FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

REDISEÑO DE LA INFRAESTRUCTURA DE RED DE LA EMPRESA AKROS

Trabajo de titulación presentado en conformidad a los requisitos
establecidos para optar por el título de
Ingeniero en Redes y Telecomunicaciones.

Profesor Guía
Andrés Almeida

Autor
David Yépez

Año
2014

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante David Yépez, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los trabajos de titulación.”

Andrés Almeida
Ing. Electrónica y Telecomunicaciones
171599997-3

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”

_____

David Alejandro Yépez Dávila

171585342-8

AGRADECIMIENTOS

A mis padres y a mi novia que siempre han sido los que me apoyan con todo y me brindan ese respaldo y ayuda invaluable día tras día.

DEDICATORIA

Este trabajo se lo dedico en especial a mi padre, porque él me ha apoyado en la consecución de mis metas y me ha respaldado siempre.

RESUMEN

El siguiente trabajo de titulación, “REDISEÑO DE LA INFRAESTRUCTURA DE RED DE LA EMPRESA AKROS” está enfocado exclusivamente en el rediseño de la red de la empresa Akros, el cual ayudará a mejorar notablemente su desempeño y eficiencia. Este rediseño contará con algunas herramientas informáticas tales como emuladores y software especializado, que permitirán visualizar algunos de los puntos de la red a mejorar.

El desarrollo de la tesis se realizará analizando los servicios actuales que están cursándose en la red, verificando un tema fundamental como lo es el costo beneficio de servicios y equipos. De igual manera, se propondrá el incremento o mejora de varias herramientas de red, lo que permitirá desarrollar las funciones laborales con mayor rapidez y eficiencia.

El objetivo de la tesis es rediseñar una red capaz de soportar la demanda actual de la empresa, contar con buenas practicas informáticas y sobre todo que sea muy eficiente.

La elaboración de la tesis se divide en cuatro capítulos los cuales de forma secuencial abarcan el estudio previo de la red, identificando los problemas que se vienen suscitando. Luego se desarrollan las herramientas practicas sobre las cuales se sustentará la solución.

Con el estudio de estos y otros puntos, se planteará un nuevo diseño de la red a mediano plazo, los mismos que se notarán tanto físicamente así como en el ámbito de rendimiento y confiabilidad.

SUMMARY

The following graduation work, "REDESIGN OF THE NETWORK INFRASTRUCTURE OF AKROS COMPANY" focuses exclusively on the network redesign of Akros company, which will help significantly to improve the performance and efficiency. This redesign will have some tools such as emulators and specialized software that will display some of the points in the network to improve.

The development of the thesis will be analyzing the current services that are attending on the network, verifying a fundamental issue as is the cost benefit of services and equipment. Similarly, it is proposed to increase or improve various network tools, thereby allowing job functions more quickly and efficiently.

The aim of the thesis is to redesign a network capable of supporting the current demand of the company, count with good computing practices and especially focused on the efficiency.

The development of the thesis is divided into four chapters which cover the sequentially previous study of the network, identifying the problems that have been raising and then develop practical tools which will be based on the solution.

With the study of these and other points, will consider a new design of the network in the medium term, the same that will be felt both physically and in the area of performance and reliability.

INDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Todo este trabajo de investigación viene de la mano con la ayuda que brinda Akros, ya que al facilitar la topología de red, interconexión entre equipos y el equipamiento tecnológico actual, permitirá obtener una mejor perspectiva de la misma, evidenciando sus falencias y virtudes.

Este proyecto realizado en la empresa Akros, se lo desarrolla bajo la pauta de "rediseño de red", ya que todas las pruebas (emulaciones, observaciones, recopilamiento de información) realizadas en este trabajo serán debidamente analizadas. Es muy importante notar que Akros al ser una empresa de tecnología, debe poseer una red muy eficaz, pero actualmente tiene varios puntos a mejorar en dicha red, y es aquí donde nace la iniciativa de rediseñar la misma.

Dentro de los puntos más importantes que se plantean para obtener una mejora en la red, está la emulación del protocolo BGP y el mecanismo de rastreo de paquetes IP SLA (ambos no están siendo empleados), utilizando para ello el software GNS3, en donde ambos permitirán utilizar redundancia entre 2 enlaces de forma automática.

Otro aspecto importante a mencionar es la utilización a futuro de las normas ITIL e ISO y TIA que la empresa no posee y que son de mucha importancia, ya que aquí se hace uso de recomendaciones de mejores prácticas a implementar en la red y en la empresa en general mediante una guía de normativas. Se debe recalcar que para ejecutar eficiente las mejores prácticas dentro de una empresa, primeramente deben existir procesos, los mismos que demandan gran cantidad de tiempo para ser desarrollados, por lo que directamente se realizará un análisis de cada norma, extrayendo lo esencial que se podría aplicar en Akros para su mejora.

CAPÍTULO I

1 Situación actual

1.1 Introducción a la empresa Akros

Akros es una empresa de tecnología informática con más de veinte años en el mercado ecuatoriano. El enfoque principal de la empresa, está basado en el mercado corporativo. Con varios reconocimientos de importantes marcas como LEXMARK, HP, DELL, MICROSOFT, CISCO, MVWARE, XEROX y SYMANTEC, Akros es uno de los socios (*partners*) de tecnología, más grandes en el Ecuador, recibiendo así, en el año 2012 el reconocimiento por parte de HP, como el "socio preferido" en ventas del año 2011.

Misión: Mejorar cada día para brindar soluciones tecnológicas corporativas alineadas a las tendencias del mercado.

Visión: Ser reconocidos como el mejor proveedor, empleador y socio comercial del sector tecnológico en el 2015.

Entre las contenidos del negocio, se puede encontrar la administración de centros de datos, virtualización de estaciones de trabajo, elaboración de cableado estructurado, respaldo y recuperación de datos, mantenimientos preventivos y correctivos, *outsourcing* de *help desk* y renta de equipos. A todo esto se debe añadir, que la compañía posee un gran proyecto de tecnología con el Gobierno llamado proyecto "Marco", donde se han vendido miles de equipos como *laptops*, *desktops*, impresoras, cableado estructurado y además se brinda soporte, asesoría y mantenimiento a los mismos.

Cabe recalcar que Akros es la primera empresa en ganar una subasta electrónica de tecnología, a través de un portal web que a su vez proveyó un catálogo electrónico de equipos de tecnología a sus compradores y además, la gran demanda en el mercado de tecnología ha permitido que Akros crezca en los últimos años y tenga la posibilidad de invertir en equipos de *networking*.

Sin embargo, la infraestructura de su red interna plantea ciertos problemas, para los cuales se han buscado cambios tecnológicos y/o necesidades técnicas tal como lo indica la siguiente tabla 1:

Tabla 1 Necesidades técnicas para el rediseño de red

Problema	Solución Planteada
Lentitud al navegar, descargar archivos, acceder a aplicaciones, etc, son algunas de las causas que enfrenta la empresa en el día a día, las mismas que no permiten un óptimo desempeño laboral y retrasan actividades.	Esto se puede resolver con la ampliación de la capacidad del canal, con el fin de mejorar la productividad al momento de realizar tareas cuotidianas tales como subastas públicas, venta de equipos a través del portal web, descarga de software, etc.
Caídas en el enlace, lo que paraliza la conexión a través de internet con los clientes y empleados que posee la empresa, tornando así la comunicación y la operatividad de la red en un problema.	Una solución viable es la contratación de un enlace de respaldo con otro ISP, el cual garantice una mayor disponibilidad y mejore el nivel de servicio en todo momento. De esta manera se podrá evitar cortes o caídas de comunicación dentro y fuera de la empresa por la falta de internet.
Falta de cobertura inalámbrica en diferentes áreas de la empresa, lo que ha conllevado a minimizar ciertos lugares de trabajo cuando se hace uso de la señal inalámbrica.	Para resolver este inconveniente se puede realizar una reubicación o un incremento de *access points,* basados previamente en una medición y recopilación de información de la señal inalámbrica.
Desperdicio innecesario del direccionamiento IP, debido a que la empresa no cuenta con una segmentación óptima, basada en las diferentes áreas laborales.	Para mejorar esto, se puede realizar un nuevo subnetting, tomando en cuenta aspectos como las VLAN's existentes y la cantidad de usuarios que a futuro podría llegar a haber.
Carencia de VLAN's creadas en comparación a la cantidad de áreas que la empresa posee, lo que representa poca flexibilidad y riesgos en la seguridad de la red LAN.	Una solución muy rápida a este problema, es la creación de más VLAN's, basadas en las áreas más influyentes dentro de la compañía, lo que permitiría mayor eficiencia en la red, ya que usuarios con requerimientos similares estarían dentro de la misma VLAN reduciendo al mismo tiempo problemas con los dominios de broadcast.

Estos cambios tecnológicos previamente planteados, son los puntos críticos donde recae el objetivo principal de este proyecto, que es el rediseñar la red de Akros, ya que la actual está teniendo dificultades para soportar la creciente demanda de servicios tecnológicos que la empresa está enfrentando por parte de sus clientes y empleados.

Una vez cubiertas las necesidades básicas por las cuales se planteó el rediseño de la red de Akros, se podrán incorporar sistemas adicionales que ayudaran a mejorar el desempeño de la red, tales como:

- Mejoramiento en la capacidad y procesamiento de los servidores que realizan virtualización, ya que aquí corren las aplicaciones empleadas para la atención al cliente final.
- Políticas de seguridad para el ingreso a áreas restringidas.
- Mejoramiento en la atención al cliente, con respecto al ingreso, configuración de equipos.
- Estandarización en la realización de mantenimientos preventivos y correctivos a los clientes.
- Un sistema biométrico para el acceso al *data center*.
- Un sistema de CCTV para la seguridad de las áreas sensibles de la empresa.
- Utilización de piso falso en el *data center.*
- Uso de un control de activos.
- Control para las contraseñas utilizadas.
- Mayor espacio en el data center para la colocación de futuros equipos.
- Redundancia de los enlaces entre los switches de distribución (*link aggregation* 802.3ad).
- Redundancia con los componentes eléctricos.
- Utilización de un sistema de distribución de energía PDU.
- Mejoramiento de la refrigeración en el *data center*, para optimizar el desempeño de sus equipos.
- Configuración dentro del *firewall* de una VPN para los técnicos o ingenieros que salgan a visitas fuera de la empresa.

- Análisis de carga para satisfacer las necesidades futuras de energía en el *data center*.
- Creación de un *bypass* para el UPS en caso de mantenimientos.
- *Backup* en el *switch* de *core.*
- Peinado del cableado estructurado.

Siendo el *data center* el área que abarca la mayor cantidad de equipos de *networking,* a continuación se podrá visualizar la situación actual del mismo con las figuras 1 y 2:

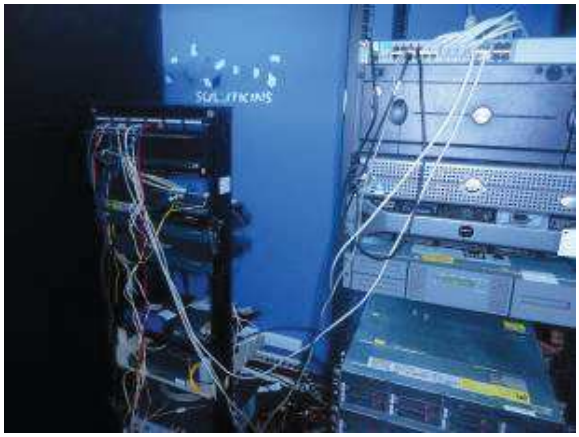


Figura 1 *Data center* actual

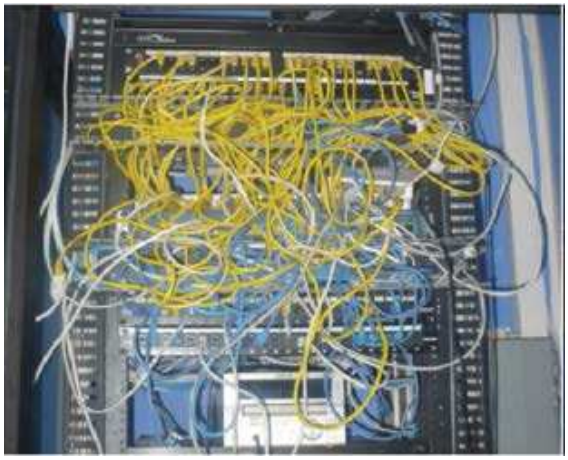


Figura 2 *Data center*, desorden de cableado en el *patch panel*

1.2 Estructura de la red

La topología de red se define como la forma en que está diseñada una red, sea esto en el aspecto físico o lógico. Con respecto a la topología física, la cual se define como la disposición real de los cables o medios de transmisión, los

cuales están conectados entre sí mediante líneas de comunicación (cables de red, etc.) y elementos de *hardware* (adaptadores de red y otros equipos que garantizan que los datos viajen correctamente).

La topología física en Akros cuenta con una topología de estrella extendida, la cual es creada al conectar desde un nodo central, uno o varios *switches,* los mismos que poseen una sub conexión hacia un *host.*

A continuación se muestra una breve reseña de esta topología:

Ventajas de la topología estrella extendida:

- El cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central.
- Si un *host* falla, solamente ese equipo queda fuera de servicio, ya que no afecta al funcionamiento del resto de la red.
- Permite agregar un *host* de manera muy rápida.
- Permite realizar cualquier reconfiguración de una manera rápida y eficiente.

Desventajas de la topología estrella extendida:

- El cable viaja por separado desde el nodo central hacia cada *host.*
- Si el nodo central deja de funcionar, ninguna de los *host* tendrá conexión a la red.
- El número de *host* conectados a la red depende de las limitaciones del *switch*.

La otra parte está compuesta por la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos. Generalmente, todas las topologías lógicas se basan en necesidades específicas y exclusivas para obtener recursos basados en los requisitos de seguridad. La topología lógica de Akros funciona mediante la topología de *broadcast***,** que significa que cada *host* envía sus datos hacia todos los demás *host* de la red. Un ejemplo claro de topología lógica, es la segmentación de *broadcast* por VLAN's, en donde se divide por segmentos lógicos la red de Akros, de tal modo que se asignan puertos específicos en cada *switch*, para la separación de la información por equipos, también se colocan los nombres de las VLAN y sus direcciones IP con

las máscaras de red correspondientes. A continuación, la figura 3 muestra como la topología de estrella extendida está diseñada, señalando a su vez las VLAN´s configuradas, con su respectiva interconexión (tabla 2).

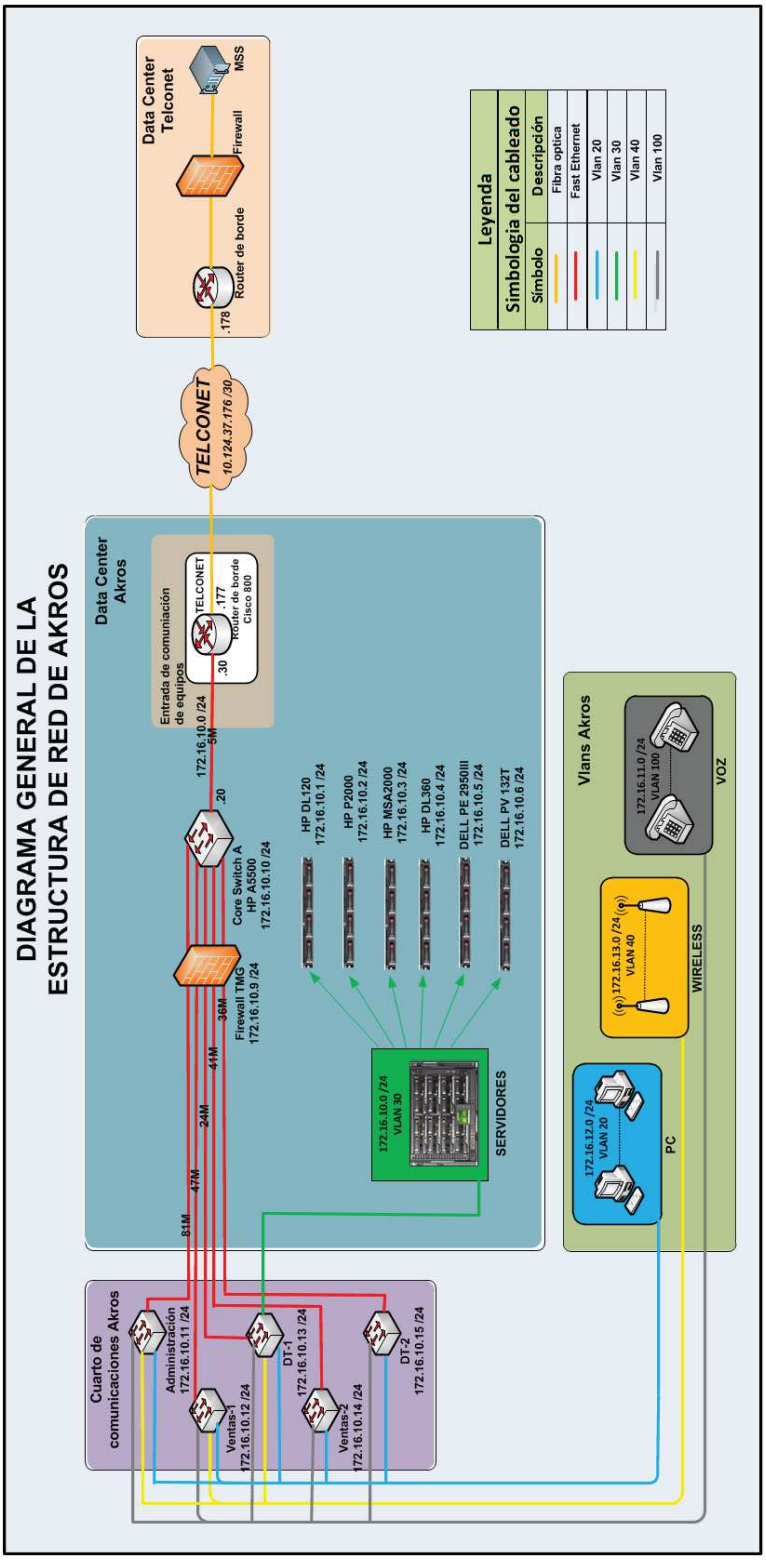


Figura 3 Topología física, lógica de red

Tabla 2 Interconexión de puertos en los *switches*

NOMBRE EQUIPO LOCAL	PUERTO LOCAL	NOMBRE EQUIPO REMOTO	PUERTO REMOTO
COMPULABPA	47	ADMINISTRACIÓN	28
COMPULABPA	48	DT-1	48
DT-1	2	DT-2	1
DT-1	48	COMPULABPA	48
ADMINISTRACION	27	VENTAS-1	46
VENTAS-1	45	VENTAS-2	49
VENTAS-1	46	ADMINISTRACIÓN	27
VENTAS-2	49	VENTAS-1	45
DT-2	8	ADMINISTRACIÓN	10
DT-2	1	DT-1	2

1.3 Protocolos de enrutamiento

1.3.1 IGP (*internal gateway Protocol*)

El objetivo de un protocolo IGP es establecer un conjunto de las mejores rutas en cada *router* de destino y al mismo tiempo se encarga de enviar paquetes entre los *routers* del mismo sistema autónomo (AS). Debido a que los dominios de *broadcast* operan bajo el mismo sistema autónomo (grupo de redes IP que poseen una política de rutas propia e independiente) se suelen aplicar generalmente las siguientes hipótesis:

- Los dominios de *broadcast* son por lo general lo suficientemente pequeños para que la información de estado acerca de los enlaces de red, pueda ser difundida.
- Los dominios de *broadcast* tienen la noción de menor número de saltos o de más bajo costo.

En el caso particular de la red de Akros, no se maneja un protocolo IGP directamente, ya que la configuración del *router* Cisco 800 lo opera solamente el proveedor de servicios Telconet mediante rutas estáticas.

1.3.2 EGP (*exterior gateway protocol*)

Por otra parte, en un protocolo EGP el enrutamiento se lo realiza a nivel inter-dominio, esto quiere decir intercambiando información de enrutamiento entre varios AS. Una vez que el paquete se reenvía a un AS diferente, ese AS tiene el control total sobre la ruta y su trayectoria futura. Cuando está disponible más de una ruta a un destino, la elección de la mejor ruta depende de la configuración del *router* local.

En EGP si un enlace de un *router* se vuelve inaccesible, los *routers* vecinos no se dan cuenta inmediatamente, por lo que se corre el riesgo de que el *router* crea que puede llegar a la red perdida a través de sus vecinos los cuales mantienen entradas antiguas. Así el *router*, añade una nueva entrada a su tabla de enrutamiento con un costo superior. A su vez, este proceso se repetirá una y otra vez, incrementándose el costo de las rutas, hasta que de alguna forma se detenga dicho proceso. La figura 4 muestra donde se sitúan IGP e EGP en una red:

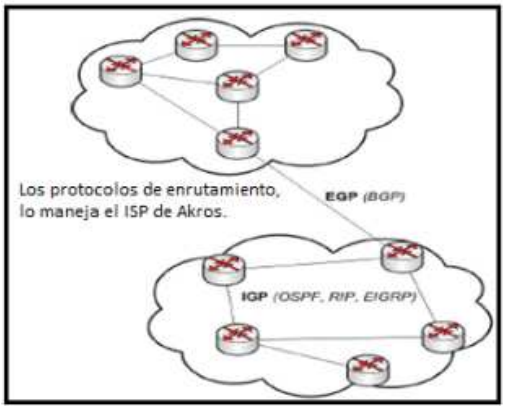


Figura 4 Protocolos IGP y EGP

El manejo y configuración del protocolo EGP, lo realiza estrictamente el proveedor Telconet, por lo que Akros no posee acceso al mismo.

1.3.2.1 BGP Concepto, funcionamiento y características

Un protocolo EGP muy utilizado es BGP (*border gateway protocol*), el cual realiza enrutamiento interdominio entre diferentes redes. Este

protocolo se diseñó para permitir la colaboración en el intercambio de información de enrutamiento entre *routers* que poseen distintos AS. Por ejemplo, los ISP registrados en Internet constan de varios AS y para este caso es necesario un protocolo como BGP. Entre los AS de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de enrutamiento se hace entre los routers externos de cada AS. BGP posee varias características tales como:

- La conexión se mantiene por *keepalives* periódicos, en donde un *keepalive* mantiene al paquete TCP activo.
- Permite un diseño escalable de la red.
- Es posible manipular las métricas, es decir que una ruta no puede enviar tráfico si el siguiente salto no desea.
- BGP no comunica el conocimiento de cada subred, solo le interesa utilizar la información para encontrar el AS.
- BGP asegura temas como la fiabilidad y el trasporte, llevando sus actualizaciones de ruteo y sincronizando todas las actualizaciones.

- **AS (*autonomous system*)**

Se define como un grupo de redes IP que poseen una política de rutas propia e independiente. BGP trabaja en conjunto con un AS el cual tiene asignado un número decimal de identificación que lo diferencia en el internet, estos números son asignados por la Lacnic (registros de direcciones de internet para Latinoamérica y el Caribe).

- **Enrutamiento entre AS**

BGP construye un gráfico de AS basados en la información intercambiada entre los *routers* BGP. Este entorno gráfico se lo conoce en ocasiones como árbol. En lo que concierne a BGP, Internet es un gráfico de AS, en donde las conexiones entre dos AS juntos forman una ruta de acceso, y el conjunto de información de rutas de acceso forma un camino para llegar a un destino

específico. BGP utiliza la información de ruta de acceso asociada con un destino dado para asegurar el enrutamiento entre los dominios. En terminología de BGP los *routers* se denominan *gateway*, y realizan tres procesos funcionales:

- La "adquisición de vecinos", implica que dos dispositivos de enrutamiento que conllevan la misma subred física, pero que pertenecen a distintos sistemas autónomos, deciden intercambiar regularmente información. En este procedimiento, un dispositivo hace una oferta a otro mediante un mensaje "*open*", el cual puede ser aceptado o rechazado mediante un mensaje "*Keepalive*".
- Una vez hecha la relación de "vecindad", se utiliza el procedimiento de "detección de vecino alcanzable" para mantenerla. Cada *gateway* necesita estar seguro de que su pareja existe y está todavía activa. Para este propósito, periódicamente ambos dispositivos de enrutamiento se envían mensajes "*keepalive*".
- El último procedimiento es la "detección de redes alcanzables", en donde cada *gateway* mantiene una base de datos con las subredes que puede alcanzar y la ruta completa para hacerlo. Siempre que se modifica esta base de datos, el *gateway* lo notifica a todos los demás dispositivos de enrutamiento que implementan BGP, por medio de paquetes de "actualización". De esta manera, el resto de *gateways* pueden actualizar su propia información.

- **IBGP (*internal border gateway protocol*) y EBGP (*external border gateway protocol*)**
  - IBGP se utiliza para transportar o intercambiar información de BGP a través del mismo AS. Posee una distancia administrativa (medida utilizada para seleccionar la mejor

ruta, cuando existe más de un camino) de 200 y no necesita estar directamente conectado con otro dispositivo.

- EBGP se utiliza para transportar o intercambiar información de BGP hacia un AS diferente. Posee una distancia administrativa (medida utilizada para seleccionar la mejor ruta, cuando existe más de un camino) de 20 y necesita estar directamente conectado con otro dispositivo.

- **Establecimiento de sesiones de BGP**
  - *Idle*.- El *router* está buscando en su tabla de enrutamiento si cuenta con una ruta para alcanzar a su vecino.
  - *Connect*.- El *router* encontró una ruta para alcanzar a su vecino
  - *Open sent*.- Mensaje *Open* enviado con los parámetros de la sesión respectiva.
  - *Open confirm*.- El *router* ha recibido confirmación acerca de los parámetros de la sesión que está estableciendo.
  - *Established.*- La sesión está completamente establecida, se intercambia información de enrutamiento.

- **PBR (*policy based routing*)**

Permiten al administrador programar el protocolo de ruteo, definiendo como se va a enrutar el tráfico. En otras palabras, es una forma de ruteo estático forzado por listas de acceso llamados *Route maps*. La PBR es independiente al protocolo, ya que utiliza *Route maps* creando procesos separados para forzar las decisiones de ruteo, encontrando y cambiando métricas de la mejor manera. La PBR puede estar dirigida basándose en la dirección de origen, la de destino o ambas y solamente afecta al siguiente salto. Existen algunas reglas tales como:

- La PBR no afecta al destino del paquete sino al camino empleado para su envío.

- La PBR no permite que el tráfico enviado a otro AS tome otro camino que el elegido por el AS.
- Es posible influir únicamente en cómo alcanzar al vecino, no como enrutarse por el AS.
- La PBR examina la dirección de origen.

- **BGP *Trobleshooting***

En caso de tener problemas con el enrutamiento de BGP, existen algunos comandos muy útiles para descifrar el problema tales como:

- *Show ip bgp neighbor x.x.x.x routes.* - Despliega la ruta que está dirigida hacia el filtro de entrada.
- *Show ip bgp neighbor x.x.x.x received-routes.* - Despliega todas las rutas recibidas, incluso las que están siendo negadas.
- *Clear ip bgp x.x.x.x in.* - Pide a la red x.x.x.x reenviar sus actualizaciones de entrada.
- *Clear ip bgp x.x.x.x out.* - Le pide a BGP que reenvíe sus actualizaciones de salida.
- *Debug ip bgp update.*- Despliega información acerca del procesamiento de BGP.
- *Debug ip bgp x.x.x.x update.*- Permite depurar las actualizaciones desde/hacia una IP especifica.

- **Atributos y comandos de BGP**

BGP también maneja sus propios atributos, los cuales ayudan a la elección de la mejor ruta hacia su destino. Los atributos de BGP son:

- *Origin.*- Indica el AS de origen.
- *AS_Path.*- Lista todos los AS que la ruta tiene que atravesar.
- *Next_Hop.*- Indica la IP del siguiente salto para un prefijo predeterminado.
- *Local_Preference.*- Utilizada por los vecinos IBGP para calcular el grado de preferencia de cada ruta externa.

- *Atomic Aggregator.-* Realiza agregación de rutas en redes que no son idénticas, pero tienen el mismo destino.
- *Aggregator.-* Brinda información de donde se realizó la agregación de una ruta, incluyendo su AS y dirección IP.
- *Community.-* Es una etiqueta que se añade a una red que comparten la misma propiedad.
- *Cluster_List.-* Previene bucles dentro del mismo AS.
- *MED.-* Indica al vecino EBGP el camino preferido para entrar en el AS.
- *Weight.-* Se utiliza como primer criterio para escoger la mejor ruta cuando se tienen varias rutas hacia el mismo destino.

La figura 5 muestra como cada AS se interconecta entre sí, utilizando IBGP y EBGP:

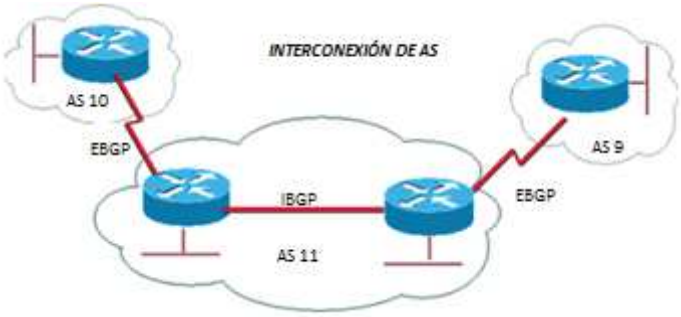


Figura 5 Interconexión de AS utilizando IBGP y EBGP

1.3.3 Ancho de banda y capacidad del canal actual

El ancho de banda es una medida de recursos disponibles para trasportar datos de una forma segura. Muchas de las veces el ancho de banda se confunde con la capacidad del canal, que es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período dado.

Existen varios factores para dimensionar el uso de la capacidad del canal que la empresa requiere, y para esto es necesario conocer primeramente los servicios que dicha red transporta:

- Voz (códec G.729)
- FTP
- Correo electrónico
- Base de datos

- Chat
- DHCP
- Datos
- Telnet
- Video (códec H.264)
- Impresión
- Acceso remoto

Muchos factores antes ya mencionados como el número de conexiones VoIP que se utilizan a la vez, el número de correos que se envían y reciben en un tiempo determinado, descarga de *drivers*, conferencias de video, etc, podrían inflar las necesidades de la capacidad del canal. Problemas relacionados con los picos de uso de la capacidad del canal son frecuentes en entornos de oficina, donde el uso máximo puede darse durante medio día y un uso moderado en horas de la mañana y/o la tarde. Existen también retardos y latencia que se generan debido a la distancia del servidor al que se desea llegar, o también por el tipo de medio de transmisión. Situaciones de la vida real varían de un usuario a otro, por lo que no existe una generalidad predeterminada para la utilización de la capacidad del canal. Adicionalmente no hay que olvidar que la velocidad de transmisión se mide en bits por segundo, y los archivos y documentos descargados desde la web están en bytes, por lo que para hacer la conversión se debe divide los bits por segundo para 8.

