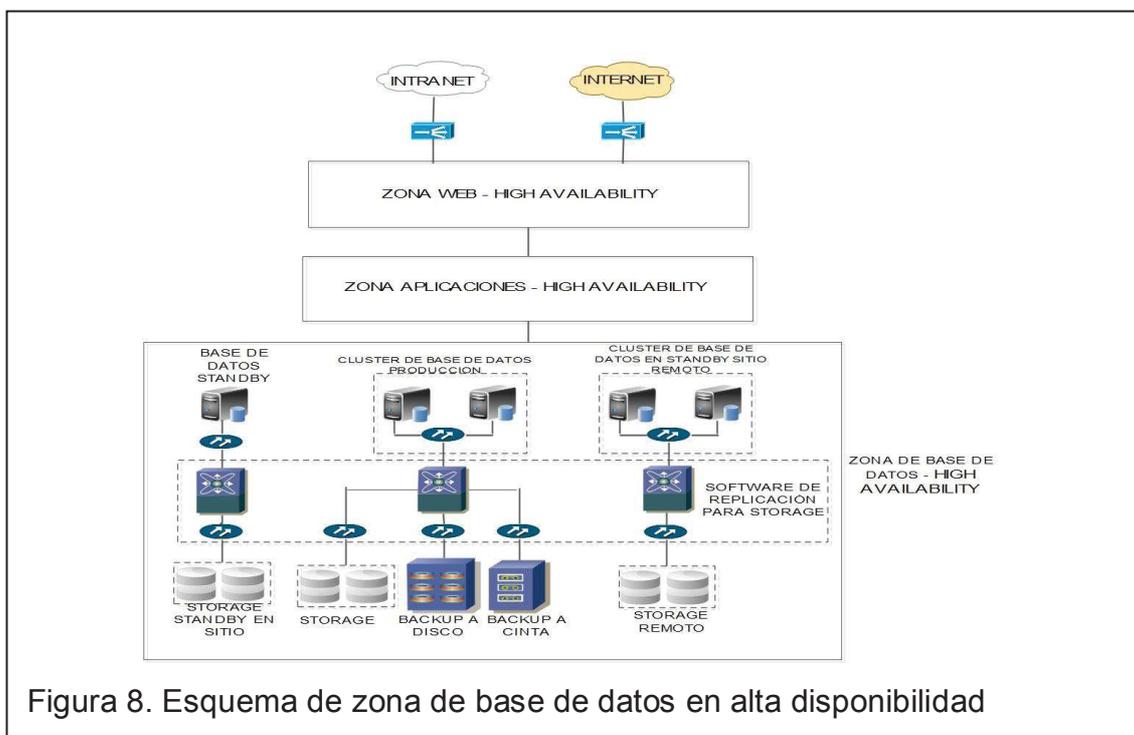


Figura 7. Esquema de zona de aplicaciones en alta disponibilidad

4.3. Zona de Base de datos

En esta capa debe estar la Base de datos de la Institución, para lo cual se establecieron las características de equipos sobre las cuales operará las base de datos. Para dar alta disponibilidad en esta capa se ha previsto mantener dos equipos de base de datos rackeables en dos racks distintos cada uno configurado en un esquema standby. Estos equipos se encontrarán directamente conectados a un almacenamiento distinto, el mismo que tendrá un software de replicación, que permitirá dar alta disponibilidad a esta capa que se la considera más crítica.

Con la finalidad de manejar los riesgos ante posibles fallas de equipos, de hardware, o humanos, se sugiere prever que el esquema de alta disponibilidad dado tenga un tiempo mínimo de pérdida de datos, considerando que la base de datos de la Institución no es transaccional, lo cual facilita la solución que se vaya a proponer, que bien podría utilizar un software de replicación a nivel de almacenamiento. En la figura 8 puede esquematizar la zona web en alta disponibilidad.



5. Capítulo V. Análisis de Costos

Para dar solución efectiva al diseño propuesto se ha previsto la adquisición de equipamiento de red para la red LAN y el centro de datos.

Los costos de cada ítem de la solución propuesta se han evaluado entre varias propuestas económicas de algunos proveedores y se ha considerado en cada caso la propuesta que cumple con las especificaciones mínimas requeridas por la Institución, sin que necesariamente sea la más económica. Es así a continuación se detalla los costos para cada necesidad:

Tabla 16. Costos de equipamiento para la red LAN

CANTIDAD	DESCRIPCIÓN EQUIPAMIENTO	VALOR UNITARIO	VALOR TOTAL
1	SWITCH CORE MODULAR HP7510	77.696,33	77.696,33
5	SWITCH DE ACCESO 48 P HP5120	7.836,75	39.183,75
1	SWITCH DE ACCESO 24 P HP5120	6.636,75	6.636,75
1	SISTEMA DE MOVILIDAD HP	7.510,18	7.510,18
288	PUNTOS DE RED CABLEADO ESTRUCTURADO	334,63	96.373,44
4	GABINETES DE PISO	1.585,07	6.340,28

Tabla 17. Costos de equipamiento de seguridades físicas para el Centro de Datos

CANTIDAD	DESCRIPCIÓN EQUIPAMIENTO	VALOR UNITARIO	VALOR TOTAL
1	SISTEMA DE DETECCIÓN Y EXTINCIÓN DE INCENDIOS	17.998,26	17.998,26
1	PUERTA DE SEGURIDAD	2.483,14	2.483,14
1	CONTROL DE ACCESOS	2.810,86	2.810,86

Tabla 18. Costos equipamiento Data Center

CANTIDAD	DESCRIPCIÓN EQUIPAMIENTO	VALOR UNITARIO	VALOR TOTAL
----------	--------------------------	----------------	-------------

2	UPS 16 kva	18.453,30	36.906,60
1	RACK CABLEADO ESTRUCTURADO PANDUIT	8.108,53	8.108,53
1	RACK DE SERVIDORES	8.108,53	8.108,53
2	EQUIPAMIENTO DE AIRE ACONDICIONADO (EQUIPOS EN REDUNDANCIA)	36.432,66	72.865,33
1	SUPRESOR DE TRANSIENTES 130 kva TRIFASICO	1.690,78	1.690,78
1	PISO ELEVADO 24 m2	12238,93	12238,93
1	PUERTA DE SEGURIDAD DATA CENTER	2483,14	2483,14