Una estimación precisa del uso de la capacidad del canal para los usuarios es difícil de obtener, pero cada vez se hace más necesaria. Es por eso que en este análisis de consumo de capacidad de canal se recomendará un incremento del mismo, basado en una estimación del consumo que genera cada empleado en cada una de las áreas.

Por ejemplo, actualmente existen 4 Vlan’s creadas en la red, las mismas que tienen asignadas una determinada capacidad de transmisión. La capacidad del canal con la que se cuenta actualmente es de 4 Mbps simétrico y se encuentra distribuida tal como indica la siguiente figura 6:

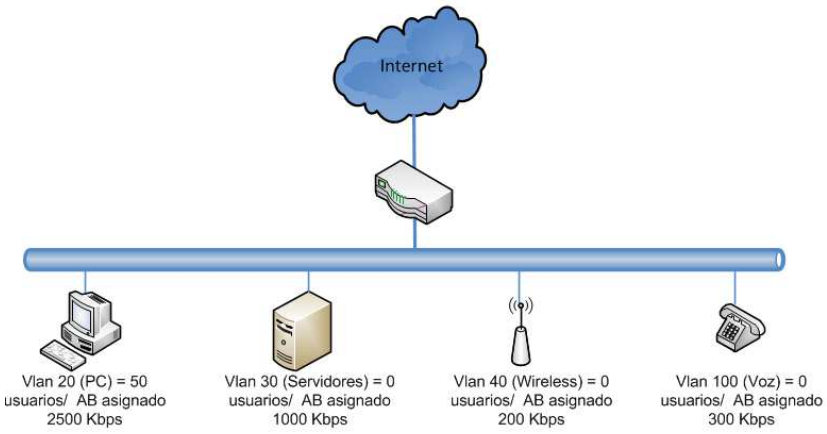


Figura 6 Gestión de la capacidad de canal actual

En donde:

- Dentro de la VLAN 20 se encuentran todas las áreas de la empresa, las cuales cuentan con 50 computadores que hacen uso de la capacidad total del canal. Estos 50 computadores se los han clasificado en tres categorías, los mismos que están basados en promedios de consumo de capacidad del canal que el departamento de TI ha obtenido.

  - Consumo bajo = 20 computadores x 40 (Kbps promedio utilizados) = 800 Kbps
  - Consumo medio = 25 computadores x 70 (Kbps promedio utilizados) = 1750 Kbps
  - Consumo alto = 5 computadores x 110 (Kbps promedio utilizados) = 550 Kbps

  En donde se tiene:

  800 + 1750 + 550 Kbps = 3.1 Mbps (Capacidad del canal utilizado)

  Lo que significa que los 50 computadores al hacer uso de internet a la vez (muy poco probable), sobrepasan la capacidad del canal ya asignada (2.5 Mbps), y esto se ve reflejado al momento de navegar en horas pico, ya que aquí se puede experimentar lentitud para el despliegue de páginas *web*, demora en las descargas, interrupción en las llamadas VoIP, *streaming* de video entrecortado, etc.

- Dentro de la VLAN 30 se encuentran todos los servidores y *switches*. Esta VLAN tiene asignado (1 Mbps) de capacidad de canal, basado en un promedio de consumo de cada equipo de 100 Kbps aproximadamente, dato obtenido por el departamento de TI.
- La VLAN 40 está designada para los *access points* que controlan y distribuyen la señal inalámbrica en las distintas áreas de la empresa. Esta VLAN tiene asignado una capacidad de canal de (200 Kbps), basado en un consumo por *access point* de 40 Kbps. Este dato fue proporcionado por el TI.
- Finalmente la VLAN 100 está destinada para la comunicación telefónica sobre IP, o mejor conocida como VOIP. Esta VLAN tiene asignada una capacidad de canal de (300 Kbps), que está basada en un promedio real de 7 llamadas simultáneas, con un consumo de 40 Kbps por llamada, utilizando para ello el códec G.729. Estos datos fueron proporcionados por el departamento de TI.

3.1Mbps+ 1Mbps+ 200Kbps+ 300Kbps= 4600Kbps(consumo actual)

Por otro lado, no solo la capacidad del canal es importante, sino también el *throughput,* que es el volumen de información que fluye a través de la red. En otras palabras, es la medida del número de mensajes que un sistema puede procesar en una cantidad de tiempo dada.

Por ejemplo, Akros cuenta con una capacidad de canal de 4 Mbps simétrico que llega a través de fibra óptica, en donde a manera de ejemplo se realiza una descarga a una velocidad de 469 KB/sec en un periodo de tiempo (ver figura 7), lo que resulta en un *throughput* de:

THROUGHPUT = 469 KB/sec x 8= 3752 Kbps

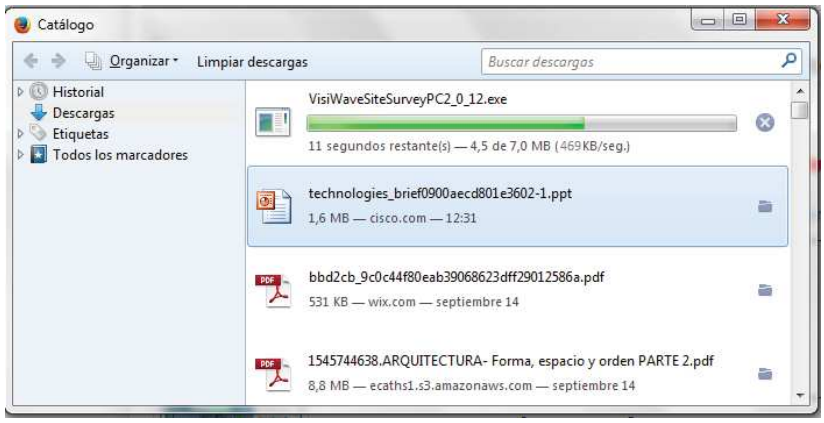


Figura 7 Velocidad de bajada de la red

El *throughput* jamás será mayor a la capacidad del canal, pero casi siempre estará cerca de serlo (3752 Kbps), debido a que existen variables tales como el número usuarios que utilicen la red en ese momento y la distancia del servidor del cual se realiza la descarga, latencia, etc).

Es por eso que en el capítulo 2 se dará una solución a la falta de capacidad de canal, proponiendo un incremento del mismo, ya que de esta manera se podrá obtener un mejor *throughput* en la red lo que significa mayor velocidad al momento de descargar archivos, abrir páginas web, subir información, etc, que finalmente se traduce en eficiencia de trabajo que cada usuario puede llegar a obtener.

1.3.4 VLAN´s

Una VLAN o Virtual Lan es una subred IP separada de manera lógica. Las VLAN´s permiten que redes IP y subredes múltiples existan en la misma red. Son útiles para reducir el tamaño de las tramas de *broadcast* ya que estas solo llegarán a la VLAN seleccionada, mas no a todos los puertos de un *switch*. También ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos para una empresa, oficina, universidades, etc.) que no deberían intercambiar datos usando la red local. Cada *host* debe pertenecer a una VLAN y debe tener una dirección IP y una máscara de

subred correspondiente a dicha subred. No es obligatorio el uso de VLAN en las redes, pero existen ventajas reales para utilizarlas como:

- Seguridad.
- Reducción de costo.
- Mejor rendimiento.
- Reducción de los tamaños de las tramas de *broadcast.*
- Mejora la administración de la red.

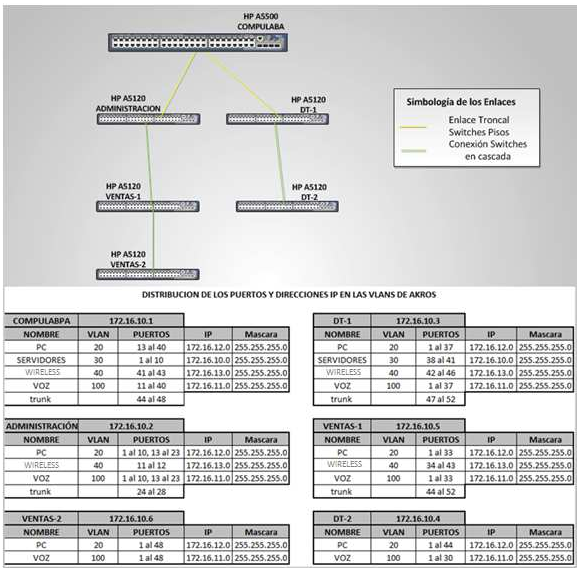
De acuerdo con la terminología común de las VLAN se clasifican en:

- **VLAN de datos.-** Es aquella que está configurada solamente para enviar tráfico de datos generado por un usuario. A una VLAN de datos también se la conoce como VLAN de usuario.

- **VLAN nativa.-** Una VLAN nativa por *default* está asignada a un puerto troncal 802.1Q, el cual admite el tráfico entrante de una VLAN y también el saliente de las mismas. La VLAN nativa sirve también como un identificador común en los extremos opuestos de un enlace troncal. Es aconsejable no utilizar la VLAN 1 como la VLAN nativa.

- **VLAN de administración.-** Es cualquier VLAN que el administrador configura para acceder a la administración de un *switch.* Comúnmente la VLAN1 es utilizada como VLAN de administración siempre y cuando no se defina otra VLAN para dicha función.

En la siguiente figura 8 se visualiza las VLAN´s existentes en Akros con los respectivos puertos que las interconectan.



DISTRIBUCION DE LOS PUERTOS Y DIRECCIONES IP EN LAS VLANS DE AKROS

COMPULABPA	172.16.10.1			
NOMBRE	VLAN	PUERTOS	IP	Mascara
PC	20	13 al 40	172.16.12.0	255.255.255.0
SERVIDORES	30	1 al 10	172.16.10.0	255.255.255.0
WIRELESS	40	41 al 43	172.16.13.0	255.255.255.0
VOZ	100	11 al 40	172.16.11.0	255.255.255.0
trunk		44 al 48		

ADMINISTRACIÓN	172.16.10.2			
NOMBRE	VLAN	PUERTOS	IP	Mascara
PC	20	1 al 10, 13 al 23	172.16.12.0	255.255.255.0
WIRELESS	40	11 al 12	172.16.13.0	255.255.255.0
VOZ	100	1 al 10, 13 al 23	172.16.11.0	255.255.255.0
trunk		24 al 28		

VENTAS-2	172.16.10.6			
NOMBRE	VLAN	PUERTOS	IP	Mascara
PC	20	1 al 48	172.16.12.0	255.255.255.0
VOZ	100	1 al 48	172.16.11.0	255.255.255.0

DT-1	172.16.10.3			
NOMBRE	VLAN	PUERTOS	IP	Mascara
PC	20	1 al 37	172.16.12.0	255.255.255.0
SERVIDORES	30	38 al 41	172.16.10.0	255.255.255.0
WIRELESS	40	42 al 46	172.16.13.0	255.255.255.0
VOZ	100	1 al 37	172.16.11.0	255.255.255.0
trunk		47 al 52		

VENTAS-1	172.16.10.5			
NOMBRE	VLAN	PUERTOS	IP	Mascara
PC	20	1 al 33	172.16.12.0	255.255.255.0
WIRELESS	40	34 al 43	172.16.13.0	255.255.255.0
VOZ	100	1 al 33	172.16.11.0	255.255.255.0
trunk		44 al 52		

DT-2	172.16.10.4			
NOMBRE	VLAN	PUERTOS	IP	Mascara
PC	20	1 al 44	172.16.12.0	255.255.255.0
VOZ	100	1 al 30	172.16.11.0	255.255.255.0

Figura 8 Distribución de VLAN´s

Una buena distribución de VLAN´s muchas de las veces necesita la segmentación por áreas de trabajo en una compañía, por lo que una mejor distribución de las mismas se la realizará en el punto 2.3.4 del capítulo dos.

1.3.5 Virtualización

La virtualización es una técnica utilizada sobre las características físicas de algunos atributos computacionales, para esconderlos de otros sistemas, aplicaciones o usuarios que interactúen con ellos. Esto conlleva a hacer que un recurso físico, tal como un servidor, un sistema operativo (SO) o un dispositivo de almacenamiento, aparezca como si fuera varios recursos lógicos a la vez, o que varios recursos físicos, como servidores o dispositivos de almacenamiento, aparezcan como un único recurso lógico. Por ejemplo, la virtualización de un SO es el uso de una aplicación de software para permitir que un mismo SO maneje varias imágenes de los SO al mismo tiempo.

Esta tecnología permite la separación del *hardware* y el *software*, lo cual posibilita a su vez que múltiples SO, aplicaciones o plataformas de cómputo se ejecuten simultáneamente en un solo servidor o host según sea el caso de aplicación que se necesite. Hay varias formas de

distinguir o catalogar la virtualización, pero en general se trata de uno de los dos siguientes casos:

1.3.5.1 Virtualización de plataforma

Trata de simular una máquina real (servidor o *host*) con todos sus componentes, los cuales no necesariamente son todos los de la máquina física y prestarle todos los recursos necesarios para su funcionamiento. En general, hay un *software* propietario que es el que controla que las diferentes máquinas virtuales sean atendidas correctamente y que está ubicado entre el *hardware* y las máquinas virtuales. Dentro de este esquema caben la mayoría de las formas de virtualización más conocidas, tales como:

- **Virtualización de SO.-** Permiten contener dentro de una misma maquina física varios SO ejecutándose a la vez sin problemas (XP, 7, server, Ubuntu, Centos, Fedora, etc). Existen varias herramientas de virtualización que permiten realizar esto, tales como: (Vmware, Virtualbox, QUEMU, etc).

- **Virtualización de aplicaciones.-** Convierte las aplicaciones en servicios virtualizados con administración centralizada. Igualmente acelera la implementación de las aplicaciones y del SO, así como también reduce el impacto en el usuario relacionado con actualizaciones y/o instalaciones de parches en las aplicaciones.

1.3.5.2 Virtualización de recursos

Este método permite agrupar varios dispositivos para que sean vistos como uno solo, o al revés, dividir un recurso en múltiples recursos independientes. Habitualmente se aplica a medios de almacenamiento. Existen varios recursos que pueden ser virtualizados tales como:

- **Discos RAID (*redundant array of independent disks*). -** Es un sistema de almacenamiento que usan múltiples discos duros entre los que distribuyen o replican los datos.

- **SAN (*storage area network*).-** Es una red concebida para conectar servidores, matrices (*arrays*) de discos y librerías de respaldo. Su función es la de conectar de manera rápida, segura y confiable los distintos elementos que la conforman.

- **VPN (*virtual private network*).-** Este método permite a un *host* conectarse a una red corporativa a través del Internet como si estuviera en la misma sede física de la compañía.

Así mismo, la virtualización consta de varios procesos que debe seguir para que la misma funcione eficientemente. A continuación se explicará de mejor forma que hace cada uno de estos procesos en una red:

Particionado.- Ejecuta varias máquinas virtuales simultáneamente en un solo servidor físico.
Aislamiento.- Cada máquina virtual se encuentra aislada de las demás máquinas virtuales del mismo servidor.

Encapsulamiento.- Las máquinas virtuales expulsan sistemas enteros (SO, aplicaciones, configuraciones) en archivos.

Independencia del hardware.- Se puede ejecutar una máquina virtual en cualquier servidor sin ninguna modificación.

La utilización de la virtualización posee beneficios tales como:

- **Ahorro de costes**.- Es una de las razones por las cuales las empresas se interesan en la virtualización, ya que permite realizar un ahorro en la utilización de equipos**.** Además permite ahorrar mucho tiempo gracias a la facilidad de administración y clonación

de los discos duros virtuales, que se realizarán como cualquier otro archivo.

- **Entornos de prueba**.- Se puede realizar una virtualización de todo un sistema sin problemas. Se puede efectuar todas estas instalaciones en el sistema virtual y dejar el sistema anfitrión sin rastros, instalando sólo aquello que se va a utilizar.

- **Entornos aislados de seguridad**.- Toda comunicación de red se realizará de manera segura. Por ejemplo, con el programa "*kaspersky security for virtualisation*", se puede explorar cada máquina virtualizada en la red de una empresa para de esta forma protegerla contra infecciones potenciales.

- **Compatibilidad de programas**.- Con la utilización del sistema operativo Linux o Mac a veces no es posible encontrar el programa que se necesita para estas plataformas, por lo que se puede instalar el SO Windows o se busca otra alternativa. Este tipo de sucesos cada vez son menos comunes, pero continúan pasando, con lo cual tener virtualizado Windows dentro de Mac o Linux puede ahorrar una buena cantidad de problemas y tiempo buscando el equivalente de un programa para estos sistemas.

Akros posee varios de sus servicios virtualizados tales como: correo, ERP, dominio, *file server*, etc, utilizando para esto el *software* VMware, los cuales están siendo ejecutados dentro de servidores físicos. El problema recae en la falta de capacidad de almacenamiento que brindan los actuales equipos, ya que por ejemplo, al utilizar arreglos de disco de tipo raid 5, en promedio se pierde hasta un 30% de la capacidad total, debido al cálculo de información de paridad y su almacenamiento alternativo por bloques en todos los discos del conjunto.

Adicional a esto, en el capítulo dos se planteará una solución a la futura falta de capacidad física en el data center, mediante la utilización de un

método llamado *cloud computing*, que es la “tendencia a basar las aplicaciones en servicios alojados de forma externa” y la adquisición de nuevos equipos para poder de esta manera incrementar la capacidad de almacenamiento así como de procesamiento.

1.3.6 Seguridad de la red (firewall)

Un *firewall* es un sistema que se utiliza para bloquear o permitir la información que proviene de internet hacia la LAN. En otras palabras, es simplemente un filtro que inspecciona todas las comunicaciones que pasan de una red a otra, basándose en un conjunto de normas y reglas preestablecidas.

En el caso de la red de Akros, el *firewall* que se utiliza es un Microsoft *forefront* TMG (*threat management gateway*) 2010, el cual está encargado de bloquear el tráfico no autorizado hacia la LAN, bloquear páginas web no autorizadas, traducción de direcciones IP NAT (*network address translation*). Adicionalmente esta plataforma incluye un anti-malware (antivirus y antispam) llamado Microsoft *endpoint protection* 2010, el cual se encarga del análisis de toda información y archivos que cursa la red.

La protección del *firewall* en la red de Akros, ha logrado mantener una buena seguridad contra los ataques cibernéticos y amenazas de virus tanto externos como internos, sin embargo esto se podría mejorar aún más, para lo cual en el punto 2.5 del capítulo 2, se propondrán el uso de mejores prácticas para la seguridad de la red de Akros dentro del firewall TMG que actualmente está en funcionamiento.

1.3.7 WLAN

La WLAN (*wireless* lan) es un medio inalámbrico para la comunicación, muy utilizado como alternativa a las LAN cableadas. Usan tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN utilizan estándares

IEEE tales como los 802.11a, 802.11b y 802.11g los cuales emplean las bandas que varían entre los 2,4GHz a los 5 GHz.

Se definieron para equipos WiFi 11 canales, los cuales pueden ser configurados de acuerdo a necesidades particulares. A pesar de esto, los 11 canales no son completamente independientes y en la práctica lo más recomendable es utilizar simultáneamente 3 canales que son 1, 6, 11. Esto se debe a que existe una separación de 5 Mhz entre estos canales y por ende existe menos posibilidad de interferir con el canal vecino, tal como se puede apreciar en la figura 9:

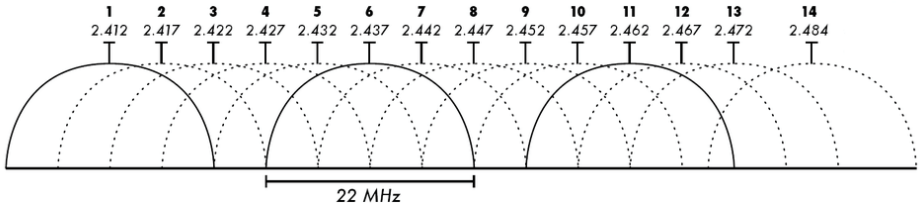


Figura 9 Superposición de canales

Tomado de: http://www.google.com.ec/im gres?imgurl=&img refur l=http %3A%2F%2Fwww.zero13wireless.net%2Fforo%2Fshowthread.php

Las WLAN poseen equipos llamados AP (access point), los cuales poseen 3 modos:

- **Modo *root*.-** Es el modo más común en donde múltiples usuarios acceden al AP al mismo tiempo. Aquí los usuarios con portátiles, *smartphones*, etc pueden acceder a internet a través de un solo AP compartiendo la conexión.

- **Modo repetidor**.- Se utiliza cuando se quiere extender la señal más allá de los límites actuales. Se necesita colocar al AP en modo repetidor dentro del área de un AP en modo *root*. Con esto la señal del AP *root* se extenderá con igual fuerza por medio de este AP repetidor mejorando el alcance.

- **Modo bridge.**- Aquí se puede crear un puente inalámbrico entre dispositivos. Dos AP en modo *bridge* solo hablarán entre ellos. Este tipo de conexión es útil cuando se interconecta dos edificios o localizaciones separadas donde instalar cableado no resulta fácil o económicamente viable.

Akros cuenta con cinco *access points* D-Link DAP 2555 distribuidos en la empresa, los mismos que serán analizados mediante un *software* de medición de cobertura de señal llamado VisiWave *site survey*. A continuación se encuentra una descripción del funcionamiento de VisiWave así como también de sus características.

1.3.7.1 Análisis actual de la WLAN empleando VisiWave

VisiWave es un *software* que recoge información detallada sobre la red y las redes vecinas y luego visualiza los datos. Cada vista está diseñada para revelar detalles importantes acerca de la red de una forma intuitiva e informativa. Esta es una herramienta eficaz para la realización de encuestas dentro de los edificios, fuera de los campus, puntos de acceso en toda la ciudad, ya desplegadas redes inalámbricas, o de los sitios pre-despliegue. Con VisiWave, se podrá realizar varias tareas tales como:

- Revelar los vacíos de cobertura.
- Revelar cualquier fuga de señal del edificio.
- Descubrir la existencia y ubicación de los puntos de acceso no autorizados.
- Visualizar superposición de cobertura del punto de acceso.

Para la realización de la toma de datos desde los AP's D-Link, existen pasos a seguir tales como la carga los mapas en VisiWave, colocación de los AP's correspondientes y finalmente la creación de reportes.

Como primer paso se procede a añadir el mapa prediseñado como se muestra en la figura 10:

Figura 10 Anadir mapas pre diseñados

Posteriormente se procede a añadir los AP's correspondientes a este mapa con la opción AP *Marker*. Una vez seleccionado el AP correspondiente, VisiWave asociará las características actuales de la señal inalámbrica con la ubicación que se ha dado en el mapa, tal como lo muestra en la figura 11:

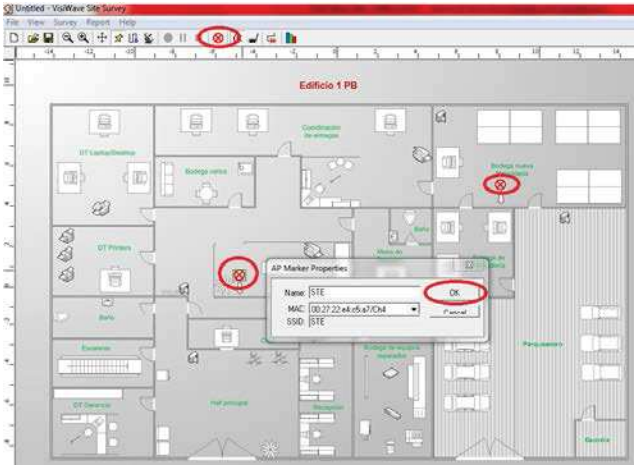


Figura 11 Selección de AP's dentro del mapa

Una vez posicionados los AP's en sus lugares correspondientes, se procede a dar click en el icono de vista de reporte figura 12, en donde se obtienen una variedad de reportes que podrían generarse dando click en la opción *add to report*. Finalmente una vez añadidos todos los reportes que se desee, se procede a dar

click en la opción *generate report* (figura 13), el cual creará un reporte .pdf donde se incluyan la cobertura señal, de canal y la velocidad de información.

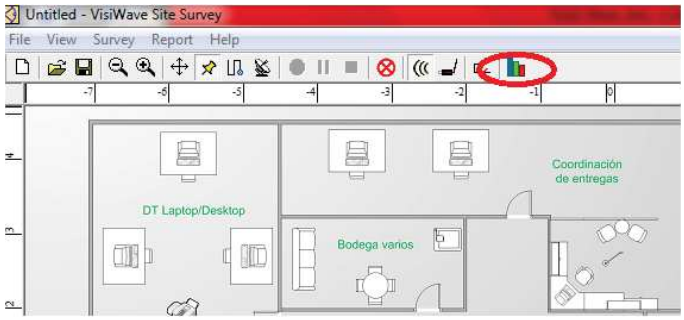


Figura 12 Vista reporte

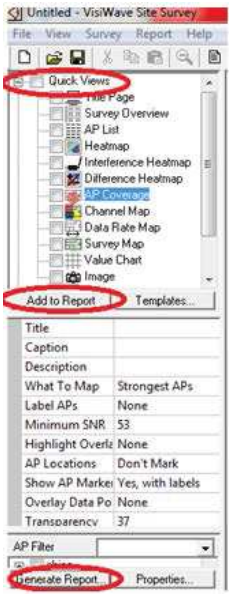


Figura 13 Lista de reportes

Como parte de este estudio de implementación de recolección de información de la red inalámbrica en Akros, se han diseñado los mapas basados en la escala real de los mismos, utilizando el programa Microsoft Visio de las áreas de ambos edificios de la empresa Akros y se ha colocado los AP´s en las ubicaciones reales, de este modo se demostrará donde la señal tiene cobertura.

El proceso de recolección de datos inalámbricos en Akros, se ha simplificado mediante el uso de una portátil que tiene instalado el *software* de demostración VisiWave, un adaptador de red inalámbrico estándar (tarjeta wireless), y una imagen pre diseñada de cada área analizada. A continuación, de cada una de las 4 áreas principales analizadas que posee Akros (ED1 PB, ED1 P2, ED2 PB, ED2 P8), se mostrará la vista general, el mapa de cobertura de señal y el mapa de cobertura de canal de cada AP, los cuales permitirán visualizar de mejor manera como las señales de los AP's están distribuidas dentro del área seleccionada:

- ***ED 1 PB***

Aquí se puede encontrar datos tales como la cantidad de AP's descubiertos, la velocidad de transmisión que poseen ambos AP's, el porcentaje de mapa cubierto por los AP's, etc.

Survey Information	
Number of Wi-Fi Data Points	4
Number of Data Points (Associated)	4
Number of Spectrum Data Points	0
Number of AP Readings Taken	4
Ave Number of APs Seen at each Point	1.0
Channels Seen (% of AP Readings)	5 (50.0%), 11 (50.0%)
Data Rates Seen (% of AP Readings)	54Mbps (50.0%), 130Mbps (50.0%)
Security Modes Seen (% of AP Readings)	WPA2 (100.0%)
Confidence Radius	5 m
Number of APs Discovered	29
Total Number of Points (Ignores AP Filter)	4
Survey Trail Length	0 m
Distance Between All Data Points	0 m
Ave Distance Between Data Points	0.00 m
Total Survey Area	109 sq m
Lat/Long of Survey Area Center	
Percentage of Survey Map Covered	95.7%

Figura 14 Vista general de los AP´s Akros_CAS y Akros_Bodega

El porcentaje de cobertura dentro del área seleccionada (figura 15), permite constatar que sitios poseen cobertura dentro del rango de los AP's y cuáles no. La figura indica que solamente en una pequeña parte del área de parqueaderos la señal es nula, por lo que la reubicación de los AP's no es necesaria.

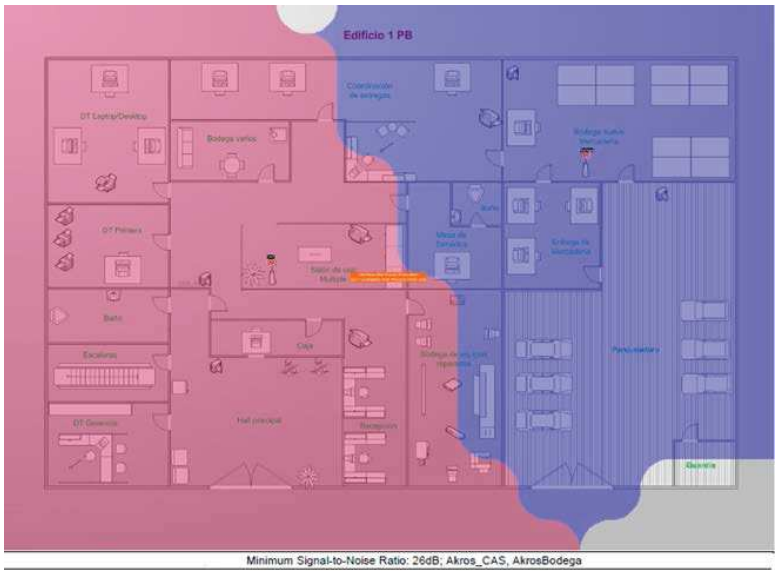


Figura 15 Áreas de cobertura de los AP´s Akros_CAS y Akros_Bodega

El canal de transmisión que utilizan ambos AP´s (figura 16), la cual permite conocer que canal se está utilizando con cada AP, para no interferir con los demás. En esta área, se muestra que ambos canales 5 y 11 están bien separados y cubren un área equitativa.

Figura 16 Mapa de canal de los AP´s Akros_CAS y Akros_Bodega

- ***ED 1 P2***

Survey Information	
Number of Wi-Fi Data Points	2
Number of Data Points (Associated)	0
Number of Spectrum Data Points	0
Number of AP Readings Taken	2
Ave Number of APs Seen at each Point	1.0
Channels Seen (% of AP Readings)	11 (100.0%)
Data Rates Seen (% of AP Readings)	54Mbps (100.0%)
Security Modes Seen (% of AP Readings)	WPA2 (100.0%)
Confidence Radius	5 m
Number of APs Discovered	12
Total Number of Points (Ignores AP Filter)	2
Survey Trail Length	0 m
Distance Between All Data Points	0 m
Ave Distance Between Data Points	0.00 m
Total Survey Area	50 sq m
Lat/Long of Survey Area Center	
Percentage of Survey Map Covered	87.5%

Figura 17 Vista general del AP Akros_Capacitación

La figura 18 indica que en las áreas de *call center* y bodega la señal no llega con fuerza, por lo que la reubicación del AP será necesaria.