Tabla 19. Costos equipamiento de equipos servidores, almacenamiento y respaldos

CANTIDAD	DESCRIPCIÓN EQUIPAMIENTO	VALOR UNITARIO	VALOR TOTAL
1	BLADE CENTER CHASIS	117093,00	117093,00
4	SERVIDORES BLADES INTEL	100512,00	402048,00
2	SERVIDORES POWER (PARA BDD EN STANDBY)	182618,15	365236,30
2	ALMACENAMIENTOS (EN ALTA DISPONIBILIDAD)	244292,56	488585,12
1	RESPALDOS VIRTUALES	111843,60	111843,60
1	LIBRERIA DE RESPALDOS	43924,80	43924,80
1	SOFTWARE DE RESPALDOS	68235,60	68235,60
1	EQUIPOS BALANCEADORES	40000,00	80000,00

Tabla 20. Costos de los enlaces

CANTIDAD	DESCRIPCIÓN EQUIPAMIENTO	VALOR UNITARIO	VALOR TOTAL
1	Enlace Quito-Guayaquil 2MB con un SLA de 99,9	237,50	237,50

2	Enlace Quito-Cuenca 2MB con un SLA de 99,9	237,50	237,50
3	Servicio de Internet 30MB SDSL clear channel 1:1. SLA 99,9	3270,00	3270,00

Tabla 21. Puntos de red para las sucursales

CANTIDAD	DESCRIPCIÓN EQUIPAMIENTO	VALOR UNITARIO	VALOR TOTAL
15	Puntos de red Suc. Guayaquil	334,63	5019,45
15	Puntos de red Suc. Cuenca	334,63	5019,45
4	Switch 24 ptos.	6.636,75	26547,00

Tabla 22. Costos de equipos de seguridad perimetral

CANTIDAD	DESCRIPCIÓN EQUIPAMIENTO	VALOR UNITARIO	VALOR TOTAL
2	Appliance de seguridad de Gateway Principal y Secundaria para mediana empresa	142949,89	142949,89
2	IPS	7400,00	14800,00
4	Appliance de seguridad de Gateway para mediana empresa empresas para las sucursales	5180,00	20720,00

5.1. Análisis de Costos / Beneficio

Entre los costos fijos que tendría el proyecto podemos enumerar a los siguientes:

Los costos del cableado estructurado son aproximadamente de: USD \$ 233740,73.

Los valores aproximados de las seguridades del centro de datos es de aproximadamente USD \$ 23292,26.

Los costos del equipamiento del centro de datos es de aproximadamente de USD \$: 142401,84

Los costos de equipamiento de equipos servidores, almacenamiento y respaldos es de aproximadamente USD \$: 1676966,42.

Los valores aproximados para los enlaces con un solo proveedor es de USD \$ 3745,00, se debería considerar el doble del valor para enlaces redundantes con otro proveedor bajo las mismas características y condiciones de servicio.

Aproximadamente el costo para los puntos de red de las sucursales tanto de Guayaquil, como de Quito sería de USD \$.36585,00 que incluye el costo de Switch's de red de 24 puertos redundantes.

El valor aproximado para equipos de seguridad perimetral redundantes tanto para la oficina principal de la ciudad de Quito, así como también para las sucursales es de USD \$ 178469,89.

Los costos de instalación, configuración, implementación, así como también de de soporte y garantía de equipos ya se encuentran incluidos en los valores de cada ítem.

Estos rubros se pueden esquematizar en la siguiente tabla:

Tabla 23. Costos totales del proyecto

ITEM	DESCRIPCION	COSTO
1	CABLEADO ESTRUCTURADO	233740,73
2	SEGURIDADES DEL DATA CENTER	23292,26
3	EQUIPAMIENTO CENTRO DE DATOS	142401,84
4	EQUIPAMIENTO SERVIDORES	1676966,42
5	COSTOS DE LOS ENLACES	3745,00
6	PUNTOS DE RED SUCURSALES	36585,00
7	SEGURIDAD PERIMETRAL	142989,89
TOTAL:		2295201,14

Se realiza a continuación un esquema gráfico del beneficio social en relación al costo de inversión del proyecto:

Costos:

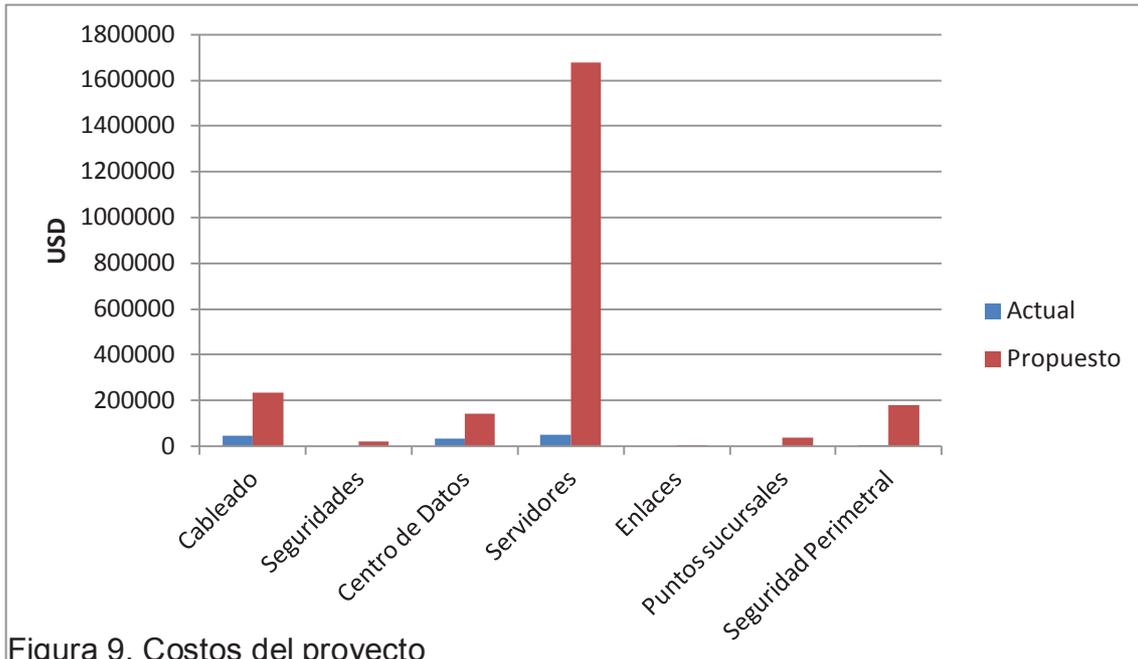


Figura 9. Costos del proyecto

Además, se puede apreciar también la cantidad de sujetos obligados que reportan actualmente vs. la cantidad de sujetos obligados que se irán incorporando a reportar luego de la implementación del presente proyecto.

Beneficio social:

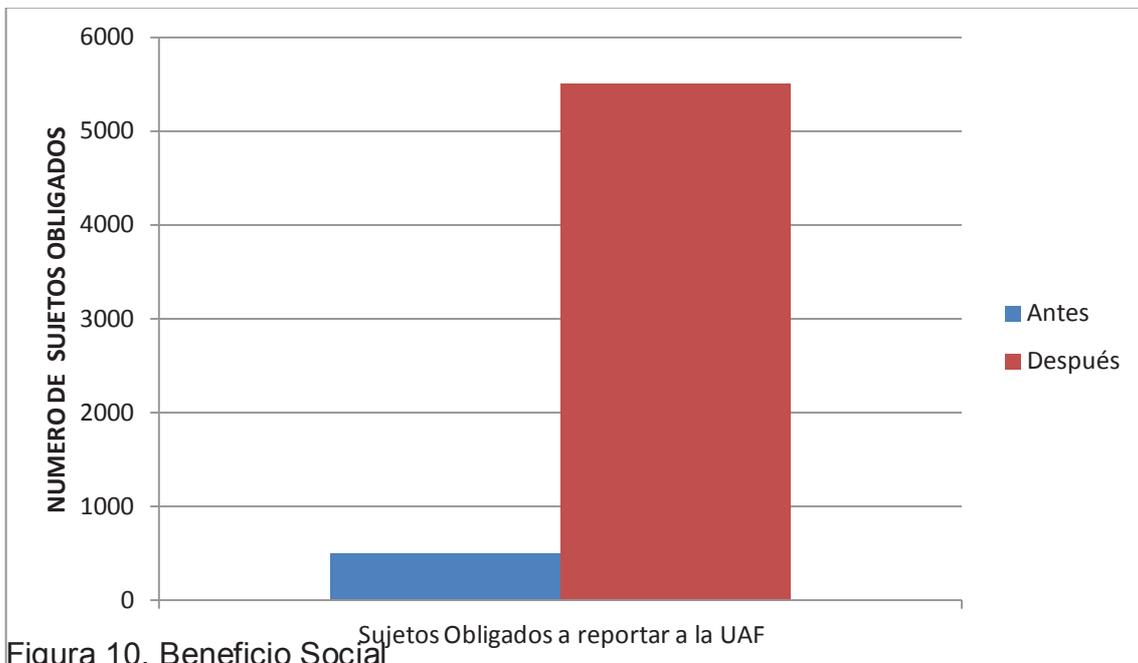


Figura 10. Beneficio Social

5.2. Costos Fijos del Proyecto

La Unidad de Análisis Financiero al ser una entidad de Gobierno tiene la responsabilidad con el país de prevenir, detectar y erradicar el lavado de activos, lo cual es una actividad criminal que comúnmente está asociada al narcotráfico, trata de personas, secuestro, pornografía infantil, actividades que financian el terrorismo, etc.

Los costos del proyecto no tienen un retorno de inversión económico, sino más bien el beneficio de la inversión realizada por la Unidad de Análisis Financiero al ser una entidad del Estado se vería reflejada en el servicio proporcionado a todos los usuarios de los diversos sectores económicos que tienen la obligación de emitir los reportes financieros hacia la Institución.

Al ejecutar el presente proyecto se obtendrá un beneficio social a todo el país, ya que la Institución tendrá los mecanismos tecnológicos suficientes y podrá colaborar con la erradicación del delito de lavado de activos el mismo que afecta a toda nuestra sociedad, en virtud que generalmente los delitos más comunes de blanqueamiento de capitales son la trata de personas, narcotráfico, pornografía infantil, etc.

El delito de lavado de activos involucra delitos que afectan a nuestra sociedad ecuatoriana en nuestro diario vivir, por lo que ejecutar el proyecto planteado a través de esta tesis ayudará a cumplir la misión de la Unidad de Análisis Financiero con el Estado Ecuatoriano.

El proveer un adecuado servicio a través de la página web institucional, proporciona al usuario (sujeto obligado) la calidad en el servicio, la rapidez y eficiencia en el servicio informático; esto representaría mejores tiempos de respuesta y garantizaría el cumplimiento de la Ley al usuario externo con la información reportada.

Los funcionarios de la Institución tendrán la posibilidad de obtener accesos a los distintos servicios informáticos en menores tiempos, lo cual generaría mejor atención al público que permanentemente solicita información a la Institución.

Las características del cableado estructurado permitirían a los funcionarios a mantener una comunicación idónea mediante video-conferencias con las Entidades de Gobierno de Control del Ecuador, así como también con las Instituciones Homólogas de los distintos países de Sur y Centro América, con el objetivo de intercambiar información y erradicar el delito de Lavado de Activos.

Con la implementación de la nueva infraestructura la Institución podrá acortar el plazo previsto para recibir los reportes de todos los sujetos obligados; es decir, la UAF tendrá la posibilidad de recibir los reportes de todos los sujetos obligados sin tener que emitir resoluciones de prórrogas al plazo. Por lo tanto, permitirá que la Institución pueda elaborar reportes de mejor calidad para la Fiscalía General del Estado, lo que le permite también consolidarse tecnológicamente dentro de las Instituciones del Estado ofreciendo un mejor servicio al país.

6. Capítulo VI. Conclusiones y Recomendaciones

Este capítulo tiene por finalidad exponer las conclusiones y las recomendaciones obtenidas en el transcurso del desarrollo del presente trabajo.