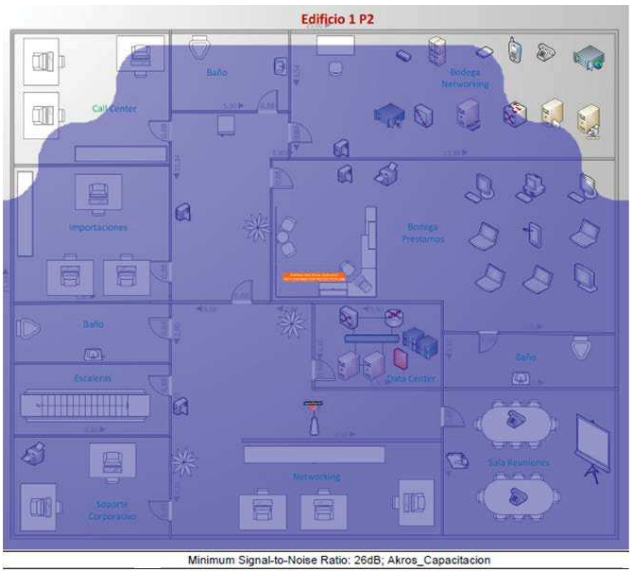


Figura 18 Mapa de cobertura del AP Akros_Capacitación

De igual manera, la figura 19 muestra que el canal 11 llega aun con menos intensidad a las áreas mencionadas anteriormente y se debe tomar la misma acción de reubicación del AP.

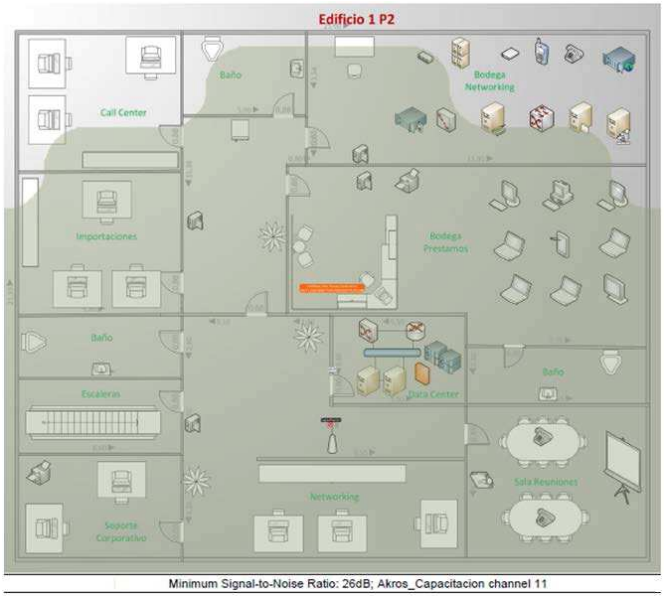


Figura 19 Mapa de canal del AP Akros_Capacitación

- **ED 2 PB**

Survey Information	
Number of Wi-Fi Data Points	2
Number of Data Points (Associated)	2
Number of Spectrum Data Points	0
Number of AP Readings Taken	2
Ave Number of APs Seen at each Point	1.0
Channels Seen (% of AP Readings)	3 (100.0%)
Data Rates Seen (% of AP Readings)	54Mbps (100.0%)
Security Modes Seen (% of AP Readings)	WPA (100.0%)
Confidence Radius	5 m
Number of APs Discovered	24
Total Number of Points (Ignores AP Filter)	2
Survey Trail Length	0 m
Distance Between All Data Points	0 m
Ave Distance Between Data Points	0.00 m
Total Survey Area	94 sq m
Lat/Long of Survey Area Center	
Percentage of Survey Map Covered	78.6%

Figura 20 Vista general del AP Akros_Ventas

La figura 21 muestra que en el área de preventa la señal no llega con gran intensidad, por lo que no solamente la reubicación del AP será necesaria, sino también la adquisición de otro nuevo AP para cubrir toda el área analizada.

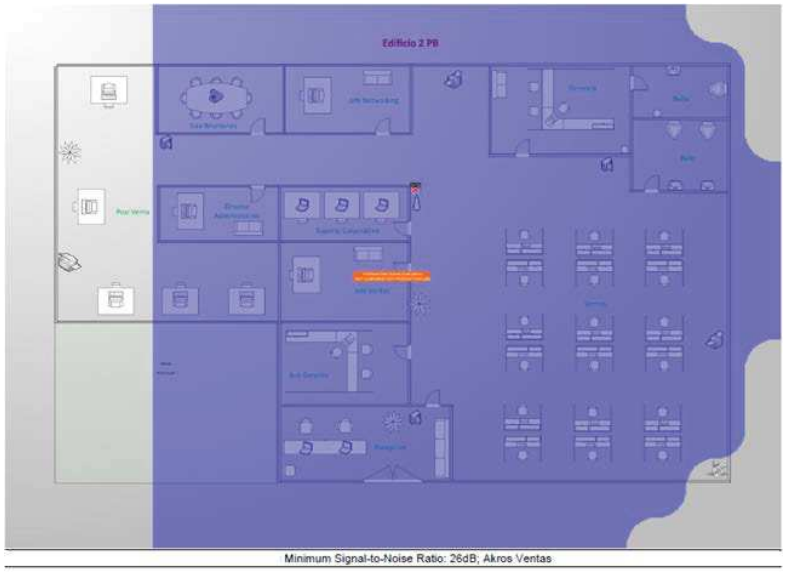


Figura 21 Mapa de cobertura del AP Akros_Ventas

De igual manera, la figura 22 muestra que el canal 3 llega aun con menos intensidad al área mencionada anteriormente y se deberá añadir otro equipo con un canal diferente para cubrir toda el área.

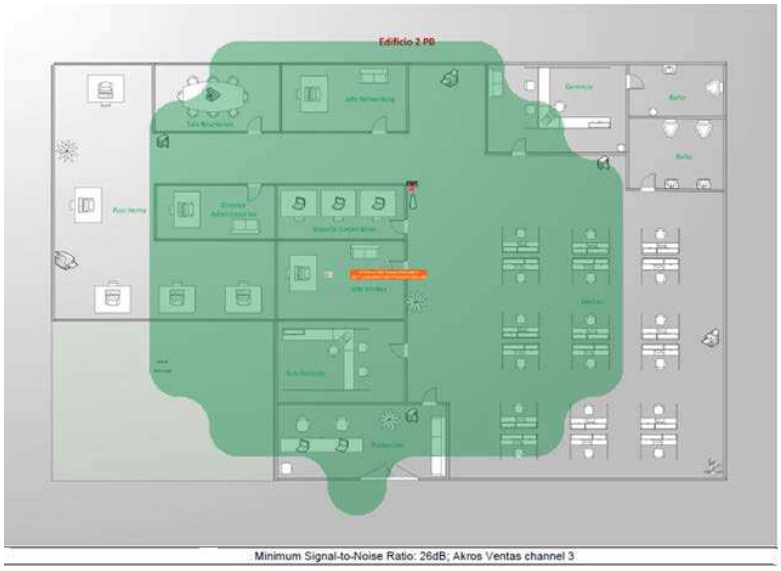


Figura 22 Mapa de canal del AP Akros_Ventas

- **ED 2 P8**

Survey Information	
Number of Wi-Fi Data Points	2
Number of Data Points (Associated)	2
Number of Spectrum Data Points	0
Number of AP Readings Taken	2
Ave Number of APs Seen at each Point	1.0
Channels Seen (% of AP Readings)	3 (100.0%)
Data Rates Seen (% of AP Readings)	54Mbps (100.0%)
Security Modes Seen (% of AP Readings)	WPA2 (100.0%)
Confidence Radius	5 m
Number of APs Discovered	31
Total Number of Points (Ignores AP Filter)	2
Survey Trail Length	0 m
Distance Between All Data Points	0 m
Ave Distance Between Data Points	0.00 m
Total Survey Area	85 sq m
Lat/Long of Survey Area Center	
Percentage of Survey Map Covered	70.7%

Figura 23 Vista general del AP WirelessRRHH

La figura 24 indica que en el área de capacitaciones la señal es muy débil, por lo que será necesario reubicar el AP actual para satisfacer el área de cobertura.

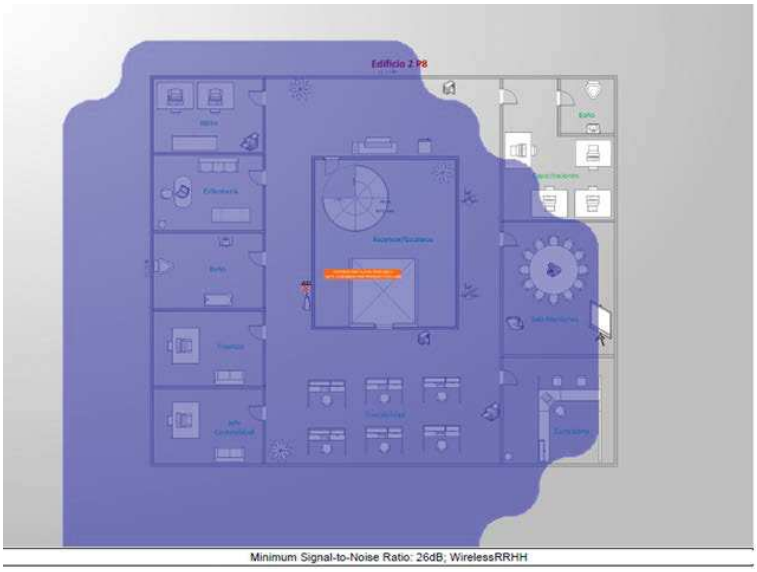


Figura 24 Mapa de cobertura del AP WirelessRRHH

De igual manera, la figura 25 muestra que el canal 3 llega aun con menos intensidad al área mencionada anteriormente por lo que se debe tomar la misma acción de reubicación del AP.

Figura 25 Mapa de canal del AP WirelessRRHH

Como se pudo constatar, existen zonas en los diferentes mapas de Akros, donde la señal inalámbrica no llega o es muy débil, y es por eso que en el capítulo dos se propondrá una reubicación de los mismos utilizando igualmente el software VisiWave para medir la cobertura. También se planteará la utilización de un wireless controller para simplificar el manejo de los AP´s y así poder ahorrar tiempo y recursos.

1.4 Elementos de red actuales

En estos momentos, la red de la empresa Akros está compuesta por equipos de red tales como:

- Un *router* Cisco 800 (propiedad de Telconet), el cual es utilizado para el enrutamiento de los paquetes entre redes independientes. Para la conexión IP con la red de Akros se utiliza un cable fast ethernet (100 Mbps) en el puerto 1 de este equipo, dejando los 3 puertos restantes libres. Este *router* permite balancear de igual forma el tráfico que se genera en la LAN hacia el proveedor de internet ISP (*internet service provider*). La siguiente figura 26 muestra el equipo:

Figura 26 *Router* Cisco 800

Tomado de : http://www.usedrouter.com/Cisco/Cisco-800-Series/Cisco-800-ISDN.html

- Un *switch* de *core* HP A5500 el cual se encarga de proveer gran velocidad hacia el backbone o puerto WAN y divide la red en pequeños dominios de colisión. Este *switch* maneja los paquetes tan rápido como sea posible ya que posee puertos *fast ethernet* (100 Mbps), que son como el cerebro de la red de Akros. Se debe tener en cuenta que este *switch* de *core* es crítico para la conectividad, y a su vez maneja un alto nivel de disponibilidad y debe adaptarse a los cambios que sufra la red de manera inmediata. La siguiente figura 27 muestra el equipo:

Figura 27 *Switch* HP A5500

Tomado de: http://es.apacelli.com/routers-and-switches-hp/hp-a5500-48g-poe-si-jd372a-/photo-1/

- Cinco *switches* de distribución HP A5120, que son utilizados para segmentar grupos de trabajo, los mismos que trabajan con puertos fast ethernet (100 Mbps). A todo esto se añade que las políticas de conectividad están configuradas en estos equipos para las diferentes áreas de la empresa. La siguiente figura 28 muestra el equipo:

Figura 28 Switch HP A5120

Tomado de: http://www.itdevices.ca/JE071A.php

- Un servidor HP proliant DL120, el cual contiene el sistema operativo *Windows server,* así como el *Firewall* y Antivirus. Aquí también se encuentra instalado el servicio de DHCP. Este protocolo se encarga de repartir direcciones dinámicas a los clientes conforme estas van quedando libres. Posee una capacidad de 1TB y 16GB de memoria RAM. La siguiente figura 29 muestra el equipo:

Figura 29 Servidor HP DL120

Tomado de: http://www.proliant.kz/shop/product_134.html

- Un *storage* HP P2000 dispositivo utilizado para el almacenaje de información. Este equipo está enfocado para clientes de nivel básico pero con una alta tecnología. Aquí se encuentra virtualizada la base de datos, el *file server*, el ERP (*enterprice resourse planning*), el CRM (*customer relationship manager*) y el GP (*Microsoft great plains*). Posee una capacidad en disco de 4TB y una memoria RAM de 8GB. Cabe recalcar que este servidor se encuentra saturado en su totalidad. La siguiente figura 30 muestra el equipo:

Figura 30 *Storage* HP P2000

Tomado de: http://www.coniston.co.uk/blog/free-server-with-a-qualifying

- Un *storage* HP MSA (*modular smart array*) 2000, el cual almacena los servicios de dominio y correo de la empresa. Posee una capacidad en disco de 4TB y una memoria RAM de 4GB. La siguiente figura 31 muestra el equipo:

Figura 31 *Storage* HP MSA2000

Tomado de: http://www.coniston.co.uk/blog/free-server-with-a-qualifying-san-in-december/

- Dos servidores HP proliant DL360 G7, los cuales combinan rendimiento, eficacia, tolerancia a fallos, todo optimizado para instalaciones con limitaciones de espacio. Dentro del primer servidor, esta virtualizado el lync communicator que es un servicio de mensajería instantánea. El segundo servidor hace de backup del lync, lo que garantiza mayor confiabilidad. Cada uno de estos equipos poseen 1 disco de 600Mb de capacidad. Cada uno de estos equipos poseen un disco de 600MB de capacidad y 8GB de memoria RAM. La siguiente figura 32 muestra el equipo:

Figura 32 Servidor HP DL360 G7

Tomado de: http://www.ultrasystem.com.py/ServidoresEstacionesTrabajo.html

- Un servidor Dell *power edge* 2950 III utilizado como servidor de *backup*, para sacar respaldos de todos los demás servidores. Este equipo se interconecta con la librería en donde se guarda toda la información. Posee un disco con una capacidad de 146GB y 8GB de memoria RAM. La siguiente figura 33 muestra el equipo:

Figura 33 Servidor Dell *power edge* 2950 III

Tomado de: http://servers.productwiki.com/dell-poweredge-2950-iii/

- Una librería Dell *powervault* 132t de 4U (unidades) utilizada para el almacenaje de información en cintas extraídas desde power edge 2950 III, la cual es fundamental ya que aquí esta guardada la información de respaldo diaria, semanal y mensual de la red de Akros. Esta librería posee una capacidad de almacenaje de 18 cintas que equivalen a 20TB. La siguiente figura 34 muestra el equipo:

Figura 34 Librería Dell *Powervault* 132t

Tomado de: http://www.9to5computer.com/dell/DELL-POWERVAULT-PV132T-LTO3-TAPE-LIBRARY.htm

- Un *blade* HP C3000, el cual es un dispositivo que permite contener hasta ocho equipos de *networking* en su interior de forma ordenada, que además brinda ahorro de energía y la disipación del calor. La siguiente figura 35 muestra el equipo:

Figura 35 *Blade* HP C3000

Tomado de: http://www.glcomp.com/hp-c3000-preconfigured-rack-model-4-power-6-fan-1-onboard-administrator-dvd-drive-8-insight-control-30-day-trial-license

- Un aire acondicionado modelo Samsung AS12UBA de 12000 BTU (*british thermal unit*) "unidad térmica con la que se miden los aires acondicionados", el cual provee enfriamiento al *data center*, con poca remoción de humedad. Actualmente Akros no cuenta con un sistema de climatización que siga ninguna norma debido a la poca cantidad de equipos existentes y al poco espacio en el *data center*. Sin embargo, en el capítulo 3 se detallaran las normas y recomendaciones de como un sistema de climatización debe interactuar con los *data centers*. La siguiente figura 36 muestra el equipo de refrigeración utilizado en Akros:

Figura 36 Aire acondicionado Samsung AS12UBA

Tomado de: http://www.samsung.com/ve/consumer/home-appliances/air-conditioners/split

- Un UPS de torre marca APC de 8KVA el cual brinda respaldo energético a los equipos que se encuentran dentro del *data center*. Cabe recalcar que este UPS no brinda el tiempo necesario para apagar todos los sistemas y su capacidad de carga esta sobresaturada. El siguiente cálculo de análisis de carga se realizó en este UPS:

  Análisis de cargas:

  - Un router Cisco 800= 50W
  - Un switch HP A5500= 160W
  - Un servidor HP DL 120 G= 400W

- Un storage works HP P2000= 340W con 2 fuentes de poder
- Un storage works HP MSA2000= 350W con 2 fuentes de poder
- Dos servidores HP proliant DL 360 G7= 610W c/u con 2 fuentes de poder
- Un servidor Dell power edge 2950 III= 620W con 2 fuentes de poder
- Una librería Dell 132t= 220W
- Un HP enclosure C3000= 1300W
- Un solucionador de VOIP Soundwind S2400= 180W
- Un NBX 3com V3000= 120W

Primeramente se debe sumar el total acumulado de consumo de todos los equipos, que es 7490W. Este consumo total se lo debe dividir para 1000 para pasar de Watios (W) a Kilowatios (KW) 7490W/1000= 7.49KW. Posteriormente, se divide los KW para el coseno de fi (0.8), para poder encontrar el consumo en Kilovoltioamperio (KVA) 7.49KW/0.8= 9.3KVA, ya que es la unidad en la que vienen dados los UPS. Finalmente se tiene el consumo total del Data Center de Akros (9.3 KVA). La siguiente figura 37 muestra el equipo utilizado:

Figura 37 UPS APC Surt 8000

Tomado de: http://guan-ming.en.alibaba.com/product/806412877

CAPÍTULO II

2 Rediseño de la red

Como primer punto se desarrollará el “ciclo de vida de una red”, que es un planteamiento establecido por Cisco en donde se describen las actividades a realizar para la preparación de cambios y actualizaciones en una red. No todos los puntos del ciclo de la vida de la red serán desarrollados en este trabajo de titulación, debido al alcance del mismo. La siguiente información (punto 2.1) fue extraída de la página de cisco:
Tomado de: http://www.cisco.com/web/LA/productos/servicios/docs/Brochure _LCS_062006_SP_Spanish.pdf

2.1 Ciclo de la vida de la red

Este ciclo define un conjunto mínimo de actividades necesarias, por tecnología y por nivel de complejidad de la red, para ayudar a instalar y operar exitosamente tecnologías y optimizar su desempeño. El ciclo de la vida de la red consta de seis pasos importantes (figura 38), los cuales son:

- ***Preparar.-*** Esta fase crea un caso de negocios para establecer una justificación financiera para la estrategia de red, basándose en la definición de los objetivos de la empresa, la consideración de limitaciones, contratación del personal adecuado y la definición del dinero disponible.

- ***Planear.-*** Aquí se realiza un plan de gestión de proyectos donde existan evaluaciones del sitio y las operaciones, identificando las modificaciones necesarias en la red y preparando el cronograma de trabajo. También debe constar de hitos y recursos para hacer el diseño y la implementación, así como de los responsables de cada actividad.

- ***Diseñar.-*** Aquí se diseña una solución que cumple los requerimientos técnicos y se alinea en la dirección estratégica del negocio, creando

planes que guíen la instalación, completando el diseño de la red y generando una propuesta final.

- ***Implementar.-*** En este paso se realiza una integración de la nueva solución, sin crear puntos de vulnerabilidad o alterar el desempeño de la red, realizando pruebas previas, haciendo pruebas de aceptación e instalando la nueva solución.

- ***Operar.-*** Aquí se realiza el mantenimiento de las condiciones de funcionamiento de la red en la operación del día a día, supervisando la red y definiendo políticas y procedimientos.

- ***Optimizar.-*** Se enfoca en la excelencia operacional, adaptando la operación y desempeño de la red a los requerimientos cambiantes del negocio, migraciones tecnológicas o requerimientos del rendimiento de la red.

Figura 38 Ciclo de la vida de la red, PPDIOO

Tomado de: http://www.sifra.net.mx/metodolog%C3%ADa/ppdioo.aspx

Entre los beneficios que conlleva implementar este proceso se puede obtener:

- Incremento del valor de la red en la gestión de negocios y el retorno de inversión y coloca al usuario final en una posición ventajosa al disminuir el costo total de propiedad de la red, mejorando ambos, la agilidad del negocio y la disponibilidad de la red.

- Acelera la estrategia de penetración del mercado al entregar soluciones a tiempo, dentro del presupuesto, y a un precio competitivo a través de una metodología comprobada y consistente.

- Mejora la disponibilidad, estabilidad, seguridad y escalabilidad de la red a través del sistema de planeación, diseño, mantenimiento y optimización.

- Maneja la complejidad creciente de la red al proveer consistencia en los procesos para instalar y mantener la tecnología.

Gracias al uso del ciclo de la vida de la red, se puede proteger, optimizar y crecer en las plataformas de red, lo que generará valor en el negocio y excelencia operacional. Además este planteamiento brindará mayor valor a las inversiones de TI.

Finalmente el “ciclo de la vida de la red” se enlaza con el punto 4.1 del capítulo 4, en donde debido al alcance de este trabajo de titulación el enfoque recaerá solamente sobre la actividad “planear”, ya que la misma desarrolla un plan de gestión con su respectivo cronograma de actividades, permitiendo describir los procesos que se deben realizar al implementar cambios en la red actual.

2.2 Ampliación de la capacidad del canal

En un negocio como el de Akros que depende y está directamente relacionado en la negociación vía internet para estar comunicado con los clientes, la pérdida de comunicación en el enlace es un gran problema cada vez que sucede. El dimensionamiento de la capacidad del canal para la red de Akros sin duda alguna será necesario realizarlo, ya que el actual no abastece las necesidades de la empresa.

Basados en el análisis realizado en el punto 1.3.3 del capítulo 1, Akros necesita incrementar su velocidad de navegación para mejorar su desempeño. De igual manera, no hay que olvidar que se ha propuesto un rediseño de las Vlan´s (referirse al punto 2.3.4), el cual al combinarse con el análisis de la capacidad del canal se obtiene la siguiente propuesta, que a su vez se ve reflejada en la figura 39:

- Se incrementa 100 Kbps en la VLAN 10 para un mejor desempeño en la conexión de los switches.
- Para la VLAN 20 se proponer dejar 1000 Kbps para la interconexión de información de los diferentes aplicativos que corren los servidores.
- Para la VLAN 30 se ha asignado 100 Kbps basándose en un consumo estimado de 15 Kbps por cada una de las 7 impresoras.
- En la VLAN 40 se asigna 100 Kbps basados en un promedio de consumo (20 Kbps) de cada uno de los access points existentes.
- En la VLAN 50 se asigna 600 Kbps, basados en promedios de consumo medio (70 Kbps por equipo).
- Para la VLAN 60 se asigna 800 Kbps ya que aquí el consumo que se asignará será bajo (40 Kbps por equipo).
- Para la VLAN 70 se asigna 1000 Kbps ya que aquí existen usuarios que necesitan mejor capacidad de navegación debido a sus roles laborales. Se estima que el consumo será alto (110 Kbps por equipo).
- En la VLAN 80 se asigna 500 Kbps ya que aquí los roles de monitoreo y control de la red por parte de la TIC no deberán superar el promedio (70 Kbps por equipo).
- Para la VLAN 100 se asigna 100 Kbps más, debido a que se prevé un incremento de llamadas para los próximos años dentro de la empresa.

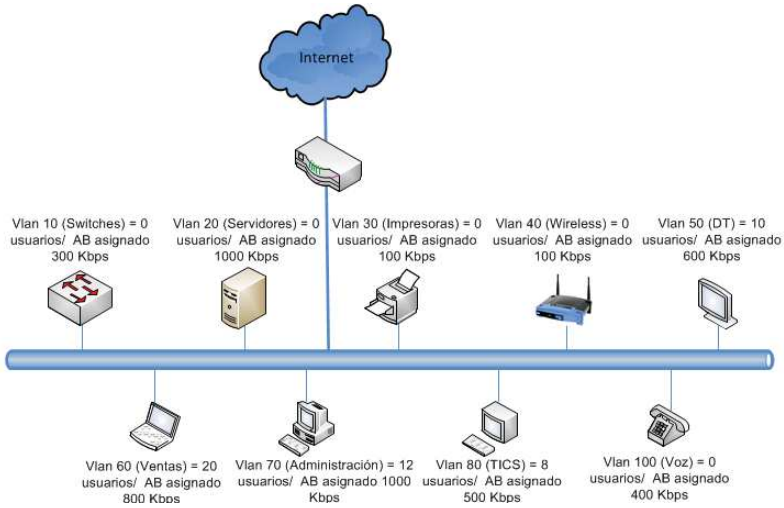


Figura 39 Gestión de la capacidad del canal propuesta

Hay que tomar en cuenta que es recomendable dejar libre capacidad de canal para el crecimiento futuro de la empresa, y se cree prudente que un 20% sería suficiente. Tomando en cuenta este espacio libre para el crecimiento futuro y proponiendo utilizar un enlace de 6Mbps, se obtendría:

6000 Kbps (AB propuesto) - 4600 Kbps (consumo actual estimado) = 1400 Kbps

6000 Kbps x 0.20% (crecimiento futuro)= 1200 Kbps

1400 Kbps – 1200 Kbps = 200 Kbps (AB restante para utilizar)

4600 Kbps (consumo actual estimado) +200 Kbps (AB restante para utilizar) = 4800 Kbps

El cálculo previamente realizado, demuestra que Akros podría disponer de más del 20% libre de capacidad de canal para crecimiento futuro utilizando 6Mbps, lo que cubriría su consumo diario. Adicionalmente se pidió una cotización de capacidad del canal de comunicación a tres ISP's (Telconet, Level3, TVcable) (ver anexos) para poder escoger la mejor opción, basándose en confiabilidad, costo y servicios adicionales.

Una vez analizada las cotizaciones, se ha optado por un cambio de proveedor de internet a Level 3 (ex Global crossing), debido a su atractivo precio ofertado y al excelente SLA (*service level agreement*) 99.8% con respecto al actual con

Telconet del 99.5% (ver anexos). Con Level 3 se obtendría una salida de navegación simétrica de 6 Mbps, la misma que permitiría el desarrollo del negocio de una manera mucho más ágil y efectiva. Al mismo tiempo, se recomienda añadir la utilización de un enlace redundante para de esta manera poder mejorar la redundancia de la red. Por tal motivo, con las siguientes propuestas se darán a conocer las ventajas que conlleva tener un enlace de *backup:*

2.2.1 Implementación del enlace de *backup* utilizando BGP, PBR y Local preference con routers de los proveedores en Akros

Diagrama de topología

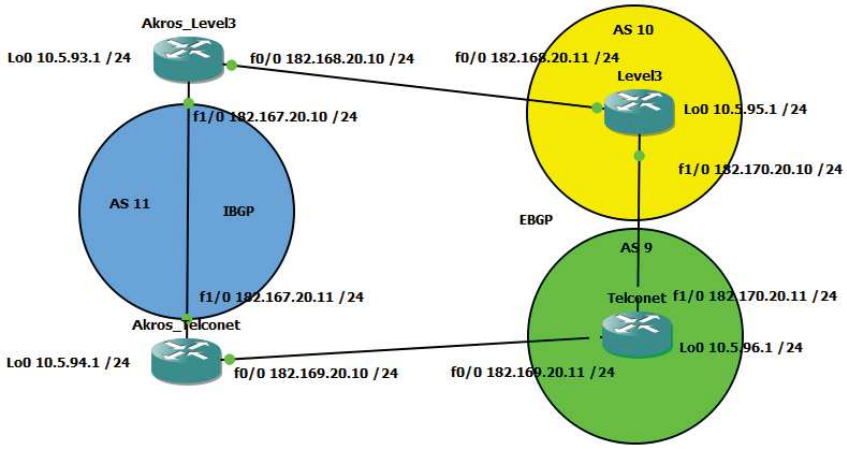


Figura 40 Diagrama enlace de Backup utilizando BGP

Objetivos de aprendizaje

- Configurar BGP con sus respectivos AS
- Configurar PBR, a través de *route-maps* basadas en ACL
- Configurar las listas de acceso requeridas
- Configurar las interfaces fa de cada *router*
- Configurar la preferencia local en las rutas establecidas
- Realizar los comandos *show* para verificar la configuración realizada

Escenario

El AS 11 acepta todas las rutas con origen en cualquiera de los dos ISP. Para conseguir el reparto de carga, el AS 11 seguirá la siguiente política de encaminamiento para los anuncios de salida:

- El tráfico destinado al AS 10 se enviará por el enlace Akros_Leve3- Level3.
- El tráfico destinado al AS 9 se enviará por el enlace Akros_Telconet-Telconet.
- El resto del tráfico (ruta por defecto 0.0.0.0) se enviará por el enlace Akros_leve3- Level3.
- Si el enlace Akros_leve3- Level3 falla, todo el tráfico se enviará por el enlace Akros_Telconet-Telconet.

Por otra parte, la política seguida para los anuncios de entrada al AS 11 es la siguiente:

- El tráfico de Internet destinado a la red 10.5.93.0/24 debe pasar por el enlace Level3-Akros_Level3.
- El tráfico de Internet destinado a la red 10.5.94.0/24 debe pasar por el enlace Telconet-Akros_Telconet.
- Si uno de los enlaces falla, el otro enlace debería encaminar todo el tráfico de Internet destinado a cualquier red interna del AS 11.

Los *routers* (Akros_Level3 y Akros_Telconet) del AS 11 están conectados a un ISP diferente (Level3, Telconet). Entre Akros_Level3 y Akros_Telconet se establece una sesión I-BGP y cada uno de estos routers establecerá una sesión E-BGP con un ISP distinto Akros_Leve3 con Level3 y Akros_Telconet con Telconet.