6.1. Conclusiones

- La Unidad de Análisis Financiero al mantener un esquema de alta disponibilidad en equipamiento de red LAN permite minimizar los riesgos de ausencia de servicios de red por razones técnicas de fallas de equipos activos, o situaciones similares, lo cual le permitirá ofrecer una atención ininterrumpida de los servicios informáticos que la Institución ofrece tanto a los usuarios internos como también a los externos.
- La aplicación de conceptos de calidad de servicio en la red de datos con la finalidad de superar los efectos de la congestión de tráfico producidos por los distintos servicios que se incorporarán ya sean de voz, datos y video, permite utilizar de manera eficiente los recursos de la red disponibles.
- Al segmentar la red se garantiza el acceso a las personas autorizadas a los diferentes servicios de red que la organización pone a disposición de los distintos tipos de usuarios internos de la red. Por la naturaleza de la Institución esta práctica es muy conveniente.
- Al tomar el concepto del modelo jerárquico de 3 capas de Cisco se espera que al proveer switches de core y de acceso en la red LAN de la Institución se pueda disponer de un diseño fácil de mantener, y además faciliten la escalabilidad en la red; este hecho aportaría significativamente a la red de la Institución cuando se requiera realizar adiciones ya sea en la configuración o en equipos.
- Mantener un esquema de alta disponibilidad en los equipos servidores, permite garantizar que los servicios informáticos que provee la Institución a los

distintos sectores económicos del país, se encuentren operativos; es decir, se garantiza la alta disponibilidad de toda la infraestructura tecnológica.

- Disponer de equipos de almacenamiento en redundancia garantiza la disponibilidad de la información en casos de fallas de equipo, errores humanos, fallas técnicas, etc.

6.2. Recomendaciones

Mantener altos estándares tecnológicos ya sea en equipamiento de red como en equipamiento de servidores y almacenamiento, puesto que los sectores económicos obligados a enviar mensualmente los reportes a esta Institución crecerán tanto en número como también el tamaño de archivos, y es necesario estar preparados para los retos futuros.

- Mantener actualizada la plataforma tecnológica en virtud que la Unidad de Análisis Financiero es una Institución que es evaluada anualmente por Organismos Internacionales, teniendo como gran responsabilidad generar altos resultados, teniendo como eje principal el manejo adecuado de la información.
- Mantener un esquema de alta disponibilidad en equipamientos de red LAN con la finalidad de garantizar la operatividad de los servicios, así como también asegurar la confiabilidad de la red, aporta significativamente a que la operatividad de todos los servicios informáticos de la Institución sean 7x24.
- Dotar de tecnología actualizada a la infraestructura de hardware de la UAF con la finalidad de mantener altos estándares de servicios a los usuarios finales, aportando directamente a las exigencias tecnológicas de las Entidades análogas internacionales y cumpliendo de esta manera con las recomendaciones del GAFISUD (Grupo de Acción Financiera de Sudamérica).
- Proveer de ambientes virtualizados en una infraestructura nueva tendiente a cloud, lo cual permitirá ahorro en costos operacionales, así como también administrativos.

- Es recomendable elaborar planes de mantenimiento para toda la infraestructura tecnológica de la UAF, con la finalidad de mantener operativos los equipos y por ende los servicios informáticos que presta la Institución.
- Se recomienda también elaborar políticas de seguridad con la finalidad de implantarlas en la Institución, ya que por la naturaleza de la misma, resulta un grave riesgo el prescindir de un documento que ofrezca directrices en cuanto a la forma de manipular información sensible.
- Es recomendable proveer alta disponibilidad en equipos de almacenamiento, con la finalidad de garantizar la disponibilidad de los datos, considerando que el mayor activo que posee la UAF es la información.
- Es recomendable dotar de una solución de respaldos robusta con la finalidad de contar con información respaldada actualizada que permita ser una medida de contingencia ante posibles eventualidades de cualquier tipo.
- Es recomendable que además de mantener alta disponibilidad con equipamiento de red y equipamiento de servidores en sitio, se provea de un centro de contingencia alterno en otro sitio que permita una capacidad de recuperación en tiempos mínimos en casos de desastres naturales o errores humanos.
- Se recomienda que la Institución elabore un documento de Políticas de Seguridad basadas en un ISO de Seguridad 27000, con la finalidad de precautelar la información de carácter confidencial y reservada que manipula.

REFERENCIAS

- Arquis., Arquitectura., (2011). La escalabilidad. La escalabilidad es en telecomunicaciones y en ingeniería informática. Recuperado el 7 de mayo de 2013 de <http://www.arqhys.com/construcciones/escalabilidad.html>
- Avaya.,(2013). Redes Informáticas. Haceredes. Escalabilidad. Recuperado el 05 de enero de 2013 de <http://haceredes.zobyhost.com/escalabilidad.html>
- Axis., Communications AB., (2013). Consideraciones sobre ancho de banda y almacenamiento. Recuperado el 5 de mayo de 2013 de http://G.729/www.axis.com/es/products/video/about_networkvideo/bandwidth.htm
- Bernardos, C., Soto, I., Calderón, M.,Dirkvon, H., Riou, E., (2011). IPV6 Más que un protocolo. Recuperado el 15 de diciembre de 2012 de Novática: Revista de la Asociación de Técnicos de Informática, ISSN 0211-2124, N°. 174, 2005 (Ejemplar dedicado a: IPv6. Más que un protocolo) , 37-43
- Bernardos, C., Soto, I., Calderón, M., (2011). The Internet ProtocolJournal - Volume 10, No. 2 - IPv6 Network Mobility . Recuperado el 15 de diciembre de 2012 de http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-2/102_ipv6.html
- Brines,L. (2010). Redes Convergentes. Recuperado el 18 de diciembre de 2012 de <http://es.scribd.com/doc/38558691/Redes-Convergentes-Leopoldo-Brines>
- Castillo, C., Rodemar, U., Hernández, G., Onofre, M., Gómez, J., Rosas, I. (2010). Redes de Computadora I. Recuperado el 7 de enero de 2013 de <http://es.scribd.com/doc/50038696/Trabajo-investigacion-1video> Tercera parte. Recuperado el 06 de mayo de 2013 de <http://noticias.alas->

la.com/version_anterior/index.php/tutoriales-anteriores/279-tutorial-ed44.html

Contreras., Omar., Contreras., Nicolás., (2011). Modelo Matemático para la Predicción de Ancho de Banda. Primera Aproximación. Recuperado el 6 de mayo de 2013 de <http://www.ingeborda.com.ar/biblioteca/Biblioteca%20Internet/Articulos%20Tecnicos%20de%20Consulta/Redes%20de%20Datos/Prediccion%20del%20ancho%20de%20Banda.pdf>

Cortés., German., (2011). Cómo calcular el ancho de banda de un enlace para video. Primera parte. Recuperado el 06 de mayo de 2013 de http://www.alas-la.org/Descargas_Socios/Ttutorial.ed41.pdf

Cortés., German., (2011). Cómo calcular el ancho de banda de un enlace para Witel., (2011). Interoperabilidad. Recuperado el 13 de enero de 2013 de <http://wikitel.info/wiki/Interoperabilidad>

EPN., EDU., EC., (2011). Diseño de una red inalámbrica . Recuperado el 15 de enero de 2013 de <http://dspace.epn.edu.ec/bitstream/15000/8652/2/T10514CAP3.pdf>

Gerometta., Oscar., (2009). Método simplificado para el cálculo de ancho de banda para VoIP. Recuperado el 18 de enero de 2013 de <http://librosnetworking.blogspot.com/2009/04/metodo-simplificado-para-el-calculo-de.html>

IMDEA., Networks. (2011). Interoperabilidad entre redes, un problema con solución. Recuperado el 15 de enero de 2013 de <http://www.madrimasd.org/blogs/sociedadinformacion/2011/09/14/131705>

Juanin.,(2009). Que es escalabilidad. Recuperado el 15 de diciembre de 2012 de <http://juanin.bligoo.com/content/view/626734/Que-es-Escalabilidad.html>

Kioskea., (2011). Alta disponibilidad. Recuperado el 18 de diciembre de 2012 de <http://es.kioskea.net/contents/surete-fonctionnement/haute-disponibilite.php3>

Ley de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos. (2010). Quito, Ecuador: Registro oficial Suplemento 352.

Mejía, A.M. (2004). Redes Convergentes. Recuperado el 12 de diciembre de 2012. <http://redalyc.uaemex.mx/pdf/911/91101407.pdf>

Microsoft, Technet.,(2013). Diseño de un servidor de seguridad perimetral. Recuperado el 25 de junio de 2013 de <https://www.microsoft.com/spain/technet/recursos/articulos/secmod156.msp>

N.N., (2008). Implementación Asterisk-VOIP. Recuperado el 16 de enero de 2013 de http://es.wikibooks.org/wiki/Implementaci%C3%B3n_Asterisk-VoIP

N/N., (2011). Interoperabilidad entre redes. Recuperado el 13 de enero de 2013 de http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/COMUNW01/Tema_6_Desarrollado.htm

NN.(2011). Redes Convergentes. Recuperado el 11 de noviembre de 2012 de <http://www.caponline.webatu.com/elastixtech/?p=380>

Oppenheimer, Priscilla.,(2011). Top-Down Network Design. Indianapolis, USA.: Cisco Press.

Petisco, J.M. (1999). La convergencia de redes Integración de Voz, Datos y Vídeo sobre IP. Recuperado el 2 de febrero de 2013 de <http://www.idg.es/computerworld/La-convergencia-de-redes.Integracion-de-Voz,-Datos/seccion-ana/articulo-100104>

Robles, T., (2007). Movilidad en Redes IP. Recuperado el 15 de diciembre de 2012 de <http://www.google.com.ec/url?sa=t&source=web&cd=1&ved=0CB0QFjAA&url=http%3A%2F%2Fcatedra-orange.upm.es%2Ffileadmin%2Fdoc%2Fmovilidad-redes-ip.pdf&rct=j&q=movilidad%20en%20redes&ei=OReOTtKZlcnb0QHbzsxW&usg=AFQjCNHs4JcemWbSQ1n0h8gn3D87caKKxg&cad=rja>

Redatel. S.A., (2011). Soluciones en Datos y Seguridad. Recuperado el 15 de enero de 2013 de <http://www.redatel.net/html/DocumentosCCTV.html>

Tanenbaum., Andrews., (2003). *Redes de Computadoras*. México: Pearson Educación.

Unne.,Edu.,(2011). Transmisión de Datos. Recuperado el 16 de enero de 2013 de http://exa.unne.edu.ar/depar/areas/informatica/teleproc/Comunicaciones/Presentaciones_Proyector/TransmisiondeDatos.pdf

Servicios y Sistema Informáticos Virtuales, (2012). Como calcular el ancho de banda en un enlace de Video. Recuperado el 2 de mayo de 2013 de <http://sysvirtuales.com/como-calcular-el-ancho-de-banda-en-un-enlace-de-video-2/>

Zamora, H. (2002). Implementación de Redes MPLS-VPN Casos de Estudio. Recuperado el 11 de abril de 2013 de <http://www.google.com.ec/url?sa=t&rct=j&q=mpls&source=web&cd=5&ved=0CGIQFjAE&url=http%3A%2F%2Fwww.cudi.mx%2Fprimavera2002%2Fpresentaciones%2FMPLSVPN.pdf&ei=NczDTt6ZGpKbtwff05zfDQ&usg=AFQjCNE05c-sSLedP8fh4wIIG5WXz-wLSQ&cad=rja>