En el *router* Akros_Telconet se utilizan dos *route map*, uno para los anuncios de entrada (*AS-9-INCOMING*) y otro para los anuncios de salida (*AS-9-OUTGOING*), los cuales se aplican a la sesión E-BGP con el ISP Telconet. En el *route map* de entrada se modifica el

atributo LOCAL_PREF para las rutas cuyo origen esté en el ISP Telconet con un valor de 150. Por otra parte, en el *route map* de salida se añade el número del AS 11 al AS_PATH de la ruta 10.5.93.0 mientras que la ruta 10.5.94.0 no se modifica. De este modo, se anuncia la red 10.5.94.0 hacia el exterior con un AS_PATH más pequeño que la red 10.5.93.0, dando preferencia al enlace Telconet-Akros_Telconet para llegar a 10.5.94.0.

De forma similar, en la configuración del router Akros_Level3 se tienen dos *route maps*, uno para los anuncios de entrada (*AS-10-INCOMING*) y otro para los de salida (*AS-10-OUTGOING*). En el *route map* de entrada se modifica el atributo LOCAL_PREF de las rutas cuyo origen esté en el AS 10 con un valor de 200. De este modo, en el caso de que el AS 11 reciba rutas iguales de ambos ISP, se preferirá el enlace Level3-Akros_Level3 que el enlace Telconet-Akros_Telconet, ya que las rutas recibidas por el primero tendrán un valor del atributo LOCAL_PREF igual a 200 frente a un valor de 150 en las rutas recibidas por el ISP Telconet.

El *route map* de salida en Akros_Level3 modifica el anuncio de la ruta 10.5.94.0 para que tenga un AS_PATH mayor que en el anuncio de la ruta 10.5.93.0 (la cual no se modifica), de modo que se preferirá el enlace Level3-Akros_Level3 para el tráfico entrante al AS 11 con destino a la red 10.5.93.0.

Finalmente, hay que tener en cuenta que los AS no deben servir de tránsito para el tráfico que circula por Internet, de forma que todo el tráfico que circule hacia el AS cliente sea local. Para ello, no se debe anunciar hacia el exterior ninguna ruta que no tenga origen en este AS, ya que anunciar una ruta implica aceptar todo el tráfico que tenga como destino esa ruta. Así que se debe filtrar las rutas recibidas por un ISP para que éstas no sean anunciadas hacia el otro ISP. La lista

de acceso necesaria para este filtrado y el *route map* que la aplicaría se describen a continuación:

ip as−path access−list 10 permit ^$

route−map localonly permit 10

match as−path 10

2.2.2 Implementación del enlace de backup utilizando rutas estáticas, IP SLA y Track con un *router* propietario de Akros

Diagrama de topología

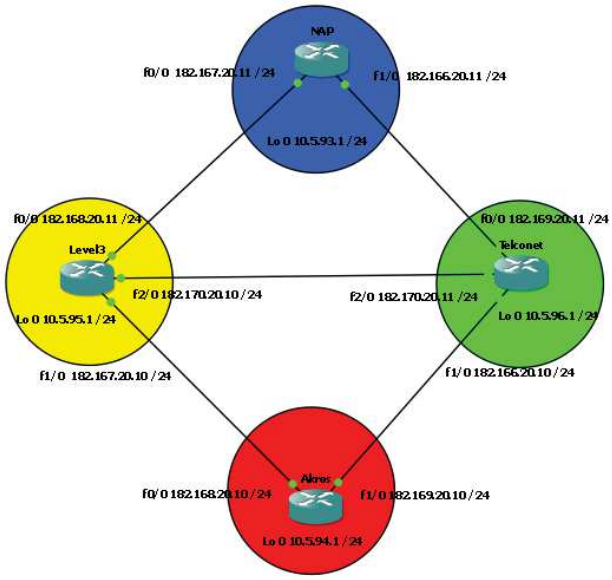


Figura 41 Diagrama enlace de Backup utilizando IP SLA

Objetivos de aprendizaje

- Configurar las interfaces *fast ethernet* de cada *router*
- Configurar las rutas estáticas correspondientes para el ruteo entre los equipos
- Configurar IP SLA
- Configurar el horario, frecuencia, tiempo de respuesta, umbral de IP SLA
- Configurar una distancia administrativa para seleccionar el enlace principal y segundario
- Establecer el rastreo (*tracking*), en la interfaz principal, para controlar el envío de paquetes ICMP

- Realizar los comandos show para verificar la configuración realizada

Escenario

El *router* Akros posee 2 enlaces conectados a distintos ISP. El primero hacia el *router* Level3 que es el principal, debido a que utiliza una distancia administrativa por defecto, y el segundo hacia el *router* Telconet, al cual se le ha colocado una distancia administrativa de 100, convirtiéndolo así, en el enlace de respaldo. Así mismo, ambos ISP están conectados a un *router* llamado NAP (*network access point*), el mismo que tendrá el rol de equipo final para el tráfico de paquetes.

Por otra parte, se crean las rutas estáticas en los 4 *routers*, las cuales permitirán la comunicación entre los mismos. A continuación, se configura IP SLA MONITOR dentro de Akros, Level3 y NAP, que es un mecanismo que permite controlar los enlaces previamente configurados, verificando los tiempos de respuesta de los paquetes ICMP (*internet control message protocol*) de forma periódica. Dentro de las características de IP SLA MONITOR se setea la frecuencia de respuesta de paquetes, el tiempo de respuesta, el umbral y la programación para la operación de IP SLA, la misma que se empezara a utilizar inmediatamente y para siempre. El *router* Telconet no utiliza ningún tipo de IP SLA o Track, debido a que solamente sirve de paso para el enlace de respaldo.

Adicionalmente, se establece un TRACK en la interfaz principal, tanto en el *router* de Level3 así como en el router Akros, el cual permite definir un objeto que rastrea el mecanismo IP SLA. Para lograr lo antes mencionado se utiliza la función REACHABILITY, permitiendo enlazar de esta manera el IP SLA MONITOR con el TRACK. Después, dentro de las rutas estáticas previamente configuradas, se les añade el TRACK correspondiente, para establecer un enlace entre la ruta estática y el TRACK.

Se debe tener cuidado en los falsos positivos, que son pequeñas caídas en la red que podrían activar los TRACKS y empezarían a desviar el tráfico por la interfaz de respaldo. Para evitar lo antes mencionado, se utiliza, los siguientes comandos:

track 5 rtr 5 reachability

Donde por un lado el parámetro permite verificar alcanzabilidad "reachability" y por otro, el comando:

delay down 10 up 5

Indica que ante la falla de recepción de IP SLA 5 se dispara un contador de 10 segundos, el cual indica que si se sobrepasa este tiempo, automáticamente se ejecuta el TRACK DOWN activando la interfaz de *backup* inmediatamente. De la misma manera, cuando la interfaz principal sube nuevamente, todo el tráfico se redireccione otra vez por la misma, ya que el contador de 5 segundos esta seteado en el comando.

Finalmente, hay que tener cuidado con el correcto uso de IP SLA y Track, ya que como es un mecanismo muy sensible a los cambios en el flujo del tráfico, puede causar falsos positivos que son pequeñas perdidas de paquetes lo que activa el *track* y a su vez la ruta de respaldo.

Ambas propuestas manejan diferentes mecanismos para brindar una redundancia muy confiable. Por ejemplo, IP SLA reúne información acerca del estado de la ruta previo envío de paquetes, TRACK permite el rastreo de los paquetes en todo momento, BGP logra un buen balanceo de carga, PRB permite definir políticas acorde a las necesidades de la empresa, Local Preference permite seleccionar el camino para el envío de paquetes, etc.

La desventaja al utilizar la primera propuesta se da que al momento que exista alguna variación en la red, los únicos habilitados para manejar las

configuraciones de los *routers* finales son los proveedores, lo que generará dependencia hacia el proveedor en los cambios a realizarse.

Por otra parte, el mayor beneficio al utilizar la segunda propuesta se encuentra en el hecho de que Akros pueda manejar su propio *router*, permitiéndole así configurar sus propias políticas y métodos para el enrutamiento del tráfico, así como también permitirá al personal de TI tener contacto directo con los protocolos de enrutamiento, lo que finalmente se traduce en un control total de la red para cambiar por ejemplo métricas y políticas de enrutamiento sin la necesidad de que intervenga el ISP como se lo venía haciendo.

En conclusión la segunda opción es la más apropiada para la empresa, ya que ofrece la posibilidad de que Akros finalmente pueda manejar sus propios protocolos de enrutamiento, permitiendo así cambiar a su conveniencia las configuraciones, políticas y métricas, utilizando para ello protocolos muy confiables y robustos.

Las configuraciones finales y comandos utilizados en ambas propuestas antes mencionadas se las realizó mediante el uso del emulador **GNS3**. Todo esto se puede consultar en anexos. Adicionalmente, se añadió como propuesta en anexos el uso de un analizador de protocolos llamado **Wireshark,** el cual permitirá examinar el tráfico que cursa la red para la detección de problemas.

2.3 Rediseño del data center, redistribución de *switches,* VLAN's y subneteo IP

2.3.1 Rediseño del *data center*

A medida que se desarrolla este proyecto, se ha tenido la posibilidad de ir realizando algunos cambios importantes en el estado del *data center* de Akros. Estos cambios han sido tanto de *hardware* como de *software* y son los siguientes:

- Ampliación del *data center* a 4.5x3.0 metros cuadrados.

Figura 42 Nuevo *Data center* (vista frontal y lateral)

- Se trajo acometidas por escalerilla para el cableado, para mantenerlo en orden y aislado del suelo.

Figura 43 Tablero de distribución

- Se colocó un *bypass* eléctrico desde el tablero, para mejorar la disponibilidad y evitar los fallos eléctricos. Este bypass está encargado de alimentar al UPS.

Figura 44 *Bypass* eléctrico

- Se implementó un tablero con circuitos eléctricos dedicados tanto en 20A/120V como en 20A/220V, el cual permitirá soportar equipos que manejen una mayor cantidad de voltaje.

Figura 45 Tablero de distribución

- En los enlaces de cada *switch* de distribución se *implementó link aggregation* 802.3ad, para poder tener redundancia en las comunicaciones que existen entre ellos.

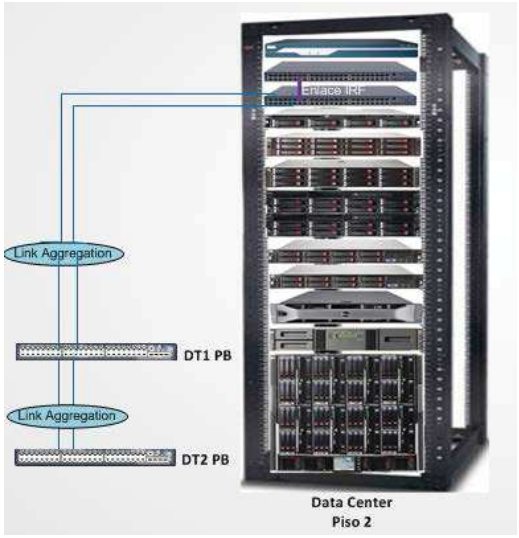


Figura 46 Enlaces *link aggregation*

- Se colocó otro *switch* de *core* HP A5500 de respaldo con un enlace IRF de 10Gb, para una mejor disponibilidad de la red.

Figura 47 *Switch* A5500

Tomado de: http://es.apacelli.com/routers-and-switches-hp/hp-a5500-48g-poe-si-jd372a-/photo-1/

- Se adquirió otro switch de distribución HP A5120 para una mejor distribución en las áreas de trabajo (segmentación VLAN's).

Figura 48 *Switch* A5120

Tomado de: http://www.itdevices.ca/JE071A.php

- Se adquirió un *blade enclosure* HP C7000 en reemplazo del C3000, debido a que el mismo se encuentra casi lleno y no permitirá el almacenamiento futuro de más servidores en su interior. El C7000 tiene una capacidad de almacenamiento total de 16 servidores.

Figura 49 Hp *Blade* C7000

Tomado de: http://www.vibriefing.com/how-to-reset-blade-slot-in-hp-c7000-chassis/

- Se adquirió dos HP *storage* P4300 con una capacidad de almacenamiento de 3.5TB cada uno, distribuidos en 6 discos duros de 600GB cada uno. En el primer equipo se colocó todos los servicios que se encontraban virtualizados en el P2000, en tanto que en el segundo equipo está siendo utilizado como *backup* permanente para evitar que los servicios queden fuera abruptamente. Mientras tanto, en el P2000 se instaló virtualmente el *lync communicator* y los dos servidores DL 360 están siendo utilizados como respaldos de *lync*. Todo esto se realizó debido que hoy en día, la empresa necesita mayor capacidad con

respecto a comunicaciones internas de video conferencia, voz y *chat*.

Figura 50 Hp *server* P4300

Tomado de: http://www.abssystems.com.my/index.php?action=productpage&fc=20

- En reemplazo de la antigua librería Dell *powervault* 132t se adquirió una nueva librería HP MSL (*modular smart library*) 2024 con mayor capacidad de almacenaje ya que posee 36 slots para cintas lo que se traduce en 40TB. Además posee un menor tamaño, solo ocupa 2U. Se adquirió esta librería debido al gran descuento 50% que brindo el proveedor HP y a la mayor capacidad de almacenamiento en comparación a la anterior librería.

Figura 51 Hp *library* MSL 2024

Tomado de: http://www.glcomp.com/hp-storageworks-msl2024-1-lto-3-ultrium-920-sas-tape-library

- Se reemplazó el servidor *power edge* 2950 III por el *power edge* rack *server* Dell R710 debido a la falta de procesamiento y capacidad de almacenamiento que posee el mismo. El nuevo equipo tiene incorporado el software VMware y a su vez posee un ahorro de energía de hasta un 25% más a comparación del 2950 III, aparte soporta hasta 288GB de memoria RAM**.** Este equipo se lo utiliza como servidor de *backup*, ya que como su antecesor, saca los respaldos de todos los demás equipos y los almacena en la nueva librería HP MSL 2024.

Figura 52 Dell *power edge* R710

Tomado de: http://www.dell.com/us/business/p/poweredge-r710/p

- Se adquirió un nuevo sistema de enfriamiento de confort LG S362CP con capacidad de 36000 BTU, el cual también posee remoción de humedad y circulación del aire externa/interna, suficiente para el espacio y número de equipos del *data center* actual.

Figura 53 *Data center* actual, sistema de refrigeración LG

- El *data center* se encuentra sellado herméticamente.

Figura 54 *Data center* hermetizado

- Se colocó la debida toma a tierra para la descarga de energía de los equipos y así evitar posibles descargas directas en los equipos.

Figura 55 Toma a tierra

- Se realizó la correcta etiquetación y ordenamiento del cableado en los *patch panels*, para un mejor control y entendimiento del mismo.

Figura 56 Orden del cableado en el *patch panel*

- Se adquirió un Eaton *blade* UPS de 14 KVA (*kilo volt amere*), encargado de brindar el respaldo energético al cuarto de servidores en caso de algún corte de energía repentino. El tiempo estimado de energía con baterías es de veinte minutos, suficiente para poder apagar todos los equipos dentro del data center si se requiriera. El cálculo para el análisis de carga que se realizó para la adquisición de este UPS es el siguiente:

Análisis actual de cargas:

- Un router Cisco 800= 50W
- Dos switches HP A5500= 160W c/u
- Un servidor HP DL 120 G= 400W
- Un storage works HP P2000= 340W con 2 fuentes de poder
- Un storage works HP MSA2000= 350W con 2 fuentes de poder
- Dos storage works HP P4300= 360W c/u con 2 fuentes de poder
- Dos servidores HP proliant DL 360 G7= 610W c/u con 2 fuentes de poder
- Un servidor Dell power edge R710= 570W con 2 fuentes de poder
- Una librería Dell MSL2024= 170W
- Un HP enclosure C7000= 2400W
- Un solucionador de VOIP Soundwind S2400= 180W
- Un NBX 3com V3000= 120W

Primeramente se debe sumar el total acumulado de consumo de todos los equipos, que es 10040W. Este consumo total se lo debe dividir para 1000 para pasar de Watios (W) a Kilowatios (KW) 10040W/1000= 10.04KW. Posteriormente, se divide los KW para el coseno de fi (0.8), para poder encontrar el consumo en Kilovoltioamperio (KVA) 10.04KW/0.8= 12.55KVA, ya que es la unidad en la que vienen dados los UPS. Finalmente se tiene el consumo total del Data Center actual de Akros (12.55 KVA). La siguiente figura 57 muestra el equipo utilizado:

Figura 57 Nuevo UPS Eaton Powerware de 14 KVA

Tomado de: http://ups-on-line-colombia-apc-powerwere.blogspot .com/p/ups-powerwere.html

2.3.2 Redistribución de *switches*

Se ha distribuido la interconexión de los *switches* con tecnologías tales como *link aggregation* e IRF ya que de esta manera se podrá obtener redundancia en los enlaces. Además, es muy importante poseer un *switch* de *core* secundario (HP A5500 igualmente) para ser utilizado en caso de que el principal no esté operativo. Así mismo, debido al crecimiento del departamento de tecnología (TI) se ha visto en la necesidad de aumentar otro *switch* de distribución, siguiendo lo misma línea HP A5120. A continuación se detallará lo antes mencionado:

- ***Link aggregation.-*** Es un término usado para describir las diferentes redes, métodos de combinación y conexiones de red en paralelo que se utilizan para aumentar el rendimiento más allá de lo que una sola conexión podría sostener, y para proporcionar redundancia en caso de que uno de los enlaces falle. Así se puede contar con los enlaces redundantes entre switches y si alguno se cae, el otro estará operativo, aumentando la disponibilidad de la red.

- **IRF.-** La tecnología IRF (*intelligent resilient framework*) presenta una solución para permitir visualizar varios *switches* como si fueran uno solo. Justamente esto es lo que se implementa entre los *switches* HP A5500 para que ambos se vean como un solo

switch, consolidando la gestión alrededor de una única dirección IP de administración.

La figura 58 muestra el antes de la red (sin *link aggregation*, IRF y *switch* HP) y la figura 59 muestra el después de la red (con *link aggregation*, IRF y *switch* HP).

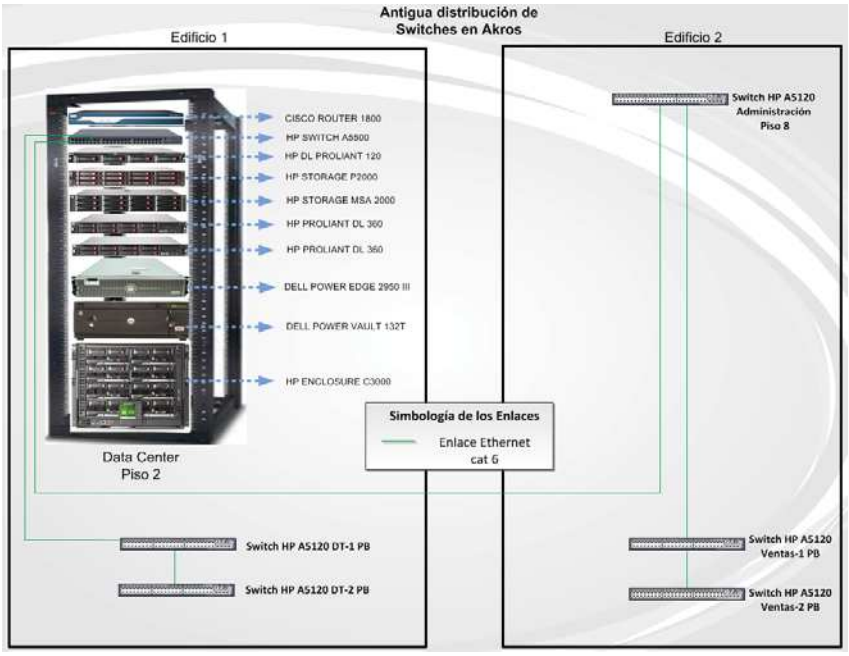


Figura 58 Antigua distribución de *switches*

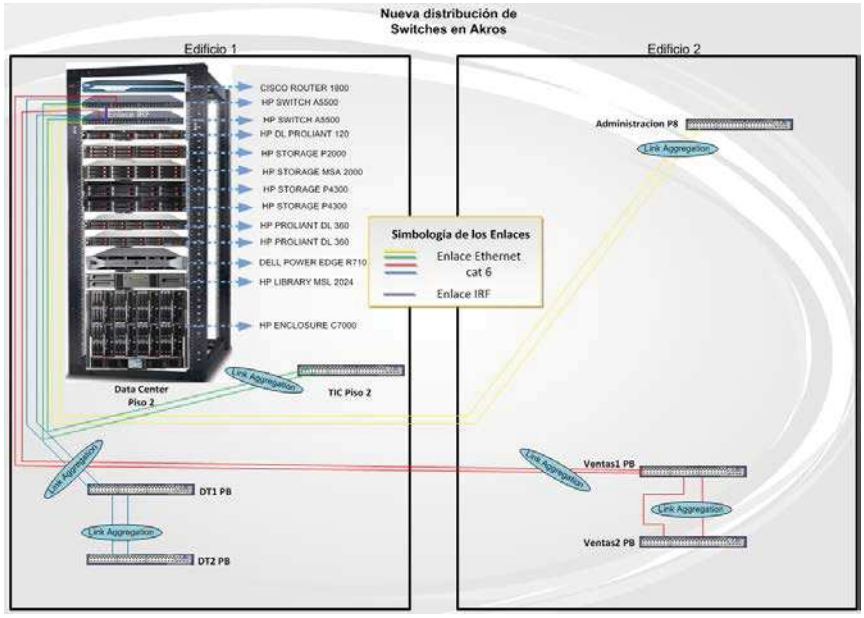


Figura 59 Nueva distribución de *switches*

2.3.3 Subnetting

Como parte de la mejora de este proyecto, el subnetting de las direcciones IP utilizadas en Akros es de gran ayuda, ya que de esta manera se podrá optimizar de mejor manera el direccionamiento ayudando directamente a una mejor distribución de las VLAN's. Para entender de más a fondo estos procesos, se los explicará a continuación.

La función del subnetting es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabaje a nivel de envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio. El subnetting permite una mejor administración, control del tráfico y seguridad al segmentar la red por función. También, mejora el rendimiento de la red al reducir el tráfico de *broadcast* de la red. Existen 2 tipos de direccionamiento y son:

- ***Classful*.-** Cada clase tiene una máscara de red por defecto, la Clase A 255.0.0.0, la Clase B 255.255.0.0 y la Clase C 255.255.255.0. Al direccionamiento que utiliza la máscara de red por defecto, se lo denomina "*classful*".

- ***Classless*.-** Siempre que se realice subneteo, se creará a partir de una dirección de red clase A, B, o C y está se adaptará según los requerimientos de subredes y hosts por subred. Al direccionamiento que utiliza una máscara de subred, se lo denomina como "classless" es decir, la clase de una dirección IP es definida por su máscara de red y no por su dirección IP. Dentro del direccionamiento classles, existen 2 técnicas utilizadas y son:

    - **VLSM (*variable length subnet mask*).-** Es una técnica por la cual se elabora un esquema de direccionamiento utilizando varias máscaras en función de la cantidad de hosts, es decir, la cantidad de hosts determina la longitud total de la máscara.

- **CIDR (*classles inter-domain router*). -** Permite un esquema de sumarización flexible, ya que el router utiliza protocolos que no consideran las clases y así envía actualizaciones incluyendo las máscaras de subred.

La siguiente tabla 3 muestra las clases de direcciones IP existentes:

3 Tabla 3 Clases de direcciones IP

Clase	Direcciones disponibles		Cantidad de redes	Cantidad de host	Aplicación
	Desde	Hasta			
A	0.0.0.0	127.255.255.255	128	16777214	Redes grandes
B	128.0.0.0	191.255.255.255	16324	65534	Redes medianas
C	192.0.0.0	223.255.255.255	2097152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	n/a	n/a	Multicast
E	240.0.0.0	255.255.255.255	n/a	n/a	Investigación

El intervalo 127.0.0.0 a 127.255.255.255 está reservado para Loopback y no se utiliza

Cada clase de direccionamiento IP, consta de cuatro octetos y dependiendo de la clase estos se dividirán en direcciones de Red o direcciones de *host*, como se muestra en la tabla 4:

Tabla 4 Octetos en cada clase de dirección IP

Clase A	Red	Host		
Octeto	1	2	3	4
Bits	11111111	00000000	00000000	00000000
Mascara	255	0	0	0

Dirección de red: Primer octeto 8 bits
Dirección de host: Últimos tres octetos 24 bits

Clase B	Red	Host		
Octeto	1	2	3	4
Bits	11111111	11111111	00000000	00000000
Mascara	255	255	0	0

Dirección de red: Primeros dos octetos 16 bits
Dirección de host: Últimos dos octetos 16 bits

Clase C	Red	Host		
Octeto	1	2	3	4
Bits	11111111	11111111	11111111	00000000
Mascara	255	255	255	0

Dirección de red: Primeros tres octetos 24 bits
Dirección de host: Ultimo octetos 8 bits

Para poder realizar subnetting, es necesario trabajar con direcciones de 32 bits, para ello se deben convertir en números decimales. En el proceso de conversión cada bit de un intervalo (8 bits) de una dirección IP, en caso de ser "1" tiene un valor de "2" elevado a la posición que ocupa ese bit en el octeto y luego se suman los resultados. Para poder entender de mejor forma, la tabla 5:

Tabla 5 Tabla de conversión

Posición valor de los bits									
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binario	1	0	0	0	0	0	0	0	= 128
Decimal	128	0	0	0	0	0	0	0	+
Binario	0	1	0	0	0	0	0	0	= 64
Decimal	0	64	0	0	0	0	0	0	+
Binario	0	0	1	0	0	0	0	0	= 32
Decimal	0	0	32	0	0	0	0	0	+
Binario	0	0	0	1	0	0	0	0	= 16
Decimal	0	0	0	16	0	0	0	0	+
Binario	0	0	0	0	1	0	0	0	= 8
Decimal	0	0	0	0	8	0	0	0	+
Binario	0	0	0	0	0	1	0	0	= 4
Decimal	0	0	0	0	0	4	0	0	+
Binario	0	0	0	0	0	0	1	0	= 2
Decimal	0	0	0	0	0	0	2	0	+
Binario	0	0	0	0	0	0	0	1	= 1
Decimal	0	0	0	0	0	0	0	1	= 255

Para la implementación del subnetting en la empresa Akros, se deberá partir de la IP que se utiliza 172.16.0.0 /16 y posteriormente comenzar el subneteo. El correcto subneteo en Akros va de la mano con la distribución de las VLAN´S que se verá a continuación.

2.3.4 Distribución de las VLAN's

Para poder optimizar de mejor manera la administración de la red, hace falta segmentarla, y la menor forma de realizar esto es con el uso de las VLAN´s. Es por eso que se ha propuesto realizar una nueva configuración de VLAN´s dentro de los *switches.* La propuesta de la

nueva distribución de VLAN´s consta en dividirlas por departamentos para obtener un mejor control sobre cada uno, tal como se muestra en la figura 60. Además en anexos, se colocarán las configuraciones realizadas para la elaboración de las VLAN's.