ANEXOS

ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS PARA EL CABLEADO ESTRUCTURADO DEL CENTRO DE DATOS DE LA UAF	
1. EQUIPOS ACTIVOS DE RED	
ITEM	CARACTERISTICAS PRINCIPALES
1	2 (dos) Switch de CORE modular, debe incluir 10 puertos de fibra SFP+ 10G, 48 puertos 10/100/1000, 24 puertos 10/100/1000, dos tarjetas procesadoras de 768 Gbps cada una. Debe Incluir soporte de hardware y software de fabricante por 3 años
2	10 (diez) Switch de acceso 48 puertos 10/100/1000 PoE+ debe incluir modulo con dos puertos SFP+ y 1 transceivers SFP+ 10G, soporte de hardware y software de fabricante por 3 años
2. SALA DE EQUIPOS	
3	1 (uno) Sistema de Detección y Extinción de Incendios con Gas Ecológico
4	2 (dos) Equipamientos de Aire Acondicionado en redundancia con capacidad total de enfriamiento de mínimo 50000 BTU/h
5	Acometida Eléctrica para el Sistema de Climatización, Evaporadora, Condensadora
6	1 (un) Supresor de transientes de 130 KVA trifásico tipo industrial
7	1 (una) puerta de seguridad con una dimensión de 90 x 205 cms, área libre elaborada en toll laminado en frio de 2,0 mm con estructura de soporte interior en 3mm.
8	1 (un) control de accesos biométrico con tarjeta de aproximación y teclado; con administración vía web sin la necesidad de costo de suscripción por software.
9	Iluminación de data center con encendido y apagado automático, debe incluir señalética y lámparas de emergencia.
3. OBRA CIVIL	
10	Levantamiento de paredes, debe incluir pintura, estucado y pintura. Dimensión 30m2
4. CUARTO DE UPS's	
11	1 (uno) Sistema automático de detección y extinción de incendios con

	Gas Ecológico
12	Pisos de vinil Antiestático para el área de cuarto de equipos
13	1 (una) puerta de seguridad con una dimensión de 90 x 205 cms, área libre elaborada en toll laminado en frío de 2,0 mm con estructura de soporte interior en 3mm.
14	Control de Acceso biométrico con tarjeta de aproximación y teclado; con administración vía web sin la necesidad de costo de suscripción por software.
15	Iluminación con encendido y apagado automático, debe incluir señalética y lámparas de emergencia.
5. EQUIPOS DE PROTECCIÓN ELÉCTRICA UPS	
16	2 (dos) UPS de 15 KVA trifásico con mínimo 15 minutos de respaldo
6. RED DE DATOS	
17	Rack Cableado Estructurado principal debe incluir manejadores verticales; número de parte CN1; regletas de conexión eléctrica, kits de aterrizado de equipos activos
18	288 (Doscientos ochenta y ocho) Puntos de red categoría 6A F/UTP. Todos los elementos de conectividad deben incluir patch cord usuario y gabinete. La canalización será utilizando canaleta plástica lisa decorativa si no existiera canalización empotrada o divisiones modulares para el efecto.
19	4 (cuatro) Gabinetes de piso abatible cerrado tipo armario, 12 UR debe incluir regleta de distribución eléctrica, 5 kits para aterrizado de equipos.
20.	4 (cuatro) Enlaces principales de fibra óptica OM3 hilos multimodo y 4 enlaces secundarios Todos los elementos de conectividad incluido fibra óptica deben ser de la misma marca. Deben incluir 8 patch cords de fibra óptica de 2 mts.
21	Memoria técnica, planos de instalación, diagramas, certificación
7. RED ELÉCTRICA REGULADA UPS	
22	Puntos de red eléctrica regulada implementado con cable bipolar flexible 3x12 AWG, tomacorriente, tierra aislada.
23	Puntos de red de energía normal implementado con cable flexible

	3x12 AWG, tomacorriente Veto Premio
24	Tablero de distribución eléctrica Data Center: debe incluir mecanismos de bypass y distribución para 4 UPS de 15 KVA. Sistema de distribución red normal y equipos de acondicionamiento de aire.
25	Tablero de distribución eléctrica regulada de piso, debe incluir acometida eléctrica
26	Acometida eléctrica 120 KVA desde tablero de medidores subsuelo 2 hasta tablero de distribución eléctrica Data Center. 3KVA con baterías para 30 minutos de respaldo automático.
27	Circuito dedicado para rack; debe incluir disyuntor de protección y canalización bajo piso falso.
28	Memoria técnica, planos de instalación, diagramas, certificación
8. SERVICIOS	
29	Instalación de 2 (dos) UPS's 15 KVA, debe incluir punto de red eléctrica normal implementado con cable flexible 3x12 AWG, tomacorriente Veto Primo. Debe incluir canalización y conductores tipo superflex desde tablero de bypass a UPS.
30	Instalación configuración y puesta en operación de toda la solución tanto de cableado estructurado, Switch's, Centro de Datos.
31	Debe incluir capacitación en toda la solución para 3 (tres) personas.
32	Debe incluir soporte de hardware y software por mínimo 3 años por parte del fabricante

**PROPUESTA ECONOMICA
EQUIPOS DE RED, CABLEADO ESTRUCTURADO, CENTRO DE DATOS,
DE UN PROVEEDOR**

DETALLE ECONÓMICO EQUIPAMIENTO INFORMATICO NUEVO EDIFICIO UNIDAD DE ANALISIS FINANCIERO					
Ítem	Unid	Descripción	Características Principales	Cant	P. sistema
GRUPO A: EQUIPAMIENTO ACTIVO DE RED					
1	u	Switch de CORE modular	Switch HP 7510, incluye 10 puertos de fibra SFP+ 10G, 48 puertos 10/100/1000, 24 puertos 10/100/1000, dos tarjetas procesadoras de 768 Gbps cada una. Incluye soporte de hardware y software de fabricante por 3 años	2	\$ 131,300.00
2	u	Switch de acceso	Switch HP 5120 de 48 puertos 10/100/1000 PoE+ incluye modulo con dos puertos SFP+ y 1 transceivers SFP+ 10G, soporte de hardware y software de fabricante por 3 años	10	
GRUPO B: CABLEADO ESTRUCTURADO					
4	u	Rack Cableado Estructurado Panduit incluye manejadores verticales; número de parte CN1	Rack Cableado Estructurado principal 45 UR, incluye manejadores verticales, regletas de conexión eléctrica, kits de aterrizado de equipos activos	1	\$ 127,618.40
5	u	Rack Servidores Panduit	Rack servidores 45 UR, incluye manejadores verticales, regletas de conexión eléctrica, kits de aterrizado de equipos activos	1	

6	u	Punto de red	Punto de red categoría 6A F/UTP, todos los elementos de conectividad Panduit incluye patch cord usuario y gabinete Panduit. La canalización será utilizando canaleta plástica lisa decorativa si no existiera canalización empotrada o divisiones modulares para el efecto.	288	
7	u	Gabinete de piso	Marca Panduit abatible cerrado tipo armario, 12 UR incluye regleta de distribución eléctrica, 5 kits	4	
8	u	Enlace Principal de fibra óptica a racks de piso	Enlace de fibra óptica OM3 6 hilos multimodo. Todos los elementos de conectividad incluido fibra óptica son de la marca Panduit. Incluye 8 patch cords de fibra óptica de 2 mts.	4	
9	u	Memoria técnica.	Memoria técnica, planos de instalación, diagramas, certificación	1	
GRUPO D: EQUIPOS DE PROTECCIÓN ELÉCTRICA UPS					
10	u	UPS 15 KVA	UPS 15 KVA trifásico 8 minutos de respaldo	2	
11	u	Instalación UPS 15 KVA	Instalación incluye canalización y conductores tipo superflex desde tablero de bypass a UPS	4	\$ 40,906.60
GRUPO E: RED ELÉCTRICA REGULADA UPS					
12	u	Puntos red eléctrica regulada	Punto de red eléctrica regulado implementado con cable multipolar flexible 3x12 AWG, tomacorriente Veto Premio o Leviton tierra aislada	215	\$ 85,285.20
13	u	Puntos de red de energía normal	Punto de red eléctrica normal implementado con cable flexible 3x12 AWG, tomacorriente Veto Premio	150	

14	u	Tablero de distribución eléctrica Data Center: incluye mecanismo s de bypass y distribución para 4 UPS s de 15 KVA. Sistema de distribución de red	Tablero de distribución y control de 4 UPSs de 15 KVA incluye sistemas de distribución para red regulada y red normal. Incluye medidores digitales de los principales parámetros eléctricos	1	
15	u	Tablero de distribución eléctrica regulada de piso	Tablero de distribución eléctrica regulada de piso incluye acometida eléctrica	4	
16	u	Acometida eléctrica 120 KVA desde tablero de medidores subsuelo 2 hasta tablero de distribución eléctrica Data Center	3 KVA con baterías para 30 minutos de respaldo automático, debe ser soportado por Windows 2003	1	
17	u	Circuito dedicado para rack	Circuito dedicado incluye disyuntor de protección y canalización bajo piso falso	10	
18	u	Memoria técnica,	Memoria técnica, planos de instalación, diagramas, mediciones	1	
GRUPO F: DATA CENTER					
19	u	Obra Civil	Levantamiento de paredes, incluye pintura, estucado y pintura	1	\$ 5,600.00
F1: SALA DE EQUIPOS					

20	u	Detección y Extinción de Incendios	Sistema automático de detección y extinción de incendios con Gas Ecológico NOVEC	1	\$ 105,660.80
21	u	Equipamiento de aire acondicionado (2 Equipos en redundancia)	Capacidad total de enfriamiento: 51100 BTU/h	2	
22	u	Acometida eléctrica	Sistema de Climatización	1	
23	u	Acometida eléctrica	Para evaporadora		
24		Acometida eléctrica	Para condensadora		
25	u	Supresor de transcientes	Tipo industrial	1	
26	u	Tablero	Sistema de Climatización	1	
27	u	Piso elevado	Paneles perforados, Rampa de acceso, paneles rellenos para 22 m2, desinstalación e instalación del piso existente	1	
28	u	Puerta de seguridad	Dimensiones: 90 X 205 cms. área libre elaborada en toll laminado en frió de 2,0 mm con estructura de soporte interior en 3 mm	1	
29	u	Control de accesos	Operación: Biométrico, tarjeta de aproximación y teclado Administración vía Web sin la necesidad software	1	
30	lote	Iluminación data center con encendido y apagado automático	Incluye señalética y lámparas de emergencia	1	
F2: CUARTO DE UPS`S					

31	u	Detección y Extinción de Incendios	Sistema automático de detección y extinción de incendios con Gas Ecológico NOVEC	1	\$ 23,293.20
32	u	Piso de Vinil Antiestático	Para el área del cuarto de equipos	1	
33	u	Puerta de seguridad	Dimensiones: 90 X 205 cms. área libre elaborada en toll laminado en frío de 2,0 mm con estructura de soporte interior en 3 mm	1	
34	u	Control de accesos	Operación: Biométrico, tarjeta de aproximación y teclado Administración vía Web sin la necesidad software	1	
35	lote	Iluminación sala de equipos con encendido y apagado automático	Incluye señalética y lámparas de emergencia	1	
TOTAL					\$519,664.20

**OFERTA ECONOMICA
DE SEGURIDAD PERIMETRAL EN ALTA DISPONIBILIDAD BASADA EN
APPLIANCES, DE UN PROVEEDOR**

Crecimiento de plataforma de Seguridad mediante Productos Check Point Dispositivos (Appliance)			
APPLIANCE DE ADMINISTRACIÓN Y APPLIANCE DE REPORTE			
Descripción	Appliance de Administración y Reporte	Cant.	Precio
Modelo de Administración Smart-1-5	Smart-1 Security Management managing gateways with 4 blades	1	\$ 9058.23
- Para 5 Gateways, expandible a 25 - 7500 log/seg. -Disco 500GB Renovación a 3 años	SmartWorkflow Blade (10 Gateways) Módulo de optimización del firewall. Es un módulo opcional que se instala en la administración que permite ver que reglas mayormente utilizadas en seguridad, reglas nunca utilizadas en la política.	1	\$ 3587.50
Reportes y Correlación de Eventos - Para 5 Gateways, expandible a 25 - 7500 logs/seg - Disco de 500GB Renovación a 3 años	Smart-1-5 SmartEvent Appliance with 3 Management blades	1	\$ 9058.23
SEGURIDAD DE GATEWAY EN ALTA DISPONIBILIDAD			
Descripción	Appliance para seguridad de Gateway principal	Cant.	Precio