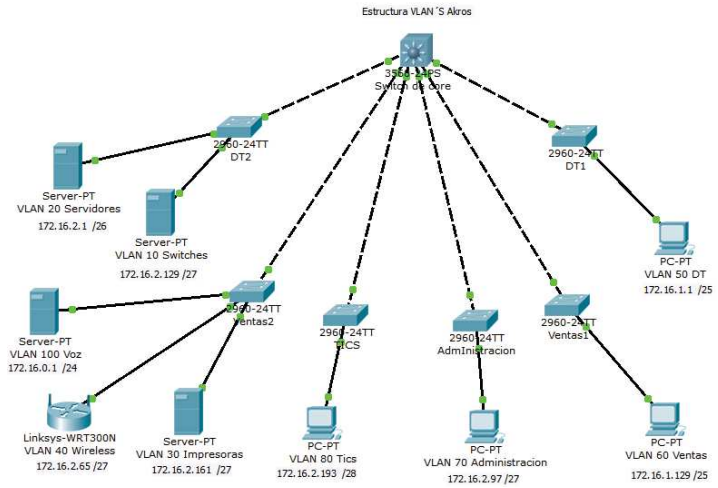


Figura 60 Esquema de VLAN´S

Primeramente se necesita saber cuántas IP´s están ocupadas para posteriormente realizar una proyección del crecimiento de la empresa para dejar suficientes IP´s disponibles para el futuro, tabla 6:

Tabla 6 IP´s utilizadas en Akros

Departamento	Cantidad de IP´S utilizadas	IP´S disponibles después de realizar el Subneteo
Voz	120	253
DT	50	126
Ventas	40	126
Servers	25	62
Wireless	21	30
Administración	20	30
Switches	12	30
Impresoras	11	30
Ti	10	14
Management	8	14

Una vez que se tiene la cantidad de IP´s utilizadas y teniendo en cuenta el crecimiento de la empresa, se procede con el subnetting que ayudará a optimizar el uso de las IP´s en la red, tal como se muestra en la tabla 7:

Tabla 7 Distribución de VLAN's y subnetting de IP´s

Distribución de VLAN´s y subneteo IP					
Numero VLAN	**Nombre VLAN**	**Red**	**Broadcast**	**Rango IP**	**Mascara**
100	Voz	172.16.0.0	172.16.0.255	172.16.0.1-172.16.1.254	255.255.255.0
50	DT	172.16.1.0	172.16.1.127	172.16.1.1-172.16.1.126	255.255.255.128
60	Ventas	172.16.1.128	172.16.1.255	172.16.1.129-172.16.1.254	255.255.255.128
20	Servidores	172.16.2.0	172.16.2.63	172.16.2.1-172.16.2.62	255.255.255.192
40	Wireless	172.16.2.64	172.16.2.95	172.16.2.65-172.16.2.94	255.255.255.224
70	Administración	172.16.2.96	172.16.2.127	172.16.2.97-172.16.2.126	255.255.255.224
10	Switches	172.16.2.128	172.16.2.159	172.16.2.129-172.16.2.158	255.255.255.224
30	Impresoras	172.16.2.160	172.16.2.191	172.16.2.161-172.16.2.190	255.255.255.224
80	Tics	172.16.2.192	172.16.2.207	172.16.2.193-172.16.2.206	255.255.255.240
90	Management	172.16.2.208	172.16.2.223	172.16.2.209-172.16.2.222	255.255.255.240

Todo el punto 2.3 se lo puede resumir en el diagrama final propuesto para la red de Akros, el cual se lo puede visualizar con la siguiente figura 61:

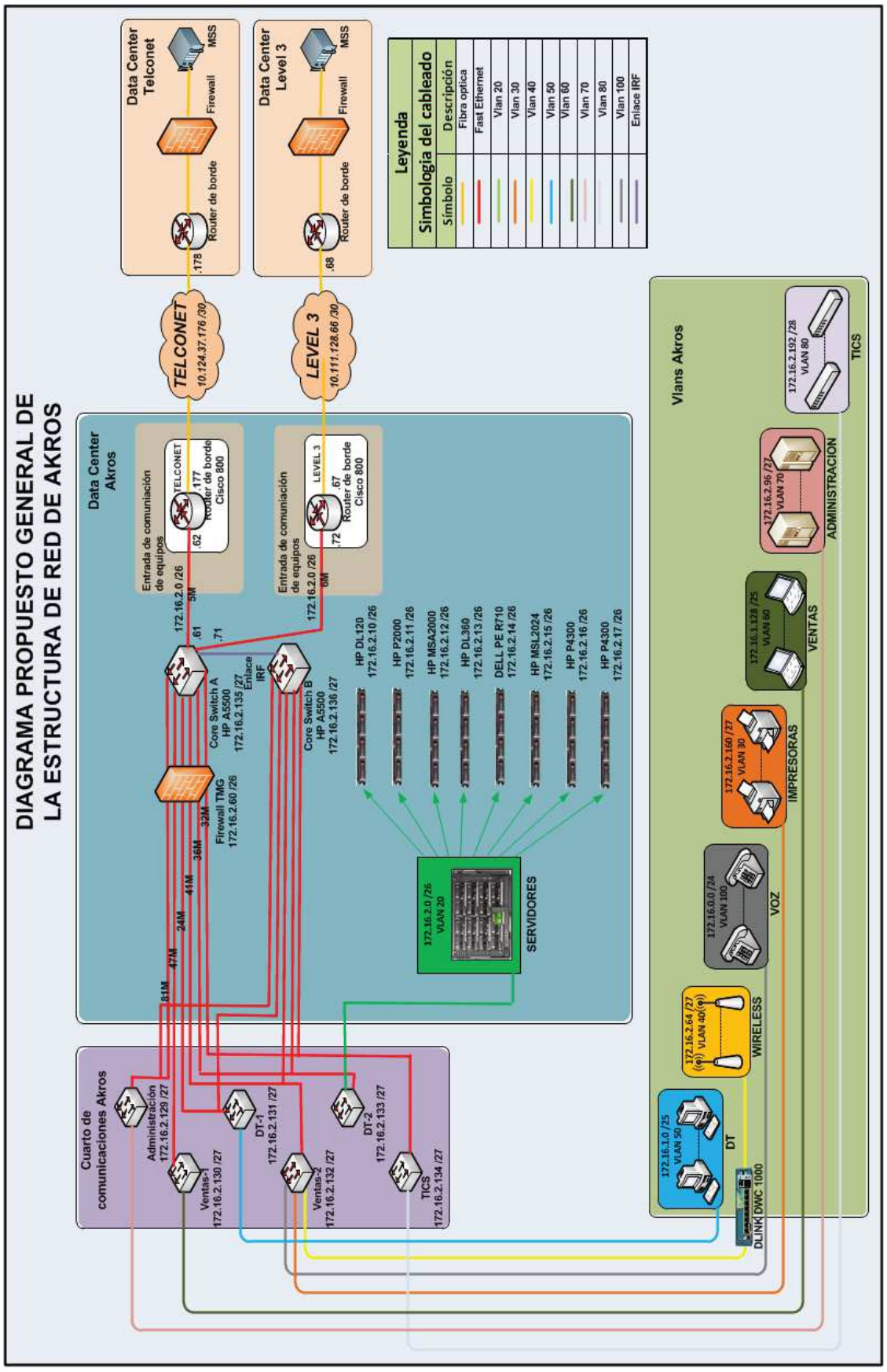


Figura 61 Diagrama general de la estructura de red

2.4 Virtualización de la información

La virtualización es un método que hoy en día la mayoría de empresas lo está implementando gracias a sus múltiples beneficios, tal como se pudo ver en el punto 1.3.5 del capítulo uno. De igual manera, en el punto 2.3.1 algunos de los equipos que fueron adquiridos, tales como el servidor que presta los servicios de backup a la red (R710), así como también los dos (P4300), poseen mucha más capacidad de almacenaje y procesamiento, lo que permitirá virtualizar el SO (plataforma) y los aplicativos (recursos) de mejor manera, ya que la virtualización ocupa mucho espacio en disco y memoria RAM.

Se realizará un ejemplo (ver anexos) en el cual se podrá constatar cómo debe virtualizar un sistema operativo, utilizando para esto el *software* VMware.

La virtualización posee una característica muy útil llamada "*cluster*", que es un mecanismo que fue diseñado para redundar equipos virtualizados, así en caso que un equipo este fuera de servicio, el otro se levantará inmediatamente en el mismo punto que lo dejó el anterior tal como lo demuestra en la figura 62, en donde a manera de ejemplo el servidor HTTP se deshabilita e inmediatamente otro servidor sube y remonta su función:

Figura 62 Uso de cluster en la virtualización

Existe una variante de la virtualización llamada *cloud computing*, la cual se está volviendo muy popular hoy en día debido a su gran versatilidad y

capacidad de integración entre otras cosas. A continuación se dará a conocer lo que es *cloud computing* y por qué se sugiere su uso en este proyecto.

2.4.1 Cloud computing

Es la tendencia a basar las aplicaciones en servicios alojados de forma externa, es decir en la propia web. La mayoría de departamentos de TI (tecnología de la información) se ven obligadas a dedicar una buena parte de su tiempo a la frustrante tarea de implementar, mantener y actualizar proyectos, que con demasiada frecuencia, no suponen un valor añadido en el balance final de la compañía. Cada vez más, los equipos de TI están volviendo sus miradas a la tecnología de cloud para minimizar el tiempo empleado en actividades de menor valor y permitir a los equipos de TI centrarse en actividades más estratégicas, que tienen un mayor impacto en los procesos comerciales. *Cloud computing*, posee grandiosas funciones tales como:

- Integración probada de servicios web con mucha mayor facilidad y rapidez con el resto de las aplicaciones empresariales (tanto *software* tradicional como *cloud computing* basado en infraestructuras), ya sean desarrolladas de manera interna o externa.
- Prestación de servicios con una mayor capacidad de adaptación, recuperación de desastres completa y reducción al mínimo de los tiempos de inactividad.

- No se necesita instalar ningún tipo de *hardware* o s*oftware* en una infraestructura 100% de *cloud computing*. La ventaja de esta tecnología es su simplicidad y el hecho de que requiera mucha menor inversión para empezar a trabajar.

- Rápida implementación y con menos riesgos donde se podrá empezar a trabajar muy rápidamente gracias a una infraestructura de *cloud computing*.

- Gran capacidad de personalización la cual proporciona útiles funciones de personalización y configuración de aplicaciones. Ideal para el desarrollo de aplicaciones que estén en concordancia con las crecientes necesidades de la organización.

- Permite informes de manera directa y sencilla, por lo que el personal de TI no necesita emplear todo su tiempo realizando pequeñas modificaciones y ejecutando informes.

- Actualizaciones automáticas que no afectan negativamente a los recursos de TI, ya que *cloud computing* obliga a decidir entre actualizar y conservar el trabajo, porque esas personalizaciones e integraciones se conservan automáticamente durante toda la actualización.

En la siguiente figura 63 se muestra como *cloud computing* se vería desde una perspectiva general de la red de Akros:

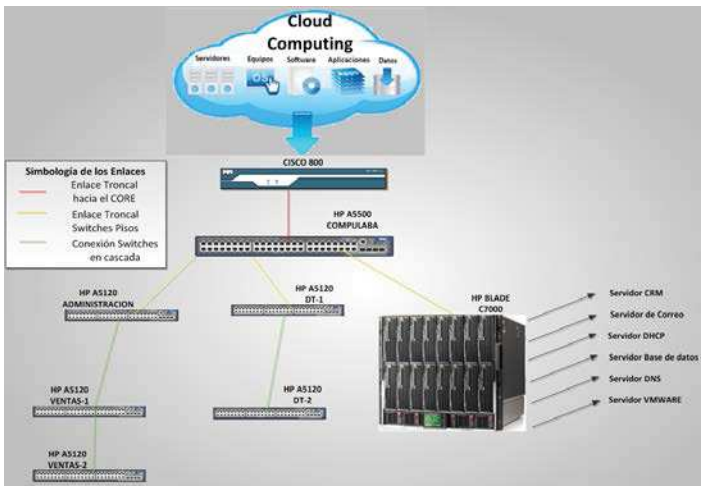


Figura 63 *Cloud computing*

Dentro de *cloud computing* se pueden encontrar tres clases diferentes las cuales son:

- ***Private cloud* (*housing*).-** Son escenarios donde las compañías migran físicamente sus equipos y operaciones a un *data center*

externo. *Private cloud* aplica los conceptos *de cloud computing* a recursos propios de la empresa que consume el servicio externo de un proveedor, facilitando la capacidad de manejar aplicaciones nuevas y existentes, mientras se brinda seguridad y regulación.

- ***Public cloud* (*hosting*).-** Son escenarios donde las compañías necesitan mover datos o aplicaciones desde su interior al exterior, sin la necesidad de mover equipos físicamente. *Public cloud* involucra recursos y servicios TI tales como monitoreo, seguridad lógica y soporte que son manejados mediante virtualización desde un *data center* externo. Todos estos servicios se pueden acceder a través de navegadores web.

- ***Hybrid cloud*.-** Es un tipo de escenario semi público, el cual se comporta como un *private cloud* con la particularidad que ciertas empresas pueden compartir su información con ciertos niveles de permiso, por ello el término semi público. El control *de public cloud* lo hace el proveedor, mientras que el control de *private cloud* lo hace la empresa, y la finalidad es que a través de ambos enfoques se logre satisfacer las necesidades de un sistema de aplicación. *Hybrid cloud* brinda la capacidad de elegir los proveedores de servicio, los mismos que serían capaces de compartir las cargas de servicio, teniendo así una relación más flexible.

Como resultado del análisis de los tipos de *cloud computing* y las características funcionales que ofrecen, en Akros se podría llegar a implementar el *private cloud*, debido a que este servicio logrará reducir el espacio físico que ocupan los servidores, lo que conlleva a un menor consumo de energía en el data center, permitiendo así un crecimiento de equipos y aplicaciones en un lugar remoto, sin la preocupación del área física y el consumo energético que todo esto demanda. Además, con *private cloud* se podría tener mejor seguridad y control del sistema ya que el mismo opera 24x7 sin interrupciones. Finalmente el personal de

TI ya no tendría que preocuparse del monitoreo, mantenimiento y control de los diferentes equipos y aplicativos que permiten que la red de Akros esté operativa, ya que todo estaría a cargo del proveedor que brinde el servicio de *housing*, los mismos que reportarían cualquier incidente al departamento de TI de Akros. En anexos, se encuentra una proforma de *cloud computing* realizada por Telconet, la cual contiene el precio y las características que conlleva implementar *private cloud* en Akros. Toda la información anterior fue recuperada de: http://www.luisespino.com/pub/cloud_computing_luis_espino.pdf

2.5 Mejores prácticas para la seguridad de la red de Akros utilizando un *firewall* TMG

Las mejores prácticas dentro del *firewall* de Akros son recomendaciones a seguir que se utilizarán para mejorar y/o optimizar las reglas y políticas de acceso o denegación a la red. El rendimiento del *firewall de Akros* está directamente relacionado con el tipo de información que el mismo deba evaluar, por lo que es necesario configurar políticas claras y precisas. Entre las políticas que se recomiendan configurar dentro del firewall de Akros se puede encontrar:

- Configurar el nombre del dominio (Akroscorp).
- Cambiar la clave cada 15 días para evitar posibles infiltraciones
- Establecer el cronograma, en el que se tendrá:
  - Bloqueo de navegación de 8:00am a 18:00pm.
  - Permiso para actualizaciones de 13:00pm a 15:00pm.
  - Modo de ocultación activo 24h todos los días.
  - Permiso para secuencias TCP activo 24h todos los días.
  - Análisis de puertos activo 24h todos los días con intervalos de 1 hora.
  - Análisis de archivos en el *file server* cada 2 horas.
  - Restricción de conexión a internet desde las aplicaciones que utiliza Akros de 18:00pm a 7:00am.

  - Restricción de puertos USB 24h los 7 días de la semana.
  - Permiso al *file server* a todos los usuarios de 8:00am a 18:00pm.
  - Filtrado del contenido (.txt, .dir, .dxr, etc) las 24h todos los días.
  - Permisos para conexión de escritorio remoto de 8:00am a 18:00pm.
  - Deshabilitar el ping hacia el *firewall* las 24h los 7 días de la semana.
- Permiso a los servicios del *Active Directory* para acceder desde un *host* local hacia la LAN, siempre y cuando se utilicen las claves de administrador.
- Denegación de permisos de escritura y ejecución dentro del file server
- Permiso para las actualizaciones de Windows desde un *host* local hacia los sitios de actualización de Microsoft.
- Activación del bloqueo de puertos USB en todas los host que no pertenezcan a un cargo gerencial.
- Acceso de navegación al internet sin ningún tipo de restricción a los gerentes de cada area, basados en la MAC (media access control) de sus equipos.
- Denegación de acceso a sitios web no autorizados (Hotmail, YouTube, Facebook, etc) a todos los usuarios que no tengan un cargo gerencial, basado en la MAC de cada equipo.
- Creación de grupos de trabajo para facilitar la configuración y aplicación de una nueva política.
- Habilitar la protección contra la falsificación de MAC, para evitar el acceso no autorizado a la LAN.
- Permitir el modo de ocultación cuando se navega por internet, para que los sitios web no puedan saber el tipo de SO y navegador que utiliza Akros.
- Permitir secuencias TCP para impedir que un intruso pueda falsificar direcciones IP calculando aleatoriamente números de secuencia TCP.
- Habilitar el control de la denegación de servicio para mantener controlada las conexiones entrantes a los diferentes puertos.

- Habilitar el análisis de puertos para supervisar todos los paquetes entrantes.
- Filtrar el tipo de contenido que va a ser manipulado por los usuarios, entre los que se pueden encontrar (archivos .txt, .dir, .dxr, .dat, etc).
- Activación del análisis de contenido de archivos descargados desde la web o correo electrónico.
- Deshabilitar el uso de ping hacia el *firewall,* para evitar la posible detección de la dirección IP.
- Bloqueo al acceso a la base de datos desde todo *host* que no esté dentro de la VLAN de TICS.
- Restricción de la conexión hacia internet de las aplicaciones (ERP, CRM, GP) fuera del horario de trabajo.
- Realizar pruebas periódicas en contra del *firewall* para validar que las políticas funcionen correctamente.

Adicionalmente, se recomienda seguir el siguiente orden de configuración de las políticas para mejorar aún más desempeño en el *firewall:*

- Reglas de denegación globales.- Deben ser utilizadas cuando se quiere denegar el acceso a protocolos específicos a todos los usuarios.
- Reglas de acceso globales.- Deben ser utilizadas cuando se quiere permitir el acceso a protocolos específicos a todos los usuarios.
- Reglas para un *host* específico.- Deben ser utilizadas para darle o quitarle acceso a un determinado *host.*
- Reglas para usuarios específicos.- Deben ser utilizadas para darle o quitarle acceso a un determinado usuario, sin importar el host en el que se autentique.
- Otras reglas de permiso.- Estas reglas deben ser utilizadas cuando ninguno de los criterios anteriores apliquen.

2.6 Rediseño de la WLAN

En este punto se contemplará la falta de cobertura inalámbrica de la red en algunos lugares de Akros. La herramienta a ser utilizada para realizar las mediciones de la señal inalámbrica será el *software* de demostración VisiWave, el cual será descrito a continuación:

2.6.1 Restructuración de la red WLAN empleando VisiWave

Como se pudo constatar en el punto 1.3.7.1, la utilización del software Visiwave *site survey* fue muy útil para darse cuenta que en Akros existe una falta de cobertura de señal inalámbrica en ciertas zonas, por lo que a continuación se realizará una simulación en donde se presentarán los mismos mapas pre cargados en Visio pero con una reubicación de los AP´s y en algunos casos la utilización de otro AP para mejorar la cobertura de la señal.

- **ED 1 PB**

  Para esta área, no es necesario reubicar los AP´s, debido a que su área de cobertura está bien distribuida.

- **ED1 P2**

Survey Information	
Number of Wi-Fi Data Points	2
Number of Data Points (Associated)	2
Number of Spectrum Data Points	0
Number of AP Readings Taken	2
Ave Number of APs Seen at each Point	1.0
Channels Seen (% of AP Readings)	11 (100.0%)
Data Rates Seen (% of AP Readings)	54Mbps (100.0%)
Security Modes Seen (% of AP Readings)	WEP (100.0%)
Confidence Radius	5 m
Number of APs Discovered	19
Total Number of Points (Ignores AP Filter)	2
Survey Trail Length	0 m
Distance Between All Data Points	0 m
Ave Distance Between Data Points	0.00 m
Total Survey Area	57 sq m
Lat/Long of Survey Area Center	
Percentage of Survey Map Covered	100.0%

Figura 64 Vista general del AP Akros_Capacitación

La figura 65 muestra que con la reubicación del AP, las áreas de *call center* y bodega poseen una mejor cobertura de señal, permitiendo así cubrir de mejor manera todo el piso.

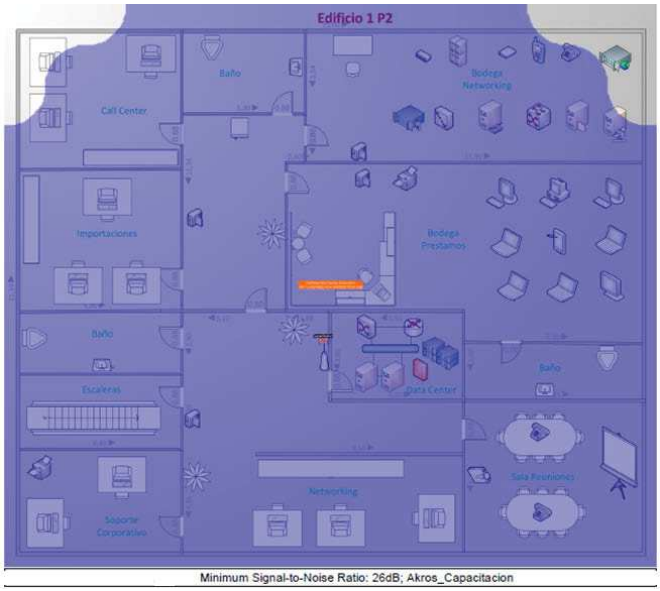


Figura 65 Mapa de cobertura del AP Akros_Capacitación

De igual manera, la figura 66 muestra que el canal 11 mejoro su cobertura en todo el piso y lo más importante no tiene interferencia con otros canales.

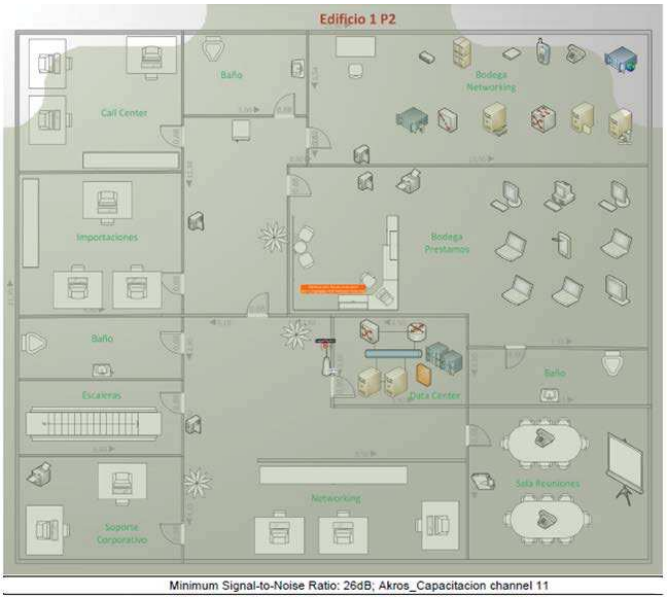


Figura 66 Mapa de canal del AP Akros_Capacitación

- **ED 2 PB**

Survey Information	
Number of Wi-Fi Data Points	4
Number of Data Points (Associated)	4
Number of Spectrum Data Points	0
Number of AP Readings Taken	7
Ave Number of APs Seen at each Point	1.8
Channels Seen (% of AP Readings)	-1 (14.3%), 1 (28.6%), 3 (57.1%)
Data Rates Seen (% of AP Readings)	54Mbps (71.4%), 144Mbps (28.6%)
Security Modes Seen (% of AP Readings)	WPA (57.1%), WPA2 (42.9%)
Confidence Radius	5 m
Number of APs Discovered	50
Total Number of Points (Ignores AP Filter)	4
Survey Trail Length	0 m
Distance Between All Data Points	23 m
Ave Distance Between Data Points	5.78 m
Total Survey Area	114 sq m
Lat/Long of Survey Area Center	
Percentage of Survey Map Covered	95.7%

Figura 67 Vista general de los AP´s Akros_Ventas y Akros_Ventas1

La figura 68 muestra que con la utilización de otro AP, la cobertura de la señal mejoro notablemente, permitiendo así tener cobertura en todo el piso.

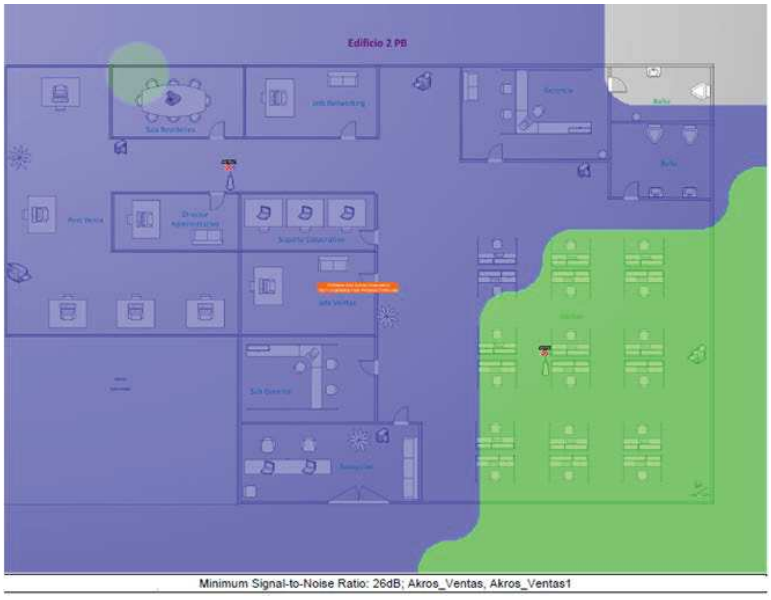


Figura 68 Mapa de cobertura de los AP´s Akros_Ventas y Akros_Ventas1

De igual manera, la figura 69 revela que el uso de un nuevo AP, permite desplegar sin problemas el uso de dos canales en el mismo piso.

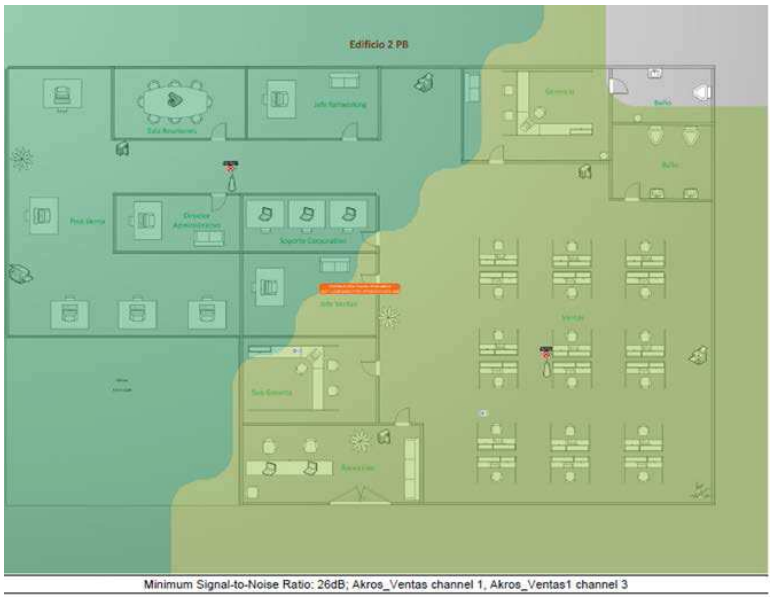


Figura 69 Mapa de canal de los AP´s Akros_Ventas y Akros_Ventas1

- **ED 2 P8**

Survey Information	
Number of Wi-Fi Data Points	2
Number of Data Points (Associated)	2
Number of Spectrum Data Points	0
Number of AP Readings Taken	2
Ave Number of APs Seen at each Point	1.0
Channels Seen (% of AP Readings)	3 (100.0%)
Data Rates Seen (% of AP Readings)	54Mbps (100.0%)
Security Modes Seen (% of AP Readings)	WPA2 (100.0%)
Confidence Radius	5 m
Number of APs Discovered	16
Total Number of Points (Ignores AP Filter)	2
Survey Trail Length	0 m
Distance Between All Data Points	0 m
Ave Distance Between Data Points	0.00 m
Total Survey Area	94 sq m
Lat/Long of Survey Area Center	
Percentage of Survey Map Covered	96.6%

Figura 70 Vista general del AP WirelessRRHH

La figura 71 demuestra que con la reubicación del AP, la cobertura de la señal abarca el área de capacitaciones sin ningún problema, permitiendo así tener cobertura en todo el piso.

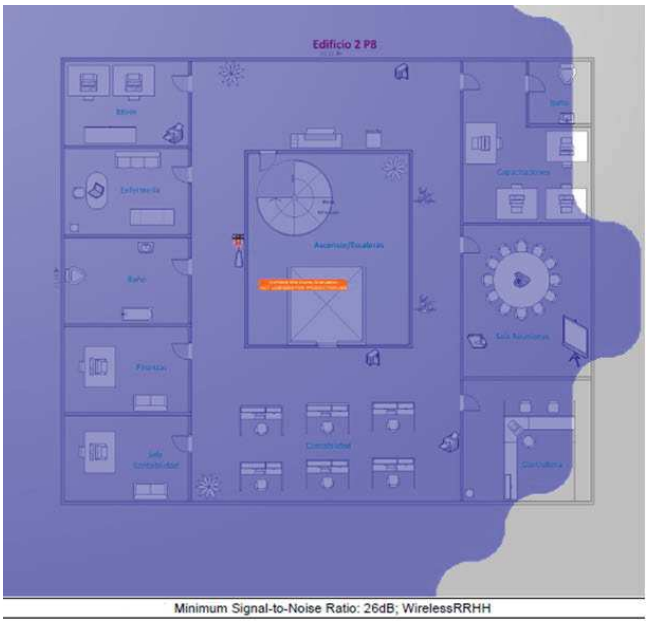


Figura 71 Mapa de cobertura del AP WirelessRRHH

De igual manera, la figura 72 muestra que el canal 3 mejoro su cobertura en todo el piso y lo más importante no tiene interferencia con otros canales.

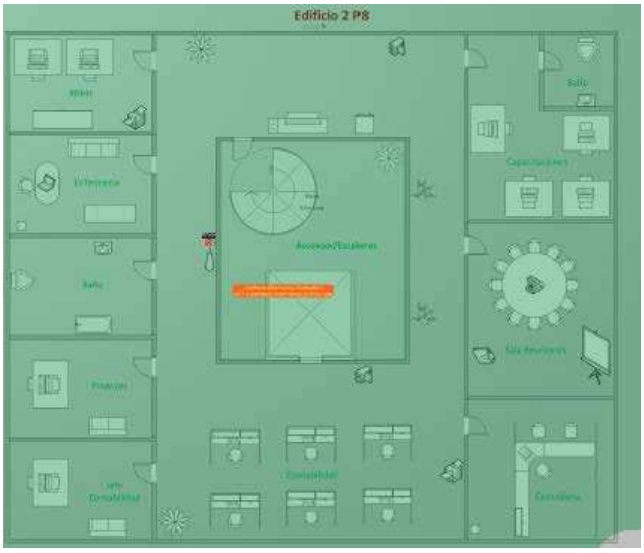


Figura 72 Mapa de canal del AP WirelessRRHH

Gracias a la utilización de esta herramienta, la cobertura en Akros puede ser mejorada notablemente, permitiendo así a los empleados trabajar desde cualquier punto de la empresa sin temor a que la cobertura inalámbrica desaparezca. A continuación, se muestra la tabla 8, en

donde se podrá comparar la cobertura de los AP's actuales con los propuestos:

Tabla 8 Tabla resumen Access Points (Visiwave)

ED 1 P2			ED 1 PB		
	Actual	**Propuesto**		**Actual**	**Propuesto**
Velocidad de datos	54 Mbps	54 Mbps	**Velocidad de datos**	54 Mbps	n/a
Seguridad	WPA2	WEP	**Seguridad**	WPA2	n/a
Canales visualizados	11	11	**Canales visualizados**	5, 11	n/a
AP's descubiertos	12	19	**AP's descubiertos**	29	n/a
Porcentaje cubierto	87.5%	100%	**Porcentaje cubierto**	95.7%	n/a

ED 2 P8			ED 2 PB		
	Actual	**Propuesto**		**Actual**	**Propuesto**
Velocidad de datos	54 Mbps	54 Mbps	**Velocidad de datos**	54 Mbps	54 Mbps
Seguridad	WPA2	WPA2	**Seguridad**	WPA	WPA, WPA2
Canales visualizados	3	3	**Canales visualizados**	3	3, 1
AP's descubiertos	31	16	**AP's descubiertos**	24	50
Porcentaje cubierto	70.7%	98.6%	**Porcentaje cubierto**	78.6%	95.7%

Como complemento para la mejora de la red inalámbrica en Akros, se puede hacer uso de un sistema centralizado para su manejo. La opción para realizar lo antes mencionado es utilizar un *wireless controller*, el cual permitirá al administrador de la red manejar de forma mucho más rápida y efectiva la señal inalámbrica, tal como se verá a continuación:

2.6.2 Wireless controller

Un controlador de WLAN es un dispositivo centralizado en la red, que normalmente se encuentra ubicado en el *data center*, al cual todos los AP´s inalámbricos de la red están conectados directa o indirectamente. Gracias a su ubicación centralizada y su gran inteligencia, el controlador inalámbrico es completamente consciente del entorno WLAN. Ofrece todos los servicios esenciales para reducir el costo de despliegue, simplificar la gestión y proporcionar múltiples capas de seguridad.