Equipo Principal Appliance de Seguridad SG-4610 Renovación a 3 años	BLADES BÁSICOS -Firewall -VPN -Advanced Networking -Identity Awareness -Movilidad para 5 usuarios concurrentes SERVICES BLADES (anual) IPS Application Control URL filtering Antivirus&Antialware Antibot Antispam	1	\$ 36022.73
	BLADE BÁSICOS ADICIONALES Mobile Acces Blade for 50 concurrent connections	1	\$2695.45
	BLADE DE SERVICIOS ADICIONAL Data Loss Prevention (DLP) Blade for 3 years – for small size appliances	1	\$7670.45
APPLIANCE PARA SEGURIDAD DE GATEWAY SECUNDARIA			
Descripción	Appliances para seguridad de Gateway secundaria	Cant.	Precio
Appliance de Seguridad SG-4610	BLADES BÁSICOS Firewall HA VPN HA Avanced Networking HA Identity Awareness HA Movilidad para 5 usuarios concurr. HA SERVICE BLADES (anual) IPS HA	1	\$ 28818.18

	Application Control HA URL filtering HA Antivirus&Antimalware HA Antibot HA Antispam HA		
	BLADE BÁSICOS ADICIONALES Mobile Acces Blade for 50 concurrent connections – HA	1	\$ 2152.27
	BLADE DE SERVICIOS ADICIONAL Data Loss Prevention (DLP) Blade for 3 years – for small-size appliances – HA	1	\$ 6136.36
SERVICIOS			
Descripción		Cant.	Precio
Instalación y Configuración - Configuración y aplicación de política de seguridad - Afinamiento y pruebas		1	\$ 5026.15
Asistencia técnica 8 x 5, 3 años - Incluye asistencia de hardware en caso de daño		3	\$ 30770.34
Capacitación - Curso CCSS, 2 asistentes		2	\$ 1900.00

SISTEMA DE AIRE ACONDICIONADO

DESCRIPCION	REQUERIDO
Marca	Especificar
Modelo	Especificar
Características	
Control de temperatura y humedad	
Capacidad total	49000 BTU/H @22°C / 50%RH
Humificador	3Kg/hr (6,6 Lb/hr) tipo electrodo con botella generadora de vapor
Filtro de aire	30% de eficiencia
Refrigerante	R22 o R407C
Control	digital de microprocesador avanzado con alarmas
Instalación	sobre piso falso y retorno por la parte superior de la unidad
Caudal de aire	1200 CFM
Peso	Aprox. 120 Kgs / Especificar
Dimensiones	Evaporador 0.6 m x 0.6 m x 1.98 m alto. C d d t t t b i t d 32°C
Condensador externo	para temperatura ambiente
Dimensiones condensador externo	970x910x770 mm Peso 40Kg
Características eléctricas del equipo	3 Fases 208 VAC, más tierra.
Tubería	cobre deshidratada para un trayecto de aprox. 25 metros
Acometidas eléctricas	Aprox. 8m

SWITCH

DESCRIPCION	REQUERIDO
puertos	2 ranuras de estructura de conmutador

	<p>10 ranuras para modulo de e/s</p> <p>84 puertos 10GB</p> <p>10/100/1000 de detección automática</p> <p>mínimo 480 puertos spf</p>
Montaje horizontal memoria y procesador estructura	mips64 a 600 mhz, 64 mb de memoria flash, 512 mb de ram
memoria	1gb de memoria flash, 2gb de ram
modulo de e/s	<p>mips64 a 400 mhz</p> <p>1 gb de ram</p> <p>velocidad 714 millones de pps</p> <p>capacidad de encaminamiento/conmutacion</p> <p>1152 gbps tamaño de tabla de enrutamiento 256000 entradas</p> <p>funciones de gestión imc - intelligent management center; interfaz de línea de comandos</p>
Puertos de administrador	Snmp, telnet
interfaz	terminal (rs-232c serie); interfaz de modem
Energía y operación de voltaje de entrada	<p>100-120 / 200-240 vca corriente de entrada de funcionamiento 16 / 50 a</p> <p>frecuencia de entrada 50 / 60 hz</p> <p>seguridad ul 60950-1; iec 60950-1; can/csa-c22.2 no. 60950-1; en 60950-1/a11 compatibilidad electromagnética vcci clase a; en 55022 clase a; ices-003 clase a; ansi c63.4 2003; as/nzs cispr22 clase a; en 61000-3-2:2006; en 61000-3-3:1995 +a1:2001+a2:2005; directiva emc 2004/108/ec; fcc (cfr 47, apartado 15) clase a</p>
Temperaturas operativas	0 a 45c intervalo de humedad en funcionamiento de 10 a 95% (sin condensacion)
Peso y tamaño	(p x a x l) 42,0 x 43,6 x 70,8 cm peso del producto 95,71 kg

Garantía	3 años en partes y piezas contra defectos de fabricación
----------	--

SISTEMA DE DETECCION Y EXTINCION DE INCENDIOS

CARACTERISTICAS	REQUERIDO
Marca	Especificar
Modelo	Especificar
Generales	Sistema diseñado para saturar el volumen en una concentración del agente HFC125 diseño hidráulico mediante software aprobado del fabricante listado UL y aprobado FM, saturación en menos de 10 segundos y más de 6 segundos según lo establece la norma
Volumen de concentración	8% según NFPA 2001
Diseño	hidráulico mediante software aprobado del fabricante listado UL y aprobado FM
Saturación	menos de 10 segundos y más de 6 segundos según lo establece la norma
Panel de control	UL Aprobado FM, para control en zona secuencial y/o cruzada de detectores de humo
Sistema de auto diagnóstico	de errores y fallas, display alfanumérico, leds de indicación de estatus
Detectores fotoeléctricos	bajo perfil y alta eficiencia para ser distribuidos estratégicamente en el ambiente de equipos y bajo piso falso
Señalización interior	Sirenas con luz estroboscópica
Pulsador	manual de descarga manual de aborto

Debe incluir	Rótulos de señalización Baterías de respaldo
SISTEMA DE EXTINCIÓN	
Agente extintor	Especificar/ Cilindro contenedor, kit de activación, kit de anclaje, manómetro indicador de presión, toberas de descarga.
Volumen	aprox. de 37.5 m3 Especificar agente
Tubería	Cédula 40 soporte e interconexión con el sistema de detección