Los factores que contribuyen de manera significativa los altos costos de implementación de una red WLAN son la pre-instalación en el sitio,

encuestas (dónde colocar el AP), cablear los AP y volver a la configuración de la infraestructura de red existente, incluyendo la configuración individual de los AP´s.

El Controlador Inalámbrico que se propone implementar es el D-LINK DWC 1000, debido a su gran versatilidad con características técnicas tales como: es administrable, posee puertos a gigabit ethernet, cuenta con control de acceso mediante MAC, soporta NAT, soporta 802.1Q, descubre AP's en capa 2 y 3, etc. Además Akros es un centro autorizado de venta de productos D-link y tiene a su favor un descuento del 20%. Este *wireless controller*, tiene la capacidad de controlar hasta seis AP´s al mismo tiempo, mediante *ethernet* con un puerto POE (*power over ethernet*), lo que elimina la necesidad de obtener energía. También localiza si una señal de un AP se cruza con la de otro AP, permitiendo cambiar el canal o bajar la potencia en uno de los dos equipos, lo que conlleva a un balanceo de carga entre las señales irradiadas. El DWC-1000 posee un WIDS (*wireless instruction detection system*), el cual detecta los puntos de acceso y clientes deshonestos y anticipa las amenazas inalámbricas, evitando cualquier daño potencial y el acceso ilegal y no se requiere que los AP´s estén directamente conectados al DWC-1000.

Los AP´s se pueden implementar en cualquier lugar de la red y logran ser descubiertos y configurados por el controlador inalámbrico, el cual va a establecer los ajustes de nivel de potencia, la seguridad y el canal para optimizar el rendimiento y la cobertura sobre una base de todo el sistema.. La figura 73 muestra cómo podría quedar la implementación del *wireless controller* en red LAN de Akros:

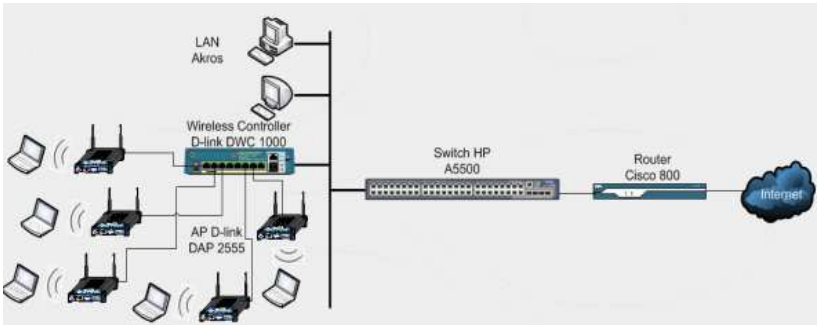


Figura 73 *Wireless controller*

Teniendo una buena distribución de señal (VisiWave) y un dispositivo centralizado (D-LINK DCW-1000) capaz de manejar todos los AP´s de mejor manera, la red inalámbrica de la empresa estaría sin ninguna duda más segura y eficiente que la actual.

CAPÍTULO III

3 Análisis de buenas prácticas y normas internacionales de telecomunicaciones, a la infraestructura de Akros

Antes de empezar el desarrollo de este capítulo, es necesario saber la definición de norma y buenas prácticas.

- *Norma.*- Una norma es un modelo, patrón, ejemplo o criterio a seguir. Comúnmente se la conoce como una fórmula que tiene valor de regla y tiene por finalidad definir las características que debe poseer un objeto. Además, una norma debe de ser aprobada previamente por un organismo normalizador reconocido.

- *Buenas prácticas.*- Se refiere al conjunto de orientaciones puestas al servicio de las instituciones que se dedican a planificar, diseñar y ejecutar actividades *e-learning* y cuyo propósito es analizar y potenciar sus procesos de trabajo de tal manera que logren ser más eficientes y obtener resultados de calidad.

Para el caso de estudio realizado en este proyecto y debido al alcance del mismo, solamente se recomendarán el uso de las normas y buenas prácticas ISO 27002, TIA-942A, TIA-569A, e ITIL las cuales se verán a continuación:

3.1 Norma ISO 27000

La ISO (organización internacional para la estandarización), es una organización no gubernamental que produce normas internacionales, industriales y comerciales con el propósito de facilitar el comercio, el intercambio de información y contribuir con unos estándares para el desarrollo y transferencia de tecnologías. Dentro de las normas ISO existe la serie 27000, que son un conjunto de estándares desarrollados que proporcionan un cuadro de gestión de la seguridad de la información empleado por cualquier tipo de organización, pública o privada, grande o pequeña.

Las normas ISO 27000, poseen varias sub normas de las cuales la más importante es la 20001, ya que aquí están los requisitos para la creación, implementación supervisión y mantenimiento de los SGSI (sistema de gestión de la seguridad de la información). En la 20001, se menciona en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002, para que sean seleccionados por organizaciones en el desarrollo de sus SGSI.

Debido al alcance de este proyecto, la ISO 27002 se convierte en una guía de buenas prácticas no certificables que podrían ser aplicadas dentro de Akros, para de esta forma ayudar a mejorar las normativas dentro de la empresa. A continuación se detallarán los puntos que de una u otra forma se serían muy útiles en Akros:

3.1.1 ISO 27002 Códigos de práctica para la gestión de la seguridad de la información

Esta norma servirá como guía práctica para el desarrollo de criterios de seguridad de la información para la empresa Akros y para las prácticas eficaces de gestión de la seguridad. En la mayoría de organizaciones la seguridad de la información no se la toma como una funcionalidad, debido a la falta de políticas disponibles para el personal de desarrollo y además en general, la seguridad informática se considera como responsabilidad del proveedor de red. La ISO 27002 no es certificable debido a que solamente realiza recomendaciones sobre el uso de la seguridad informática y solamente se harán referencia a ciertos puntos dentro de la norma los cuales podrían ser aplicados en Akros.

La seguridad de la información se define con la preservación de:

- *Confidencialidad:* Es la aseguración de la privacidad de la información de una empresa.
- *Integridad:* Garantía del estado original de los datos.
- *Disponibilidad:* Acceso cuando sea requerido por los usuarios.

Antes de comenzar el desarrollo de esta norma, se debe conocer los términos y definiciones más comunes los cuales son:

- *Activo.-* Cualquier objeto que tenga un valor para la organización o empresa.
- *Control.-* Medios para gestionar el riesgo, incluyendo políticas, procedimientos, prácticas que pueden ser de naturaleza administrativa, técnica o legal.
- *Directriz.-* Dirección que aclara lo que se debería hacer o cómo hacerlo, para alcanzar los objetivos.
- *Seguridad de la información.-* Preservación de la confidencialidad, integridad, disponibilidad de la información y el no repudio.
- *Riesgo.-* Mezcla de la probabilidad de un suceso y sus consecuencias.
- *Política.-* Toda intención y directriz expresada formalmente por la dirección.
- *Gestión de riesgo.-* Actividades sistematizadas para regir y controlar una empresa con respecto al riesgo.
- *Amenaza.-* Causa potencial de un suceso no deseado, que puede ocasionar daño a un sistema u empresa.
- *Vulnerabilidad.-* Debilidad de un archivo o grupo de activos que puede ser aprovechada por una o más amenazas.
- *Procedimiento.-* Es la manera específica de realizar una acción, y de poder desarrollar las fases sucesivas de un proceso.
- *Proceso.-* Es un conjunto de actividades o que se realizan o suceden bajo ciertas circunstancias con un fin determinado.
- *Incidencia.-* Es cualquier acontecimiento que no es parte de la operación regular de un servicio y que causa, o puede causar una interrupción.
- *Problema.-* Es el comienzo de uno o varios incidentes.

Una vez descritas las definiciones y términos más comunes, hay que definir que es un activo de la información.

- Activo de la información.- Es todo aquello que una entidad o empresa lo considera necesario, ya que contiene información de gran importancia tal como base de datos, contraseñas, números de cuenta, etc.

Para tener una idea más clara de lo que es un activo de la información, se ha desarrollado la siguiente tabla 9, en conjunto con una encuesta cuantitativa realizada al personal de TI de Akros (anexos), las cuales tuvieron como fin, medir la importancia de cada aspecto de los activos de la información que posee la empresa, tomando en cuenta la confidencialidad, disponibilidad e integridad de cada una.

Tabla 9 Activos de la información en Akros

Nombre del activo	Tipo de activo	Descripción	Importancia
Formato de visitas a clientes	Documento electrónico	Documento donde se registra la ejecución de las visitas para negociaciones con clientes.	☐ Alta ☒ Media ☐ Baja
Archivos de factibilidades técnicas	Documento electrónico	Documento utilizado para realizar propuesta técnica.	☐ Alta ☒ Media ☐ Baja
Acuerdo de confiabilidad para licitaciones	Documento electrónico y físico	Documento aplicable para clientes gubernamentales que solicitan servicio.	☒ Alta ☐ Media ☐ Baja
Propuesta técnica	Documento electrónico y físico	Documento que contiene información sobre las factibilidades técnicas indicadas por la gerencia.	☐ Alta ☒ Media ☐ Baja
Oficios de autorizaciones de descuentos	Documento físico	Documento dirigido a la gerencia comercial para autorizar descuentos	☐ Alta ☐ Media ☒ Baja
Contratos firmados	Documento físico	Documento en el cual se detallan los derechos y obligaciones entre el cliente y Akros.	☒ Alta ☐ Media ☐ Baja
Acuerdo de niveles de servicio	Documento físico	Documento que contiene los niveles de servicio.	☐ Alta ☒ Media ☐ Baja
Correo electrónico interno	Software	Medio de intercambio de información crítica entre las distintas áreas de la empresa.	☒ Alta ☐ Media ☐ Baja
Servidor de correo electrónico interno	Hardware	Es el servidor en el que funciona el servicio de correo electrónico interno.	☒ Alta ☐ Media ☐ Baja
Sistema operativo	Software	Es el sistema operativo del servidor en el cual	☒ Alta ☐ Media ☐ Baja

del servidor de correo electrónico interno		funciona el servicio de correo electrónico interno.	
Lync communicator	Software	Medio de conversación interno utilizado para realizar conferencias e intercambio de información.	☒ Alta ☐ Media ☐ Baja
Servidor del *Lync communicator*	Hardware	Es el servidor en el que funciona el servicio de *Lync communicator*.	☒ Alta ☐ Media ☐ Baja
Sistema operativo del servidor del *Lync communicator*	Software	Es el sistema operativo del servidor en el cual funciona el servicio de *Lync communicator*.	☒ Alta ☐ Media ☐ Baja
ERP	Software	Medio de planificación para recursos empresariales.	☐ Alta ☒ Media ☐ Baja
Servidor del ERP	Hardware	Es el servidor en el que funciona el servicio de ERP.	☐ Alta ☒ Media ☐ Baja
Sistema operativo del servidor del ERP	Software	Es el sistema operativo del servidor en el cual funciona el servicio de ERP.	☐ Alta ☒ Media ☐ Baja
CRM	Software	Medio de administración basada en la relación con clientes.	☐ Alta ☒ Media ☐ Baja
Servidor del CRM	Hardware	Es el servidor en el que funciona el servicio de CRM.	☐ Alta ☒ Media ☐ Baja
Sistema operativo del servidor del CRM	Software	Es el sistema operativo del servidor en el cual funciona el servicio de CRM.	☐ Alta ☒ Media ☐ Baja
GP	Software	Medio de solución de gestión empresarial.	☐ Alta ☒ Media ☐ Baja
Servidor del GP	Hardware	Es el servidor en el que funciona el servicio de GP.	☐ Alta ☒ Media ☐ Baja
Sistema operativo del servidor del GP	Software	Es el sistema operativo del servidor en el cual funciona el servicio de GP.	☐ Alta ☒ Media ☐ Baja
Equipos de comunicación de red	Switches	Equipos (switch) que permiten segmentar una red.	☒ Alta ☐ Media ☐ Baja
Equipos de comunicación de red	Servidores	Equipos (servidores) que permiten el manejo de So y aplicaciones en su interior.	☒ Alta ☐ Media ☐ Baja
Equipos de comunicación de red	PC's	Equipos (pc) que permiten el manejo de varios aplicativos.	☒ Alta ☐ Media ☐ Baja
File server	Software	Ubicación en donde se encuentran almacenados los archivos compartidos de Akros.	☐ Alta ☐ Media ☒ Baja
Acta de entrega-recepción de equipos	Documento electrónico y físico	Documento de conformidad en donde consta la entrega de equipos a personal tanto interno como externo.	☐ Alta ☐ Media ☒ Baja
Archivo maestro de IP's (Excel)	Documento electrónico	Documento que contiene las direcciones IP de toda la empresa.	☒ Alta ☐ Media ☐ Baja
Backup de configuración de equipos	Documento electrónico	Son las copias de respaldo (backup) que almacenan la información de la configuración de los equipos de comunicación de red que se utilizan para la prestación de servicios	☒ Alta ☐ Media ☐ Baja

Tanto en anexos, como en la tabla 9, los activos de la información forman una parte muy importante en Akros y hay que tomarlos muy en cuenta, ya que sin ellos sería muy difícil no solo continuar con la red operativa, sino también con todo el negocio en general.

Finalmente los siguientes puntos abarcan los “códigos de práctica para la gestión de la seguridad de la información” y son:

- *Consideraciones de la seguridad de la información con terceras personas.*- El objetivo es llegar a un acuerdo entre Akros y las terceras personas (clientes), sin existir malos entendidos. Los puntos más relevantes a tratar son:
    - Procedimientos para proteger los archivos de la organización, incluyendo información, *software* y *hardware*.
    - Controles para asegurar la protección contra *software* malicioso.
    - Procedimientos para validar si alguna vez se ha puesto en peligro los activos.
    - Controles para asegurar la devolución o la destrucción de información y los activos al finalizar un acuerdo.
    - Restricciones de la copia y la divulgación de información.
    - Asegurar la concienciación al usuario sobre las responsabilidades y aspectos de la seguridad de la información.
    - Realizar un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes de la finalización de los acuerdos.

- *Responsabilidad por los activos.*- El propósito es lograr mantener la protección adecuada de los activos que posee Akros. Los puntos más relevantes a tratar son:
    - Definir y revisar periódicamente las restricciones y clasificaciones del acceso.

- Definir el uso del correo electrónico y de internet.
- Definir el uso de los dispositivos móviles, especialmente fuera de la empresa.
- Elaborar un proceso para el etiquetado y manejo de los activos.
- Documentar e identificar todos los activos ya sean estos físicos (equipos) o intangibles (reputación e imagen).

➢ *Seguridad física.-* Su objetivo es evitar el acceso físico no autorizado, el daño o la inferencia a las instalaciones y a la información de Akros. Los puntos más relevantes a tratar son:

- Definir claramente los perímetros de seguridad con sus respectivas ubicaciones.
- Establecer un área de recepción con personal para poder controlar el acceso físico al lugar.
- Colocar sistema biométrico en las puertas, para controlar el acceso de personal no autorizado.
- Instalar sistemas de seguridad ya sean CCTV o alarmas para salvaguardar la integridad de un área restringida.
- Los servicios de procesamiento de información (*data centers*, *service desk*, etc) deberían estar físicamente separados de aquellos dirigidos por terceras personas.
- Se debe poseer un registro con fecha y hora para el ingreso o salida del personal de las áreas de alta sensibilidad para la empresa.
- Retirar o bloquear inmediatamente los derechos de acceso a los usuarios que cambien de función o dejen la empresa.
- Tener sistemas de incendios probados periódicamente, para evitar problemas al momento de un siniestro real.
- Exigir a los usuarios firmar declaraciones que indiquen que ellos entienden las condiciones del acceso.

- *Seguridad de equipos.-* El objetivo es evitar la pérdida, daño, robo o puesta en peligro de los activos de que posee Akros. Los puntos más relevantes a tratar son:
    - Los equipos informáticos se deberían ubicar de tal modo que se logre minimizar el acceso innecesario a las áreas de trabajo.
    - Los equipos que manejen información sensible, deberían estar ubicados de tal forma que se reduzca el riesgo de visualización de la información por personas no autorizadas.
    - Los equipos que requieran protección especial (*networking*) deberían estar aislados físicamente para reducir el nivel general de protección de los demás equipos.
    - Establecer reglas para no comer, beber, fumar en las cercanías de los equipos.
    - Es conveniente monitorear las condiciones ambientales ya sea humedad, calor frio para un óptimo funcionamiento de los equipos.
    - Aplicar protección contra rayos, para minimizar el sobre voltaje en los equipos.

- *Seguridad del cableado.-* Su objetivo es brindar seguridad en el cableado eléctrico y de telecomunicación el cual transporta datos. Los puntos más relevantes a tratar son:
    - Las líneas de energía eléctrica y de telecomunicación deberían ser subterráneas, cuando sea posible, o tener protección alterna adecuada.
    - El cableado de red debería estar protegido contra interceptación no autorizada o daño, por ejemplo utilizando conductos y evitando rutas por áreas públicas.
    - Los cables de energía deberían estar separados de los cables de telecomunicación para evitar interferencias.
    - Se debe identificar todos los cables, para evitar errores de manejo.

- Es recomendable utilizar un plano del cableado para evitar errores.
- Uso de blindaje para el cableado, para evitar interferencias o daños.
- Acceso controlado a los *patch panel*.
- Busca rutinaria por parte de los técnicos, para verificar que ningún equipo externo esté conectado al cableado.

➢ *Seguridad de los medios de almacenamiento.*- Su objetivo consiste en preservar la información confidencial de Akros, evitando la copia mediante dispositivos de almacenamiento. Se debe tener en cuenta las siguiente sugerencias:

- La categorización e identificación de los medios de almacenamiento, va acorde al propósito por el cual se respalda.
- Es totalmente prohibido para los usuarios de la red el intervenir con las labores de respaldo del personal de informática.
- Bajo ninguna circunstancia se dejarán sin custodia los medios de almacenamiento, o copias de seguridad de los sistemas.
- Todo medio de almacenamiento deberá ser documentado e inventariado en un registro específico.
- La ubicación física de los medios de almacenamiento deberá estar lejos del polvo, humedad, o cualquier contacto con material o químicos.
- La llave de seguridad que pertenece a los medios de almacenamiento debe estar bajo supervisión de la gerencia.

➢ *Mantenimiento de equipos.*- El objetivo principal es mantener a los equipos en óptimo funcionamiento, realizando periódicamente mantenimientos correctivos y preventivos dentro y fuera de Akros. Los puntos más relevantes a tratar son:

- Los mantenimientos deberán estar acorde con los intervalos y descripciones del proveedor.

- Solamente personal de mantenimiento previamente calificado, debería realizar esta actividad.
- Mantener registro de todas las fallas reales o sospechosas encontradas durante el mantenimiento.
- Retirar partes sensibles (discos duras, ventiladores, memorias) durante la ejecución del mantenimiento.
- Si el equipo llega a salir de la empresa debido a su respectivo mantenimiento, por ningún motivo se lo debe dejar sin custodia.

➢ *Monitoreo.-* Su objetivo es detectar actividades de procesamiento de la información no autorizada dentro de Akros. Los puntos más relevantes a tratar son:

- Identificar el ID del usuario.
- Identificar fecha, hora y detalles de los registros de inicio y de cierre.
- Registrar ubicación del *host.*
- Registrar los intentos aceptados o rechazados de ingreso al sistema.
- Chequear cambios en la configuración del sistema.
- Chequear el uso de privilegios.
- Registrar el acceso a páginas web.
- Revisar los registros de fallas para garantizar que estas se han resuelto eficazmente.
- Identificar fecha, hora en la ocurrió determinada falla.

➢ *Contraseñas para usuarios.-* Su objetivo es controlar el uso debido de contraseñas por parte de los usuarios de Akros. Los puntos más relevantes a tratar son:

- Exigir a los usuarios firmar una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo.

- Suministrar una contraseña temporal a un usuario, cuando es nuevo o cambio de área en una empresa.
- Las contraseñas temporales, deben ser entregadas personalmente, nunca ser enviadas por correo u otros medios de comunicación.
- Las contraseñas temporales, deben ser cambiadas inmediatamente por el usuario.
- Validar la identificación de un individuo, antes de entregarle una contraseña.
- Los usuarios deberían confirmar las entregas de las contraseñas.
- Las contraseñas nunca deben ser almacenadas dentro de un computador sin contar con un formato de protección.
- No utilizar las mismas contraseñas de la empresa para propósitos personales.
- No incluir contraseñas en ningún proceso de registro automático.

➢ *Control de acceso a las redes.-* Su objetivo es evitar el acceso no autorizado a los servicios en red de Akros. Los puntos más relevantes a tratar son:

- Determinar a quien se le permite el acceso a determinada red y a los servicios de red.
- Proteger el acceso a las conexiones de red y a los servicios de red.
- Controlar el ingreso de los medios utilizados para acceder a las redes, por ejemplo, las condiciones para permitir el acceso a la marcación a un ISP o a un sistema remoto.
- Crear dominios de red tanto internos como externos, para dividir la red y mantenerla protegida.
- Utilizar una VPN (red privada virtual) para conexiones externas hacia la red de la empresa.

- Limitar el tiempo de conexión a escritorio remoto, fuera de horario de oficina.
- Considerar la repetición de la autenticación a intervalos determinados.

➢ *Control del software operativo.-* Su objetivo es garantizar la seguridad de los archivos del sistema operativo que posee Akros, así como también evitar la degradación del mismo. Los puntos más relevantes a tratar son:

- La actualización del sistema operativo, solo debe ser realizada por administradores capacitados y con la debida autorización de la dirección.
- Los sistemas operativos solo deben contener códigos ejecutables aprobados y no códigos en desarrollo ni compiladores.
- El *software* de las aplicaciones y el sistema operativo, solo se deberían implementar después de realizar pruebas y ensayos.
- Se debería utilizar un sistema de configuración para mantener el control del sistema operativo.
- Poseer una estrategia de restauración del sistema operativo, en caso de que falle o al momento de aplicar algún cambio.
- Conservar un registro para auditoria de toda actualización o cambio dentro del sistema operativo.

➢ *Fuga de información.-* El objetivo es evitar las oportunidades para que se produzca fuga de información dentro de Akros. Los puntos más relevantes a tratar son:

- Se debe explorar los medios de salida de comunicación frecuentemente, para determinar si existe información oculta.
- Utilización de *software* especial para identificar la integridad de la información.
- Monitoreo regular de las actividades del personal y del sistema.

- Monitorear el uso de los recursos en los sistemas del computador.

➢ *Directrices para los procedimientos de los incidentes.*- Su objetivo es manejar los diferentes tipos de incidentes de seguridad de la información de la mejor manera en Akros. Los incidentes se generan si se producen:

- Fallas en el sistema de información y pérdida del servicio.
- Existen códigos maliciosos.
- Hay denegación de servicio.
- Existen errores producidos por datos de la empresa, incompletos o inexactos.
- Existe violación de la confidencialidad y la integridad.
- Existe uso inadecuado de los sistemas de la información.

➢ *Cumplimiento con las políticas y las normas de la seguridad de la información.*- Su objetivo es asegurar que los sistemas cumplan con las normativas y políticas de Akros. Si se halla algún incumplimiento como resultado de la revisión, Akros debería:

- Determinar la causa del incumplimiento.
- Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.
- Determinar e implementar la acción correctiva apropiada.
- Revisar la acción correctiva que se ejecutó.

➢ *Capacitación de usuarios.*- Su objetivo capacitar a los empleados en cuestiones de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan. Tomar en cuenta todas las medidas de seguridad necesarias, antes de proceder a una capacitación al personal interno o externo del establecimiento, siempre y cuando se vea implicada la utilización de los servicios de red o se exponga material de importancia

considerable para el establecimiento. Los empleados en Akros deben saber:

- Utilizar de forma segura las aplicaciones corporativas.
- Utilizar de forma segura los servicios que hayan sido autorizados de internet.
- Como evitar la entrada de virus y otros códigos dañinos.
- Reconocer las técnicas más frecuentes de ingeniería social, para evitar ser víctimas de este tipo de engaños.
- Conocimiento de sus obligaciones y responsabilidades derivadas del actual marco normativo.
- Como gestionar los soportes informáticos, los equipos y los dispositivos portátiles.
- Como reaccionar ante determinados incidentes que puedan comprometer la seguridad de la información o el acceso a los recursos del sistema.

➢ *Vinculación de personal.-* Su objetivo es proveer un mecanismo de seguridad, analizando el perfil del nuevo empleado, para prevenir que el mismo pueda hacer daño importante a Akros. Hay que tomar en cuenta lo siguiente:

- Antes de realizar la vinculación de personal nuevo se deben conocer sus antecedentes, referencias personales y laborales, con el fin de determinar que no genera una amenaza para la empresa.
- El contrato de vinculación debe incluir cláusulas de confidencialidad asociadas a la protección de la información y a los delitos contenidos en la ley.
- Asignar un usuario al nuevo personal junto con una contraseña que el usuario pueda cambiar.
- Delimitar y estratificar la información de acuerdo a la información requerida para las actividades del cargo.

- Si es posible se asignará un equipo al nuevo personal, con el fin de conocer los usos que le da a los recursos de la empresa.
- Si es posible asignación de una cuenta de correo electrónico empresarial, que le permita al empresario filtrar la información que pueden compartir sus empleados.
- El contrato de vinculación debe informar en qué condiciones se auditara el correo electrónico institucional del empleado.
- Informar a los empleados que el acceso a internet solo estará disponible a fines profesionales
- Notificar los derechos, responsabilidades y deberes que asumen en cada cargo en cuanto a la seguridad del equipo y la información contenida en este.

Como se pudo constatar, la norma ISO 27002 son normativas y guías para mejores prácticas informáticas para la seguridad de la información, las cuales son factibles a ser implementadas en Akros. A continuación, se presenta una tabla matriz “causa-efecto”, de los posibles problemas que se podrían generar dentro de la empresa si no se enfatiza en el uso de la seguridad de la información.

Tabla 10 Matriz causa-efecto

Formulación del problema	Objetivo	Conjeturas
¿Cuáles normas de seguridad de la información se están empleando en Akros, para proteger la disponibilidad, integridad y confidencialidad de los activos de la información?	Impedir accesos no autorizados para evitar violaciones a las, normas, políticas y procedimientos de la gestión de la seguridad de la información en la empresa Akros. El cumplimiento de todas estas funciones debe ser observado por todo el personal técnico de la organización.	El no tener implementadas normas internacionales de seguridad de la información dentro de la organización, podrá provocar fuga de información, infecciones en la red, falta de control sobre los SO, etc.
¿Qué consecuencias se producen con la falta de seguridad de la información en Akros?	Comprender toda la protección de la información contra acceso, modificación o divulgación no autorizada, así como también asegurar la disponibilidad de la información.	La falta de normas de seguridad en Akros, trae como consecuencia que los riesgos asociados a los activos de información causen daños al realizar las operaciones.
¿Qué seguridades existen con respecto a los sistemas de información desarrollados o adquiridos por Akros?	Promover las mejores prácticas de seguridad al desarrollo o adquisición de sistemas de información.	Proporcionar demasiada información al generarse errores en los sistemas de Akros, podrían causar pistas para un posible hackeo de la red.

¿Cómo podría mejorar la seguridad de la información que se maneja en Akros?	Implementar y concientizar el uso de las normas de seguridad de la información a los usuarios finales para la protección de los activos de la información.	Controlar el cumplimiento de las políticas de seguridad de la información para la protección de los activos de la información.

Analizando la matriz “causa-efecto”, sin duda la red en Akros estará mucho más segura y disponible, no solamente de ataques externos sino también internos y además los equipos podrán estar mucho más funcionales ya que se los verifica periódicamente. Finalmente la siguiente tabla 11 muestra el *checklist* diseñado el cual podría servir para constatar el uso de la ISO 27002 en Akros:

Tabla 11 *Checklist* ISO 27002

ISO 27002 Codigos de practica para la gestion de la seguridad de la informacion															
SGSI terceras personas	Responsabilidad por los activos	Seguridad fisica	Seguridad de equipos	Seguridad cableado	Seguridad de los medios de almacenamiento	Mantenimiento de equipos	Monitoreo	Contraseñas para usuario	Control de acceso a las redes	Control de software operativo	Fuga de información	Directrices para los procedimientos de los incidentes	Cumplimineto de politicas y normas de los SGSI	Capacitacion de usuarios	Vinculación de personal
Protección de archivos	*Revisar periodicamente las restricciones de acceso*	*Definir perimetros de seguridad*	*Colocar los equipos para minimizar el acceso a las areas de trabajo*	*Lineas soterradas de energia y telecomunicaciones*	*Clasificación e identificación de los medios de almacenamiento*	*Mantenimiento de acuerdo al proveedor*	*Identificación del ID del usuario*	*Declaración firmada de confidencialidad de contraseña*	*Acceso limitado a usuarios a la red*	*Actualización del SO realizado por personal calificado*	*Explotación de los medios de salida de comunicación*	*Fallas en el sistema de información*	*Determinación de la causa del incumplimiento*	*Utilización de aplicaciones corporativas*	*Reconocimiento de antecedentes del nuevo personal*
Protección software malicioso	*Uso del Mail e Internet*	*Establecer un area de recepcion para control de acceso fisico*	*Reducción de visualización*	*Cableado protegido contra interceptación*	*No intervención en labores de respaldo*	*Personal calificado realiza el mantenimiento*	*Identificación fecha y hora de inicio y cierre de sesion*	*Suministrar contraseña temporal a un usuario*	*Protección de acceso a las conexiones de red*	*SO contiene codigos ejecutables aprobados*	*Identificación de la integridad de la información*	*Existencia de codigos maliciosos*	*Garantización que no existan incumplimientos*	*Utilización segura de servicios de internet*	*Firma de contrato de confidencialidad de la información*
Validación puesta de peligros de archivos	*Uso de dispositivos moviles fuera de la empresa*	*Colocación del sistema biometrico en puertas*	*Equipos de Networking deben estar aislados*	*Cables de energia y telecomunicación separados*	*Control sobre medios de almacenamiento*	*Registro de fallas durante el mantenimiento*	*Registro de ubicación del host*	*Contraseña temporal entregada personalmente*	*Controlar el acceso de los medios para accesar a la red*	*Software del SO debidamente probado*	*Monitoreo regular de las actividades del personal*	*Existencia de denegación de servicio*	*Implementación de acciones correctivas apropiadas*	*Evitar la entrada de virus y codigos dañinos*	*Asignar nueva contraseña al nuevo usuario*
Validación destrucción de información	*Proceso para el etiquetado y manejo de activos*	*Instalación de CCTV o alarmas*	*Prohibición de comidas y bebidas dentro de las instalaciones sensibles*	*Etiquetación del cableado*	*Protección contra el polvo y humedad*	*Retiro de partes sencibles durante el mantenimiento*	*Registro de intentos aceptados y fallidos*	*Cambio de contraseña temporal*	*Creación de dominios de red*	*Utilización del sistema de configuración*	*Monitoreo de recursos del computador*	*Errores producidos por datos incompletos*	*Revisión de la acción correctiva ejecutada*	*Reconocimiento de ingeniería social para evitar engaños*	*Delimitar la información de acuerdo a las actividades*
Restriccion para divulgar información	*Identificación de todos los activos*	*Cuartos de equipos separados de terceras personas*	*Monitoreo de las condiciones ambientales*	*Utilización de plano del cableado*	*Los medios de almacenamiento estan guardados*	*No dejar solo el equipo si sale fuera de la empresa*	*Chequeo de cambios en la configuración del sistema*	*Validación de ID del usuario previa entrega de la contraseña*	*Utilización de VPN*	*Estrategia de restauración del sistema*		*Violación de la integridad y confidencialidad*		*Conocimiento de las obligaciones y responsabilidades*	*Asignación de nuevo equipo*
Concienciación al usuario sobre el uso del SGSI		*Registro de personal en areas sencibles*	*Protección contra rayos*	*Uso de blindaje del cableado*			*Registro de la activación o desactivación del firewall*	*No almacenar contraseñas dentro de un computador sin protección*	*Implementación de un firewall para control de acceso a la red*	*Conservación de registro de actualizaciones del SO*		*Uso inadecuado de los sistemas de información*		*Gestionamiento de los soportes informaticos*	*Asignación de una cuenta de correo empresarial*
Plan de contingencia para terminar acuerdos		*Uso de ID a empleados o visitantes*		*Acceso controlado a los Patch panel*			*Registro a paginas web*	*No utilizar contraseñas de la empresa con propósitos personalmente*	*Limitación de tiempo de conexión al escritorio remoto*					*Capacitación en caso de incidentes*	*El contrato debe contener auditorias frecuentes de la cuenta de correo*
		Retirar derechos de acceso a usuarios que cambian de función		*Verificación diaria sobre posibles conexiones no autorizadas*			*Revisión de registros de fallas*	*No incluir contraseñas en procesos de registro automaticos*	*Repetición en la autenticación en intervalos repetitivos*						*Informar que el internet solo es para uso laboral*
		Funcionalidad de sistemas de incendios					*Identificación de fechas y hora cuando se produce una falla*								*Informar la responsabilidad que tienen sobre los equipos asignados*
		Firma de declaraciones a los usuarios sobre las condicciones de acceso													

3.2 Introducción a las normas TIA

La TIA (asociación de la industria de las telecomunicaciones) está acreditada por el ANSI (instituto nacional americano de estándares) para desarrollar estándares industriales para una amplia variedad de tecnologías de la información y la comunicación (TIC). Las normas TIA y el departamento de tecnología desarrollan guías para los equipos de radio privada, torres de celulares, terminales de datos, satélites, equipos de terminal telefónico, la accesibilidad, dispositivos de VOIP, cableado estructurado, *data center*, etc.

Para este proyecto se harán mención a los estándares TIA-942A y TIA-569A, debido a que están relacionados con temas tales como cableado estructurado y *data center*. A continuación, se desarrollará cada uno de los estándares antes mencionados con el propósito de darlos a conocer y analizar lo que se podría llegar a implementar en la empresa Akros.

3.2.1 TIA-942A Estándar para *data centers*

Este estándar se basa en normas y procedimientos que un cuarto de equipos (*data center*) debería poseer, para que de esta manera el mismo pueda brindar un mejor desempeño. Dentro del mundo de la TI, existen algunas propiedades exclusivas de la información tales como la confidencialidad, disponibilidad e integridad, las mismas que deben asegurar la continuidad de las operaciones.

Trasladada estas propiedades al campo de acción del *data center*, se debe considerar a este como la interrelación de una serie de subsistemas que dan respaldo al equipamiento importante, para mantener una disponibilidad de sistemas acorde a las características propias del negocio.

Existen cuatro niveles de *tiers* que plantea el estándar TIA-942A corresponden a los cuatro niveles de disponibilidad, teniendo que a mayor número de *tier* mayor disponibilidad, lo que implica también mayores costos constructivos. Esta clasificación es aplicable en forma

independiente a cada uno de los subsistemas de infraestructura (telecomunicaciones, arquitectura, eléctrica y mecánica). Se debe tener en cuenta que la clasificación global del *data center* será igual a la de aquel subsistema que tenga el menor número de *tier*. Esto significa que si un *data center* tiene todos los subsistemas *tier* IV excepto el eléctrico que es *Tier* III, la clasificación global será *tier* III. Los tipos de *tiers* antes mencionados son los siguientes:

- *Tier I Data center básico.*- Un *data center tier* I puede ser susceptible a interrupciones coordinadas como no coordinadas. Posee sistemas de climatización y distribución de energía, pero puede o no tener piso falso, UPS o generador eléctrico, si los tiene pueden estos no tener redundancia y existir varios puntos falla. La carga máxima de los sistemas en escenarios críticos es del 100%. Esta clase de *data center* puede estar fuera de servicio por lo menos una vez al año por razones de mantenimiento y/o reparaciones. En caso de problemas más críticos se pueden programar paradas más frecuentes y errores de operación o fallas en los componentes de su infraestructura los mismos que causarán la detención del *data center*. La tasa de disponibilidad máxima del *data center* es 99.67%.

- *Tier II Componentes redundantes.*- Son un poco menos susceptibles a interrupciones, tanto planeadas como no planeadas. Estos *data centers* poseen piso falso, UPS+1 y un generador eléctrico, pero solamente están vinculados a una sola línea de distribución eléctrica. Su diseño cuenta con componentes básicos más uno de respaldo (N+1). La carga máxima de los sistemas en situaciones de riesgo es del 100%. El mantenimiento en sus componentes de infraestructura pueden causar una interrupción del procesamiento. La tasa de disponibilidad máxima del *data center* es 99.74%.

- *Tier III Mantenimiento concurrente.-* Las capacidades de un *data center* de este dimensión, permiten ejecutar cualquier actividad planeada sobre cualquier componente sin interrupciones en su actividad. Esto puede incluir mantenimiento preventivo y programado, reparaciones o reemplazo de partes. Para infraestructuras que manejan sistemas de enfriamiento por agua, significa que poseen doble ducto de tuberías. Además debe existir suficiente capacidad y doble línea de distribución de los componentes. La carga máxima en los sistemas en situaciones de riesgo es de 90%. Muchos de los *data centers tier* III son prediseñados para poder ser actualizados a *tier* IV, cuando las exigencias de la compañía justifiquen el costo. La tasa de disponibilidad máxima del *data center* es 99.98%.

- *Tier IV Tolerante a fallas.-* Estos *data center* suministran la capacidad para ejecutar cualquier acción proyectada sin interrupciones en las cargas críticas, y además poseen un sistema tolerante a fallas que otorga a la infraestructura continuidad de operación aun ante cualquier evento crítico no planeado. Esto demanda dos líneas de distribución simultáneamente activas, esto significa dos sistemas de UPS independientes, cada sistema con un nivel de redundancia N+1. La carga máxima de los sistemas en situaciones de riesgo es de 90%. La tasa de disponibilidad máxima del *data center* es 99.99%.

La tabla 12 detalla los tiempos y la disponibilidad (SLA) de cada *tier* según la norma TIA-942A:

Tabla 12 Tiempos de cobertura

Tier	% Disponibilidad	% de Parada	Tiempo de parada anual
Tier I	99,67%	0,33%	28,82 horas
Tier II	99,74%	0,25%	22,68 horas
Tier III	99,98%	0,02%	1,57 horas
Tier IV	99,995%	0,01%	52,26 minutos

Los cuatro niveles de tiers descritos anteriormente, van de la mano con los subsistemas de infraestructura de telecomunicaciones, arquitectura, eléctrica y mecánica, los cuales serán descritos en la siguiente tabla 13:

Tabla 13 *Tiers* y subsistemas de infraestructura

	Telecomunicaciones	Arquitectura	Eléctrica	Mecánica
***Tier* I**	* Un solo proveedor, una sola ruta de cableado.	* Sin protección a eventos físicos, naturales o intencionales.	* Piso falso (opcional). *UPS sin redundancia. * El UPS debe contar con bypass para mantenimiento. * PDUs y paneles de distribución utilizados para distribución de la carga. * Sistemas de tierra. * El monitoreo de los sistemas es opcional.	* Una o varias unidades de aire acondicionado sin redundancia. * Tuberías con una sola ruta.
Tier II	* Redundancia en equipos críticos, fuentes de poder, procesadores.	* Protección mínima a eventos críticos. * Puerta de seguridad.	* UPS redundante N+1. *Un generador. * PDUs redundantes, preferiblemente alimentados de sistemas UPS separados. * Gabinetes deben de contar con dos circuitos eléctricos dedicados de 20A/120V. * *Emergency Power Off System* (EPO).	* Capacidad de enfriamiento combinada, temperatura y humedad 7 x 24 x 365.
Tier III	* Dos proveedores, dos cuartos de entrada de servicio.	* Acceso controlado (Sistema Biométrico). * Muros exteriores sin ventanas. * Seguridad perimetral, CCTV.	* Al menos redundancia N+1 en el generador. * UPS y sistema de distribución. * Dos vías de distribución (una activa y otra alterna). * Sistema de aterrizaje y sistema de protección para alumbrado. * Sistema de Control para monitorear la mayoría de los equipos eléctricos. * Servidor redundante para asegurar monitoreo y control continuo.	* Múltiples unidades de aire acondicionado. * Tuberías y bombas duales. * Detección de derrames.
Tier IV	* Áreas aisladas.	* Protección desastres naturales, sismos, inundaciones, huracanes. * Edificio separado. * Cercanía a lugares públicos (Aeropuertos, Líneas Férreas). * Requerimientos antisísmicos según la zona.	* Diseño 2(N+1). * Un sistema de monitoreo de baterías. * UPS deben poseer un bypass manual para mantenimiento o falla. * Data Center debe poseer una entrada de servicios dedicada, aislada de preferencia. * Dos alimentaciones de diferentes subestaciones (2 activas simultáneamente). * Detección y transferencia automática.	* Soporta fallas en un tablero de alimentación. * Fuentes de agua alternas.

Definiendo ya los niveles de *tiers* y los subsistemas de infraestructura y basados en las normas de instalación para equipos dentro y fuera de un

data center aplicados por la TIA-942A, se ha propuesto la siguiente tabla 14 para poder normar la instalación de los diferentes componentes que podrían ser utilizados en el *data center* de Akros.

Tabla 14 Normas de instalación para equipos en el DC de Akros

Rack	Generador	UPS	PDU	Climatización
Altura máxima 2.4m, preferiblemente 2.1m.	Alimentar los sistemas de A/C.	Suficiente tiempo de respaldo para que se encienda el Generador.	Transformador de aislamiento.	Se recomienda una humedad relativa de 45% con variantes de más menos 5%.
No se debe dejar espacios vacíos dentro del Rack, ya que aquí se pueden mezclar aires fríos con calientes, lo que se traduce en un Rack poco eficiente.	Instalar TVSS (*Transient Voltage Surge Supressors)* en la salida.	Respaldo entre 5 a 30 minutos en baterías.	Supresor de transientes.	Es necesario un aire acondicionado de precisión no de confort, ya que este extrae de 5% a 15% de humedad, lo que permite que un Data center tenga la humedad necesaria para que no se torne muy seco, lo que podría generar estática en el ambiente.
Deben contar con al menos 82cm de espacio libre para trabajos al frente y detrás.	Combustible preferiblemente diésel, permite un arranque más rápido que con gas natural.	*Tier* IV debe contar con un sistema Dual Bus con UPS Redundantes.	Paneles de distribución.	No obstruir las entradas y salidas de aire en los compartimientos para no crear desequilibrio en la climatización.
El rack debe ser perforado para permitir la ventilación del mismo.	Sistema remoto de monitoreo y alarmas para el sistema de almacenaje de combustible.	El cuarto de UPS y Baterías deben contar con un Aire acondicionado de precisión (PAC).	Monitoreo (local y remoto).	Poseer el Data center lo más limpio posible para evitar problemas con el polvo y suciedad en los equipos.
Regletas al menos una de 120V, 20A.			EPO (*Emergency Power Off)*.	
Deben contar con control de acceso.				
Profundidad de 1.0 a 1.1 m.				
42U de espacio mínimo.				

Amanera de análisis, después de todo el material presentado, teniendo en cuenta la capacidad del negocio y el costo elevado de poseer un *data center tier* III o *tier* IV, Akros podría sustentarse con un data center *tier* II, cubriendo primeramente los requerimientos que esto amerita tales como:

- Protección mínima contra eventos críticos.
- Puerta de seguridad.

- UPS+1.
- Generador.
- PDU+1.
- *Emergency power off* (EPO).

De esta forma se mejorará la redundancia de equipos y la seguridad física del sitio. Gracias al apoyo del TI de Akros, ya se están cumpliendo varios de los requerimientos que se piden para poder ser un data center *tier* II, tales como:

- Redundancia en equipos críticos, fuentes de poder, procesadores.
- Gabinetes con dos circuitos eléctricos dedicados 20A/120V.
- Capacidad de enfriamiento combinada, temperatura y humedad 7X24X365.
- Rack de 42U perforado para aumentar el enfriamiento.
- Equipos alineados frontalmente para mejorar la climatización.
- Suficiente tiempo en baterías de UPS.

A pesar de estas mejoras aún faltan algunas más, que se tendrán en cuenta para renovaciones futuras a mediano plazo, dependiendo de su costo y productividad.

3.2.2 TIA-569A Normas de recorridos y espacios en telecomunicaciones en edificios comerciales

Describe los elementos de diseño para trayectos (ducterías) y cuartos dedicados a equipos de telecomunicaciones. Esta norma no cumple los aspectos de seguridad en el diseño del edificio, se limita a los aspectos de telecomunicaciones en el diseño y construcción de edificios comerciales. Esto puede ser muy útil para el futuro de Akros, ya que a medida que crece la empresa se pueden crear sucursales y/o mejoramientos en la estructura física actual.

La TIA-942A trata de estandarizar las prácticas de diseño y construcción específicos los cuales darán soporte a los medios de transmisión y al equipo de comunicaciones. Entre sus principales componentes se tiene:

- *Bandejas metálicas bajo el piso falso.-* Consiste en la distribución de bandejas metálicas empotradas bajo el piso falso, en profundidad de 2.5” y 4”. Poseen forma rectangular y vienen en varios tamaños, sencillas, dobles o triples. La figuras 74 y 75 muestran dos tipos de canaletas metálicas:

Figura 74 Bandeja metálica

Figura 75 Bandeja metálica perforada

Tomados de: http://www.construnario.com/catalogo/pequeno-material-electrico-sa-pemsa/productos

- *Tubo Conduit.-* Es un tubo galvanizado para instalaciones eléctricas expuestas a agentes dañinos (figura 76). Existe un componente que se utiliza a la par que es la caja de registro, utilizada para localizar los cables (figura 77). Entre sus características se debe respetar lo siguiente:

- Un *Conduit* se debe utilizar si las localizaciones de salidas son permanentes, la densidad del cableado es baja y no se requiere flexibilidad (PVC rígido).
- No debe servir a más de tres salidas.
- Ninguna sección deberá ser mayor a 30 m o contener más de dos ángulos de 90° sin un registro.
- La canalización mediante tubo *conduit* con un diámetro mayor deberán tener un diámetro de curvatura de, al menos, 10 veces su diámetro interno.
- El tamaño de la caja de registro debe ser ocho veces mayor al tubo *conduit*.
- La caja de Registro debe estar colocada en una sección accesible, no se debe usar para empalmes de cables en lugares donde existan ángulos.

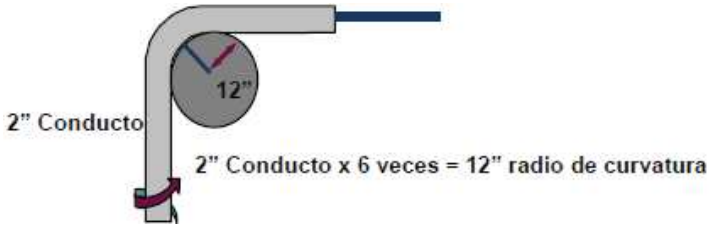


Figura 76 Tubo *conduit*

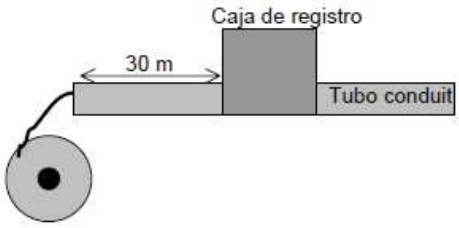


Figura 77 Caja de registro

Tomados de: http://www.artmark.com/products_associates_esp

- *Tubo corrugado y fiber runner.*- El tubo corrugado es un tubo de plástico flexible muy resistente al fuego, utilizado comúnmente para transportar fibra óptica. Actualmente lo más óptimo y recomendable para el trasporte de fibra óptica es el *fiber runner*, que es un canal capaz de proteger a la fibra contra el ruido, la degradación de señal y las curvaturas excesivas, gracias a su

novedoso diseño que separa cada hilo de fibra en un pequeño canal interno. La figura 78 muestra lo antes mencionado:

Figura 78 Tubo corrugado y *fiber runner*

Tomado de: http://wdminc.com/details/bringing-manageability-to-the-data-center/

- *Piso falso.-* Consiste en paneles modulares de piso con características semi aislantes, con una altura no mayor a 0.75m apoyados por pedestales, usados en los *data center*. Los pisos falsos tienen una resistencia entre 30 a 50kg/m2. Existen varios tipos tales como los suspendidos, posición libre (pedestales) y los *cornerlock* (sostenidos en las esquinas). La figura 79 muestra el grafico de un piso falso:

Figura 79 Piso falso

Tomado de: http://frankorozco.wordpress.com/tag/piso-falso

- Techo falso.- Son estructuras móviles ubicadas en el techo (figura 80). Entre sus características se debe respetar lo siguiente:
  - La altura máxima es de 3.60 m sobre el piso y de 7.6 cm entre el cable y el techo falso.

- Los espacios de techo falso inaccesibles no deben ser usados como vías de distribución.
- El alambre o barra de soporte del techo falso no debe ser el medio de soporte de los cables, a menos que este diseñado específicamente con ese propósito.
- El cable no debe caer directamente sobre las láminas del techo falso.

Figura 80 Techo falso

Tomado de: http://www.arkadiadatacenter.com/?_escaped_fragment_=falso-techo

- *Pasillos fríos.-* Un sistema de pasillos fríos (CACS), contiene el flujo de aire frío del *data center* separado del caliente. Para lograr esto, hay que tener en cuenta que se requiere que las filas de racks tengan una disposición coherente entre pasillos calientes/pasillos fríos de (2m de separación), y una temperatura de entrada de aire de 10 °C. Comúnmente la parte frontal de los equipos en los racks van al lado del pasillo frio. Existen también pasillos fríos hermetizados, los cuales cuentan con una puerta de acceso al interior del *data center*, tal como se muestra en la figura 81:

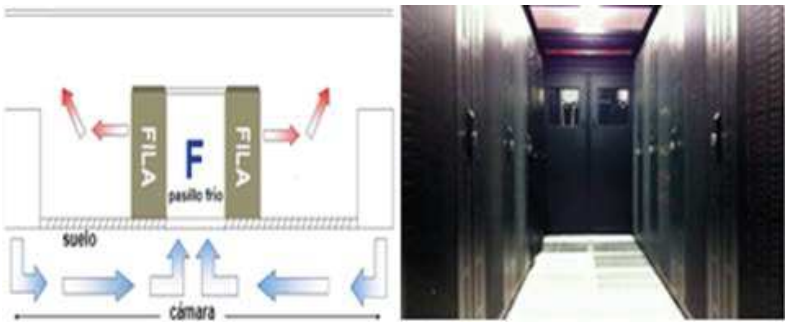


Figura 81 Pasillo frio

Tomado de: http://www.openup.es/cerramientos-de-pasillos-frio-o-caliente/

- *Pasillos calientes.*- Un sistema de pasillos calientes (HACS), contiene el flujo de aire caliente del *data center* separado del frio. Comúnmente la parte trasera de los equipos dispuestos en los racks van al lado del pasillo caliente, ya que por ahí sale el aire temperado de los ventiladores, los mismos que son absorbidos nuevamente por el sistema de refrigeración para volver a ingresar a los pasillos fríos, tal como se aprecia en la figura 82. La temperatura máxima de aire permitida es de 27 °C.

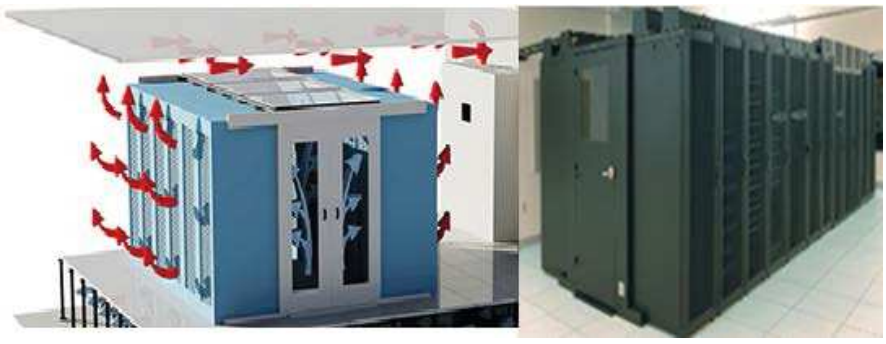


Figura 82 Pasillo caliente

Tomado de: http://www.openup.es/cerramientos-de-pasillos-frio-o-caliente/

- *Escalerillas.*- Son estructuras rígidas para contener cables de telecomunicaciones. La mínima altura para el acceso debe ser de 30 cm (del techo a la bandeja). Las escalerillas no deben contener en la misma estructura metálica cables (UTP, fibra) con cables

energéticos, ya que podría generarse interferencia entre los mismos. La figura 83 muestra una escalerilla:

Figura 83 Escalerillas

- *Canaletas.-* Son estructuras rígidas de plástico empleadas para transportar el cableado. Las canaletas deben tener cuatro veces el diámetro del cable UTP para garantizar un fácil manejo. Estas canaletas deben ir separadas del cableado eléctrico. La figura 84 muestra una canaleta y su acople para curvaturas:

Figura 84 Canaletas

- *Áreas de trabajo.-* Son áreas en el edificio donde el usuario puede interactuar con el equipo de telecomunicaciones (figura 85). Entre sus características se debe respetar lo siguiente:
  - El área de trabajo por promedio debería tener 10 m2.
  - Se deberá instalar una salida de eléctrica cerca de cada salida de telecomunicaciones (*face plate*).
  - Estas salidas de telecomunicaciones deben estar colocadas a la misma altura de las salidas eléctricas.

- El cableado instalado debe tener fácil acceso para su cambio en caso de ser requerido.
- La distancia máxima entre el *face plate* y el *host* deberá ser de 3m.
- Las salidas del área de trabajo deben poseer 2 conectores, uno para datos y otro para voz.

Figura 85 Salida de telecomunicación

- *Cuarto de equipos.*- Es el espacio en que ocurre la conexión de equipos o instalaciones de telecomunicaciones ínter o intra edificio (figura 86). Entre sus características se debe respetar lo siguiente:
  - En edificios con un área inferior a 500 m2 puede utilizarse un pequeño gabinete superficial.
  - Si el área es inferior a 100 m2 puede utilizarse un gabinete de pared.
  - La iluminación debe estar a 2.6m del piso falso.
  - La iluminación debe tener 540 LX (lumen) a un metro del piso.
  - Como mínimo debe existir dos circuitos de energía eléctrica 120V, 20A.
  - Se recomienda emplear *patch cord* categoría 6 o superior.
  - La puerta de acceso deberá siempre abrir hacia el exterior.
  - La puerta de acceso deberá tener mínimo 1m de ancho por 2m de alto.
  - Se recomienda utilizar pintura especial contra incendios.

- No debe existir tuberías de agua que pasen sobre o por debajo, para evitar inundaciones.

Figura 86 Cuarto de equipos o *data center*

Tomado de: http://mx.clipdealer.com/video/media/1659484

- Armario de distribución.- Es el espacio asignado para equipos de telecomunicaciones que hacen uso los ocupantes del edificio. Es el encargado de interconectar el *data center* hasta los *face plate* de los usuarios finales (figura 87). Entre sus características se debe respetar lo siguiente:
  - Evitar lugares que puedan limitar a futuro el crecimiento.
  - Debe ser ubicado en la mitad del piso y en la planta baja.
  - Debe estar conectado hacia las rutas de cableado de *backbone.*
  - La altura mínima deberá ser de 2.44m sin ninguna obstrucción.
  - La iluminación debe tener 540 LX (lumen) a un metro del piso.
  - Debe estar debidamente conectado a una barra de tierra.
  - Se aconseja utilizar *patch cord* categoría 6 o superior.
  - La temperatura debe estar entre los 18° a 24° con una humedad relativa entre 30° a 55°.

Figura 87 Armario de distribución

La ejecución y cumplimiento de la TIA-569A dentro de la estructura actual de red que posee Akros, mejorará la manera en como los medios de transmisión deben estar ubicados, obedeciendo las distancias, materiales y curvaturas máximas permitidas. Así mismo, permitirá tener un mayor orden, control y un mantenimiento mucho más fácil, el cual ayudará a la administración del cableado y equipos, lo que finalmente permitirá obtener un desempeño superior al actual en la red de Akros.

3.3 Introducción a ITIL

ITIL (biblioteca de Infraestructura de tecnologías de la información) está basada en la calidad de servicio y la mejora eficaz de los procesos que envuelven las actividades más importantes de las empresas en sus TI. Cabe recordar que, ITIL no es una norma, sino un conjunto de las mejores prácticas del mercado que mejorarán la disponibilidad, confiabilidad y seguridad de la compañía.

Debido a que ITIL es muy amplio y está encauzado en varios campos, en este proyecto solamente se enfocará el efecto que posee ITIL sobre el departamento de tecnología de la información (TI) de Akros, el cual se lo desarrollará a continuación.

3.3.1 ITIL, funciones operacionales y roles de trabajo enfocados a la ingeniería de TI

ITIL con el apoyo del TI trata de efectuar los objetivos de negocios de la organización, basándose y enfocándose en la ejecución de procesos, en la calidad para alcanzar la efectividad y la eficacia del uso

de los sistemas. Aquí se representan las mejores prácticas para entregar servicios de calidad, incluyendo roles, labores y acciones que se aplican en los procesos. A continuación se detallan las ventajas y desventajas de ITIL que podrán generarse sobre el departamento de TI de Akros.

Ventajas de ITIL para TI de Akros

- El departamento de TI desarrollará una estructura más clara, se vuelve más eficaz, y se centra más en los objetivos de la organización.
- La administración poseerá un mejoramiento en el control, se normalizan e identifican los procedimientos, y además los cambios resultan mucho más fáciles de manejar.
- Con la utilización de las mejores prácticas de ITIL, se puede dar un cambio en la cultura de TI y su orientación hacia el servicio, lo que facilitará la introducción de un sistema de administración de calidad.
- ITIL proporcionará un marco de referencia uniforme para la comunicación interna y con proveedores.

Desventajas de ITIL para TI de Akros

- Mucho tiempo y esfuerzo empleado para su implementación.
- Que no exista el cambio en la cultura del área involucrada.
- Poca compresión sobre los procesos, indicadores, lo que no permite una mejora.
- Falta de involucración del personal.

Los procesos de ITIL tendrán como objetivo ser implementados para que apoyen a los procesos de Akros, no para que los definan. El departamento de TI mejorará la calidad de servicio pero, así mismo, estará intentando reducir costos, o por lo menos mantenerlos a su nivel actual. Existen varios tipos de gestiones dentro del ITIL aplicadas a TI, de las cuales Akros podría utilizar las siguientes:

- *Gestión de incidencias.-* El departamento de TI tiene como labor atender incidentes en *hardware* o *software*, y otras tareas de servicio como perdidas de servicio, pedidos de información, renovación de clave, etc. Si esta responsabilidad de apoyo diario no se sistematiza se depende casi totalmente de la capacidad de cada técnico y no se reutiliza todo el conocimiento aprendido para futuros problemas. Existen varios ejemplos de incidencias que se pueden presentar tales como: demora en la entrega de un *software*, problemas en la infraestructura de desarrollo, enfermedad de un miembro de un proyecto, etc. El uso de la gestión de incidencias tiene tres objetivos básicos:
  - Recortar las fases de fuera de servicio.
  - Guardar la información relevante de todas las incidencias.
  - Reunir las mejores prácticas de forma sistemática.

  La gestión de incidencias es uno de los procesos más relevantes definidos por ITIL, ya que se centra en restablecer la marcha normal del servicio lo más rápidamente posible, y con el menor impacto sobre la acción del negocio. Las ventajas de una gestión eficaz de incidencias son:
  - Disminución del impacto de las incidencias sobre la compañía.
  - Mejora en el uso de los recursos de personal.
  - Redacta la solución, adjuntando archivos con información relacionada.
  - Guarda la incidencia, informando del tipo de problema, síntomas, equipo involucrado, etc.
  - Archiva la incidencia y asignar la responsabilidad a un grupo de soporte.
  - Crea informes, que faciliten el reconocimiento de lo qué está sucediendo para mejorar el proceso.
  - Comunica prontamente al usuario la fase de su requerimiento a través de un *e-mail*.

- *Gestión de configuración.-* Es el proceso de reconocer y precisar los elementos en el sistema, vigilando el cambio de estos elementos, registrando e informando la situación de los elementos y las peticiones de cambio, y comprobando que los elementos estén completos. El objetivo de la gestión de la configuración es conservar la integridad de los elementos que se logran a lo largo del desarrollo de los sistemas de información, avalando que no se ejecuten cambios sin control y verificando que todos los integrantes manejen la versión de los productos. La gestión de configuración se realiza en todas las acciones relacionadas con el desarrollo del sistema. Por ejemplo, al instante que un nuevo equipo se adquiera, escogiendo como elemento de configuración en el plan de gestión de configuración, se deberá reconocerlo e incluirlo en el sistema de gestión. Así mismo, cuando se reestructure un equipo que ya está reconocido en este sistema, se deberá añadirlo indicando su versión y estado. Una vez certificada la propuesta, se adjunta el cambio en el sistema de gestión de la configuración. Este cambio refleja las peticiones de mantenimiento que serán realizadas en el cambio.

- *Gestión de problemas.-* Aquí, los problemas son guardados en la CMDB (base de datos de dirección de configuración), apartadamente de los incidentes que están relacionados. El inconveniente que origino el problema puede ser nuevo o antiguo. Una vez conocida la causa, se elabora un nuevo ítem llamado “error conocido”. Cada error conocido es identificado, guardado como registros en el CMDB, vinculados a los problemas que ellos producen.

  En sí, la CMDB es una recopilación de Ítems de configuración, o CI. Un CI puede ser cualquier cosa que posea atributos

relevantes. Un CI no es más que todos los incidentes, problemas, y errores en conjunto.

Existen diferentes niveles de problemas y se los clasifica en:

- Impacto ALTO: Es el incumplimiento del cronograma del proyecto o acción a realizar.
- Impacto MEDIO: Puede ocasionar el incumplimiento del cronograma.
- Impacto BAJO: No perturba la ejecución del proyecto o acción a realizar.

- *Gestión de cambios.-* Es el proceso que controla el soporte del servicio de TI. Cada cambio ejecutado requiere de un RFC (*request for change*) que se guarda en el CMDB.

  El proceso de gestión de cambios conserva la infraestructura de TI acorde a las necesidades del negocio. Este proceso logra manejar cualquier cambio para la debida entrega de servicios mediante un proceso de aprobación.

- *Gestión de disponibilidad.-* Tiene como objetivo optimizar la capacidad de la infraestructura de TI, incluyendo sus servicios. Posee una fuerte disponibilidad en los niveles de servicios, los cuales le permiten a la compañía cumplir sus objetivos. La gestión de disponibilidad incluye: seguridad, servicialidad, recuperabilidad, sostenibilidad y resistencia de los recursos de TI. Lo antes mencionado se cumple determinando todos los requerimientos de disponibilidad del negocio equilibrando estos con la capacidad de la infraestructura de TI. Donde existe una desigualdad entre los requerimientos versus capacidad, la gestión de disponibilidad asegurará que el negocio esté equipado con un buen servicio a costos razonables.

Después de realizar todo el análisis de los diferentes puntos de estudio de ITIL que se proponen aplicar al departamento de TI de Akros, se podría crear un excelente modelo de procesos, el cual promovería la calidad para alcanzar efectividad en el negocio y eficiencia en el uso de los sistemas de información. Así mismo, permitiría realizar una mejor utilización de los recursos tanto informáticos como humanos ya que estos tendrían claramente definidos sus objetivos y funciones.

Como parte del alcance de este proyecto y tomando en cuenta todo lo mencionado anteriormente, se procederá a realizar un manual básico de procedimientos enfocados al departamento de TI (ver anexos), en el cual se describirán las funciones y actividades más relevantes que se deben efectuar para tener una armonía y control tanto de equipos así como de la seguridad de la información.

Finalmente la siguiente tabla 15 muestra el *checklist* diseñado el cual podría servir para constatar el uso de ITIL en Akros:

Tabla 15 *Checklist* ITIL

ITIL Funciones operacionales y roles de trabajo enfocados a la ingeniería de TI									
Gestion de incidencias	Cumplimiento	Gestion de configuracion	Cumplimiento	Gestion de problemas	Cumplimiento	Gestion de cambios	Cumplimiento	Gestion de disponibilidad	Cumplimiento
Minimiza periodos fuera de sevicio	Si ☐ No ☐ Porcentaje %	Identifica y define elementos del sistema	Si ☐ No ☐ Porcentaje %	Definir tipo de problema	Reactivo ☐ Proactivo ☐	Existio un RFC en los cambios	Si ☐ No ☐ Porcentaje %	Duracion del plazo del plan de disponibilidad	Corto ☐ Mediano ☐ Largo ☐
Existe un registro de informacion relevante	Si ☐ No ☐ Porcentaje %	Mantiene la integridad de los productos	Si ☐ No ☐ Porcentaje %	Existen problemas registrados en la CMBD	Si ☐ No ☐ Porcentaje %	Los RFC son atendidos según su prioridad	Si ☐ No ☐ Porcentaje %	Optimiza la capacidad de la infraestructura de TI	Si ☐ No ☐ Porcentaje %
Existe incorporacion de mejores practicas	Si ☐ No ☐ Porcentaje %	Registro de productos en el sistema	Si ☐ No ☐ Porcentaje %	Identificacion de la causa de los problemas	Si ☐ No ☐ Causa %	Mantencion de la infraestructura de TI con las necesidaddes del negocio	Si ☐ No ☐ Porcentaje %	Permite al negocio cumplir sus objetivos	Si ☐ No ☐ Porcentaje %
Uso eficiente del personal	Si ☐ No ☐ Porcentaje %	Planifica la estructura de TI y asegura su disponibilidad	Si ☐ No ☐ Porcentaje %	Identificacion de los responsables del problema	Si ☐ No ☐ Resposable %	Preservacion de la integridad de las CMDB asocidas	Si ☐ No ☐ Porcentaje %	Permite al negocio poseer costos razonables	Si ☐ No ☐ Porcentaje %
Resgistro de incidencia	Si ☐ No ☐ Porcentaje %	Existio definicion del alcance de la CMDB	Si ☐ No ☐ Porcentaje %	Nivel del problema	Alto ☐ Medio ☐ Bajo ☐	Correcion de errores	Si ☐ No ☐ Porcentaje %	Cumplimiento del SLA	Si ☐ No ☐ Porcentaje %
Clasifica la incidencias	Si ☐ No ☐ Porcentaje %			Se convirtio el problema en un error conocido	Si ☐ No ☐ Porcentaje %	Aceptacion del cambio	Si ☐ No ☐ Porcentaje %	Gestionar las interrupciones del servicio para el debido mantenimiento	Si ☐ No ☐ Porcentaje %
Investiga la causa de la incidencia	Si ☐ No ☐ Porcentaje %					Preservacion de la calidad de servicio durante el cambio	Si ☐ No ☐ Porcentaje %	Elaboracion de informes de dsiponibilidad (#fallos, tiempo, etc)	Si ☐ No ☐ Porcentaje %
Documenta la solucion	Si ☐ No ☐ Porcentaje %					Elaboracion de metricas sobre los cambios realizados	Si ☐ No ☐ Porcentaje %		
Comunica al usuario sobre el estado de la solicitud	Si ☐ No ☐ Porcentaje %								
Elaboracion de informes	Si ☐ No ☐ Porcentaje %								

CAPÍTULO IV

4 Planeación y costos

Este capítulo se enfoca en la planeación de una red y el costo-beneficio que la misma conlleva. Como primer tema se describirá el plan de gestión de proyectos, que está basado en la instalación y configuración de los nuevos equipos del *data center.*

4.1 Plan de gestión de proyectos

El plan de gestión de proyectos se enlaza directamente con la actividad "planear" del ciclo de la vida de la red que se describió anteriormente en el punto 2.1 del capítulo 2. Este plan de proyectos fue desarrollado con el fin de detallar las actividades, roles, hitos, etc que pueden surgir durante la trayectoria de la instalación y puesta en marcha de los equipos en el *data center*.

4.1.1 Gestión de adquisiciones

Aquí se especificarán los equipos y/o *software* a instalarse, describiendo el tiempo y el personal empleado para esto. Se realizarán actividades tales como:

- **Reacondicionamiento del área,** en donde:

- Se instalará dos tomas de 220V para *enclosure.*
- Se conectará y energizará los PDU's del *rack*.

- **Enclousure y servidores,** en donde:

- Se desempaquetarán los nuevos equipos y se inspeccionará el *hardware* antes de la instalación.
- Se montará el *hardware* relacionado con el *rack* (como los rieles y los soportes) en el *rack*.
- Si es necesario, se retirarán los componentes (como blades, fuentes de alimentación y controladores) del producto cubierto para facilitar la instalación reduciendo el peso general.
- Se montará el producto en el *rack*.

- Se reinstalarán los componentes que se hayan retirado del servidor.
- Se instalarán las PDU en el *rack*, según sea necesario, para la adecuada configuración de alimentación del producto cubierto.
- Se instalarán y los cables de alimentación al servidor.
- Se conectarán los cables al producto si es necesario.
- Se colocarán etiquetas pre impresas a los cables o al producto cubierto.
- Se organizará, agrupará y unirá los cables de forma ordenada para permitir un acceso fácil al producto cubierto.
- Se encenderá el servidor para asegurar que se inicie y funcione sin indicadores de falla visibles.
- Se verificará que el servidor tenga todas las revisiones de *firmware* adecuadas y actualizar según sea necesario.
- Se realizará un diagnóstico de la utilidad del *hardware* básico y probar el servidor y los componentes internos.
- Se conectará el cable de la UPS.
- Se probará la funcionalidad de la UPS.
- Se realizará conectividad, de todos los equipos que forman parte de esta solución, adicionalmente 1 servidor R710 y el *storage* P4300 y la librería MSL2024.
- Se realizará la configuración del sistema de almacenamiento *storage* según lo requerido para la nueva solución y se la integrará con la configuración de la solución existente.

➢ **Capacitación de la solución blade,** que consta de las siguientes actividades y/o acciones:

- Duración: 15 horas.
- Asistentes: 3 personas.
- Temas a tratar:
- Instalación y administración del *enclousure* y servidores *blade.*

- Consolidación de la solución *blade* con el sistema de almacenamiento existente.

➢ **Implementación de *software* de virtualización,** en donde se realizarán actividades tales como:

- Instalación y configuración del sistema operativo VMware Vsphere 5.0 sobre los servidores físicos (2 servidores).
- Creación de máquinas virtuales Windows server 2008.
- Instalación del *software* de administración del ambiente virtual (VMware vCenter *server*).
- Migración de servidores físicos hacia máquinas virtuales, con *software* de migración especializado.
- Pruebas de rendimiento, funcionalidad, conectividad de la plataforma de virtualización.
- Es responsabilidad del administrador del área sistemas informar a sus usuarios sobre el mantenimiento o instalación que se realice a la infraestructura y del tiempo en el que los servicios no se encontrarán disponibles.
- Es responsabilidad del administrador del área de sistemas, en caso de ser necesario, respaldar toda aquella información crítica y/o relevante para la él.

A continuación, la tabla 16 muestra el detalle de equipos y servicios a entregarse para este proyecto:

Tabla 16 *Hardware*

Item	Descripción	Cantidad
1	Chasis HP *blade* C7000	1
2	*Switch* HP A5500 24g 4SFP	1
3	*Switch* HP A5120 24g	1
4	Servidor Dell *power edge* R710	1
5	HP *storage* P4300	2

6	Librería Dell MSL 2024	1
7	*Rack* cerrado de piso 42 UR desmontable, de 200x800x 1000mm. 19 pulgadas de ancho, puerta de malla modelo Júpiter	1
8	Bandeja estándar fija de 19"	1
9	Bandeja para teclado móvil deslizable	1
10	Sistema de enfriamiento LG S362CP	1
11	Organizador vertical 80x80 para cada lado	2
12	Ventilador con cable 2mt y enchufe	3
13	VMware vSphere 4 estándar para 1 procesador (máximo 6 *cores* por procesador)	4
14	Soporte básico / suscripción para VMware vSphere estándar para un procesador para 1 ano	4
15	VMware vCenter Server 4 standard para vSphere	1
16	Soporte básico / suscripción para vCenter server 4 standard	1
17	Servicios de instalación de *rack* y componentes	1
18	Servicios de instalación y configuración de solución *blade*	1
19	Servicios de instalación y configuración de solución de virtualización	1

4.1.2 Supuestos y observaciones

Para el cumplimiento de la instalación y configuración de los nuevos equipos, se realizarán las siguientes ampliaciones físicas:

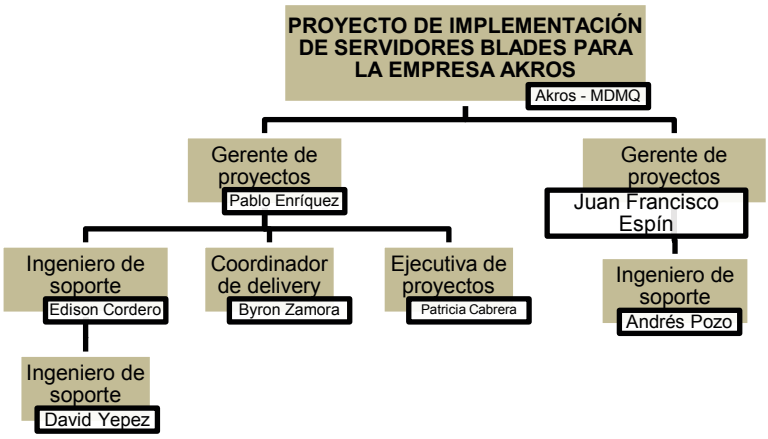
- **Requisitos ambientales,** en donde se encuentra detallado lo siguiente:

- Espacio físico:
- El área mínima disponible para la instalación del *rack* debe ser de:
- Altura: 2.4m
- Ancho: 3m
- Largo: 3m
- El tamaño mínimo de las puertas de acceso debe ser de:
- Ancho: 70cm
- Instalaciones eléctricas:
- Voltaje de alimentación: 220V
- Tipo de alimentación bifásica, regulada.
- Tipo de cable entre la acometida y el *rack* 10AWG, 3 líneas.
- Tablero de distribución debidamente balanceado, *breaker* recomendado 30A.

4.1.3 Organigrama

El organigrama de Akros se lo puede visualizar de la siguiente tabla:

Tabla 17 Organigrama



4.1.4 Gestión de los RRHH del proyecto

Las responsabilidades describirán los roles y/o funciones que cada persona involucrada en el plan de gestión de proyectos debe desempeñar y se visualiza con la siguiente tabla 18:

Tabla 18 Responsabilidades

Nombre	Cargo	Código
Cabrera Patricia	Ejecutiva proyectos	PC
Cordero Edison	Ingeniero de soporte	EC
Enríquez Pablo	Gerente de proyecto	PE
Pazmiño Ernesto	Ingeniero de soporte	EP
Andrés Pozo	Ingeniero de soporte	AP
Juan Francisco Espín	Director de proyecto	JE
David Yépez	Ingeniero de soporte	DY
Villacis Orlando	Gerente general Akros	OV
Zamora Byron	Coordinador Delivery	BZ

4.1.5 Gestión de actividades del proyecto

Aquí se describirán las actividades a realizarse a lo largo del proyecto, tales como:

4.1.5.1 Implementación y puesta en marcha de la solución

Aquí se contempla la puesta en marcha de toda la solución, instalación física, primer encendido de equipos, actualizaciones de *firmware*, configuraciones, pruebas de operación y puesta en producción de todos los equipos entregados.

Hito 1- Puesta en producción de equipos

Instalación física, primer encendido, actualización de versiones de firmware (de ser necesario) y configuraciones. Realizar una hoja de trabajo para estas actividades.

Tabla 19 Puesta en producción de equipos

Tarea	Descripción	Responsable	Recursos
1	**Instalación física de equipos** Ubicación de los equipos y accesorios en los Racks.	EC, DY.	Manuales, hoja de trabajo
2	**Primer encendido de equipos** Energizar los equipos, prueba de funcionamiento.	EC, DY.	Manuales, hoja de trabajo
3	**Verificación y actualización de *firmware*** Revisión de versiones y actualización de *firmware* en caso de ser necesario.	EC, DY.	Manuales, hoja de trabajo, internet
4	**Configuración de direcciones IP** Configuración de la red plana con las direcciones IP's que le corresponda a cada equipo.	EC, DY.	Diagramas de red, esquema de direccionamiento, hoja de trabajo
5	**Pruebas de conectividad de red** Ejecución de pruebas de conectividad que certifique la correcta operación de los equipos y la conectividad con la red de Akros.	EC, DY.	Diagramas de red, hoja de trabajo
6	**Peinado y Etiquetado de cableado** Realizar el etiquetado e identificación del cableado y puntos de red, además del peinado del cableado en caso de ser necesario.	EC, DY.	Diagramas de red, hoja de trabajo

Hito 2- Transferencia de conocimientos - virtualización

Realizar la capacitación sobre virtualización a 3 personas designadas con una duración de 15 horas, empleando una hoja de asistencia.

Tabla 20 Transferencia de conocimientos- virtualización

Tarea	Descripción	Responsable	Recursos
1	**Validación de requerimientos previos** Coordinación de Lugar y hora de la capacitación, además del temario y los asistentes.	PE	Cronograma, temario
2	**Cumplimiento del Temario** Ejecución de la capacitación cumpliendo el temario planificado.	PE	Temario
3	**Firma de hoja de asistencia y encuesta de satisfacción** Realizar el registro respectivo de asistentes y encuesta de satisfacción.	PE	Registro de asistentes, encuesta

Hito 3- Transferencia de conocimientos - *blades*

Realizar la capacitación sobre de la solución de *blades* instalada a 3 personas designadas con una duración de 15 horas, empleando una hoja de asistencia.

Tabla 21 Transferencia de conocimientos- *blades*

Tarea	Descripción	Responsable	Recursos
1	**Validación de requerimientos previos** Coordinación de Lugar y hora de la capacitación, además del temario y los asistentes.	EC	Cronograma, temario
2	**Cumplimiento del temario** Ejecución de la capacitación	EC	Temario

	cumpliendo el temario planificado.		
3	**Firma de hoja de asistencia y encuesta de satisfacción** Realizar el registro respectivo de asistentes y encuesta de satisfacción.	EC	Registro de asistentes, encuesta

Hito 4- Instalación y configuración de software de virtualización

Realizar la instalación de la aplicación de virtualización para migrar los servidores virtuales existentes de un servidor anterior hacia la nueva plataforma *blade.*

Tabla 22 Instalación y configuración de software de virtualización

Tarea	Descripción	Responsable	Recursos
1	**Instalación y configuración del sistema operativo** Instalación de S.O. Vmware vSphere 4.1 sobre los servidores físicos (2 servidores)	EC, AP, DY	Hoja de trabajo
2	**Creación de una máquina virtual** con S.O. Windows *server* 2008 de 64 bits	EC, AP, DY	Hoja de trabajo
3	**Instalación del *software*** Instalación de aplicación de administración del ambiente virtual (Vmware vCenter *server*)	EC, AP, DY	Hoja de trabajo
4	**Migración de servidores virtuales** Migración de 5 servidores virtuales hacia máquinas virtuales, con *software* de migración especializado.	EC, AP, DY	Hoja de trabajo
5	**Pruebas de funcionamiento** Realizar todas las pruebas de, funcionalidad, conectividad de la plataforma de virtualización para asegurar el correcto funcionamiento.	EC, AP, DY	Hoja de trabajo

4.1.5.2 Documentación y finalización del proyecto

Consolidación de toda la información, realizando un informe final del proyecto.

Hito 1- Verificación de cumplimiento de alcances

Akros y el Contratista deben verificar que toda la solución entregada cumpla con los alcances establecidos en el objeto del contrato, ejecutando la firma de actas de entrega definitiva.

Tabla 23 Verificación de cumplimiento de alcances

Tarea	Descripción	Responsable	Recursos
1	**Inspección de toda la solución implementada** Realizar una inspección de todos los sitios y equipos instalados.	JE, PE, EC, EP.	Pliegos, plan de gestión
2	**Realización de documentación e informes finales del proyecto** Realizar un documento consolidado de todo el proyecto y actas de cierre de proyecto.	PE	Actas de cierre parciales, informes de fase
3	**Envío de actas de finalización / consolidado** Enviar documento consolidado previo a la firma del acta de entrega definitiva.	PE	Informe final de proyecto

Hito 2- Cierre del proyecto

Realización de la reunión de cierre formal del proyecto y facturación, entregando el acta de cierre de proyecto firmada y su respectiva factura.

Tabla 24 Cierre del proyecto

Tarea	Descripción	Responsable	Recursos
1	**Reunión de cierre de proyecto** Revisión general del cumplimiento del plan de trabajo y proyecto.	JE, PE.	Informe final del proyecto
2	**Aceptación formal de cierre de proyecto** Firma de acta de cierre de proyecto.	JE, PE.	Acta de cierre
3	**Facturación** Revisar la factura del contratista.	PC	Factura

1		PROYECTO IMPLEMENTACION DE SERVIDORES BLADES PARA AKROS	129 días	vie 23/11/12	mié 22/05/13	98%
2	✓	FASE I - CONFIGURACIÓN DE BLADE Y STORAGE	9 días	vie 23/11/12	mié 05/12/12	100%
3	✓	Adecuar el data center - Requerimientos previos a la instalación	1 día	vie 23/11/12	vie 23/11/12	David Yepez,Muaricio Guaño 100%
4	✓	Instalación Física del Blade y storage	1 día	vie 23/11/12	vie 23/11/12	David Yepez,Muaricio Guaño 100%
5	✓	Configuración inicial del Blade	1 día	sáb 24/11/12	sáb 24/11/12	David Yepez,Muaricio Guaño 100%
6	✓	Configuración de enrutamiento de switch	1 día	sáb 24/11/12	sáb 24/11/12	David Yepez,Muaricio Guaño 100%
7	✓	Peinado y etiquetado del cableado	3 días	lun 26/11/12	mié 28/11/12	David Yepez,Muaricio Guaño 100%
8	✓	Pruebas de conectividad	2 días	jue 29/11/12	vie 30/11/12	David Yepez,Muaricio Guaño 100%
9	✓	Configuracion de direcciones IP	2 días	lun 03/12/12	mar 04/12/12	Edison Cordero,Lupe Plaza 100%
10	✓	Verificación y actualización del firmware	1 día	mié 05/12/12	mié 05/12/12	Franklin Pilapanta 100%
11	✓	FASE II - CONFIGURACIÓN INICIAL Y PRIMERA MIGRACIÓN	7 días	vie 04/01/13	lun 14/01/13	100%
12	✓	Validación y disponibilidad de licencias de VMWare	7 días	vie 04/01/13	sáb 12/01/13	Gabriel Mensias,Lupe Plaza 100%
13	✓	Asignación física para la migración de equipos	7 días	sáb 05/01/13	sáb 12/01/13	David Yepez,Franklin Pilapanta 100%
14	✓	Prearmado de infraestructura total	6 horas	lun 14/01/13	lun 14/01/13	Roberto Vaca 100%
15	✓	Envio del informe técnico (OK o faltantes)	2 horas	lun 14/01/13	lun 14/01/13	Roberto Vaca 100%
16	✓	FASE III - PRUEBA DE FUNCIONAMIENTO	6 días	jue 24/01/13	jue 31/01/13	100%
17	✓	Creación de arreglos en el Storage	1 día	jue 24/01/13	jue 24/01/13	David Yepez,Jaime Cajamarca 100%
18	✓	Integración del switch con el P4000	3 días	jue 24/01/13	lun 28/01/13	Franklin Pilapanta,Jaime Cajamarca 100%
19	✓	Instalación de Vmware, datastore	2 días	vie 25/01/13	lun 28/01/13	Franklin Pilapanta,David Yepez 100%
20	✓	Migración de servidores de Virtual a Virtual (no críticos)	2 días	sáb 26/01/13	lun 28/01/13	Franklin Pilapanta,David Yepez 100%
21	✓	Migración de servidores de Físico a Virtual (no críticos)	3 días	lun 28/01/13	mié 30/01/13	Franklin Pilapanta,David Yepez 100%
22	✓	Pruebas de funcionamiento y validación de los sistemas	2 días	mié 30/01/13	jue 31/01/13	Franklin Pilapanta,Lupe Plaza 100%
23	✓	FASE IV - MIGRACIÓN DE SERVIDORES CRÍTICOS	41 días	mié 30/01/13	vie 29/03/13	100%
24	✓	Validación de resultados de las pruebas FASE III	1 día	mié 30/01/13	mié 30/01/13	Franklin Pilapanta,Roberto Vaca 100%
25	✓	Migración de servidor Dominio	1 día	jue 31/01/13	jue 31/01/13	Franklin Pilapanta,David Yepez 100%
26	✓	Configuración nuevo esquema de red	1 día	vie 01/02/13	vie 01/02/13	Muaricio Guaño 100%
27	✓	Pruebas nueva estructura de res	1 día	sáb 02/02/13	sáb 02/02/13	Franklin Pilapanta,David Yepez 100%
28	✓	Migración de servidor Exchange	1 día	dom 03/02/13	dom 03/02/13	Franklin Pilapanta,Roberto Vaca 100%
29	✓	Migración de servidor CRM	1 día	jue 07/02/13	jue 07/02/13	Franklin Pilapanta,Roberto Vaca 100%
30	✓	Migración de servidor Aplicativos	1 día	vie 08/02/13	vie 08/02/13	Franklin Pilapanta,Roberto Vaca 100%
31	✓	Migración de servidor ERP	1 día	vie 22/03/13	vie 22/03/13	Franklin Pilapanta,Roberto Vaca 100%
32	✓	Migración de servidor Intranet	0,5 días	sáb 23/03/13	sáb 23/03/13	Franklin Pilapanta,Roberto Vaca 100%
33	✓	Migración de servidor Fileserver	0,5 días	sáb 23/03/13	sáb 23/03/13	Franklin Pilapanta,Roberto Vaca 100%
34	✓	Creación de Lync Server	1 día	mar 26/03/13	mar 26/03/13	Franklin Pilapanta,David Yepez 100%
35	✓	Creación de Project Server	1 día	mié 27/03/13	mié 27/03/13	Franklin Pilapanta,David Yepez 100%
36	✓	Creación de Servidor Testigo Base de Datos	1 día	jue 28/03/13	jue 28/03/13	Franklin Pilapanta,David Yepez 100%
37	✓	FASE V - PRUEBA DE FUNCIONAMIENTO DE TODA LA NUEVA ESTRUCTURA	4 días	sáb 23/03/13	jue 28/03/13	100%
38	✓	Pruebas de funcionamiento y validación de los sistemas	3 días	sáb 23/03/13	mar 26/03/13	Franklin Pilapanta,Lupe Plaza 100%
39	✓	Bono o Descuentos a roles y/o despidos	1 día	jue 28/03/13	jue 28/03/13	Pablo Enriquez 100%
40		FASE VI - CONFIGURACIÓN DE NIVELES DE RESPALDO	3 días	vie 29/03/13	mar 02/04/13	86%
41	✓	Validación de requerimientos previos (licencias de uso)	0,5 días	vie 29/03/13	vie 29/03/13	Lupe Plaza,Gabriel Mensias 100%
42	✓	Configurar agentes de Backup exec o net backup	0,5 días	vie 29/03/13	sáb 30/03/13	Jaime Cajamarca,David Yepez 100%
43	✓	Configuración de respaldo libreria	1 día	mar 02/04/13	mar 02/04/13	David Yepez 100%
44		FASE VII - CIERRE DEL PROYECTO	6 días	lun 01/04/13	lun 08/04/13	80%
45		Realización e informes finales del proyecto	2 días	lun 01/04/13	mar 02/04/13	José Padilla,Jaime Cajamarca,Lupe P 50%
46	✓	Envio de actas de finalización del proyecto	1 día	mié 03/04/13	jue 04/04/13	José Padilla 100%
47	✓	Reunión del cierre del proyecto	1 día	vie 05/04/13	vie 05/04/13	Gabriel Mensias,Pablo Enriquez 100%
48	✓	Aceptación formal del cierre del proyecto	1 día	lun 08/04/13	lun 08/04/13	Jaime Cajamarca,Edison Cordero,Fra 100%

Figura 88 Cronograma de actividades

Concluido el plan de gestión de proyectos, se describirán posteriormente los costos que implicaron la adquisición de los nuevos equipos y el valor que tendrían las propuestas realizadas a lo largo de este documento analizando simultáneamente el beneficio que se obtendría.

4.2 Análisis costo-beneficio

El análisis costo-beneficio es una herramienta utilizada en finanzas que calcula la relación que existe entre los costos y beneficios relacionados a un proyecto con el fin de evaluar su rentabilidad, teniendo en cuenta que un proyecto puede ser tanto de inversión así como de creación.

Mientras que la relación costo-beneficio (B/C) está dada por la siguiente fórmula:

$$\mathbf{B/C = VAN / (1+TIR)^2) / VAC / (1+TDD)^2)}$$

En donde se tienen valores tales como el cociente que se obtiene del resultado de la subdivisión entre el valor actual netos o beneficios netos (VAN) y la tasa interna de retorno (TIR) elevada al cuadrado más uno, los mismos que están divididos para el resultado de la subdivisión entre el valor actual de los costos de inversión o costos totales (VAC) y la *test driven development* (TDD) elevada al cuadrado más uno.

- VAN (valor actual neto).- Es la diferencia entre ingresos y costos expresados en moneda equivalente en un momento de tiempo.

- TIR (tasa interna de retorno).- Es el promedio de los rendimientos monetarios futuros esperados de una inversión realizada.

- VAC (valor actual de costos).- Permite comparar alternativas que poseen una vida útil similar.
- TDD (test driven development).- Es un proceso de desarrollo que está basado en la repetición de un ciclo de desarrollo muy corto.

En un análisis costo-beneficio, un proyecto o negocio será rentable cuando la relación costo-beneficio es mayor a uno.

$$\mathbf{B/C > 1}$$

Existen cinco fases para analizar una relación costo-beneficio:

- *Hallar costos y beneficios.-* Primeramente se debe hallar la proyección de los costos de inversión o costos totales y los ingresos totales netos o beneficios netos del proyecto o negocio para un periodo de tiempo determinado.

- *Convertir costos y beneficios a un valor actual*.- Debido a que los montos que se han proyectado no toman en cuenta el valor del dinero en el tiempo, se debe actualizar a través de una tasa de descuento.

- *Hallar relación costo-beneficio*.- Se divide el valor actual de los beneficios entre el valor actual de los costos del proyecto.

- *Analizar relación costo-beneficio*.- En caso de que el valor resultante sea mayor que 1 el proyecto es rentable, pero si es igual o menor que 1 el proyecto no es viable pues significa que los beneficios serán iguales o menores que los costos de inversión o costos totales.

- *Comparar con otros proyectos*.- Si se debe elegir entre varios proyectos de inversión, teniendo en cuenta el análisis costo-beneficio, se escogería el que posea la mayor relación costo-beneficio.

En el caso particular de Akros, el análisis costo-beneficio que se debe realizar está enfocado en la adquisición de los nuevos equipos, compra de *software*, adecuaciones, los cuales componen la salida de capital para este proyecto. El siguiente análisis costo-beneficio muestra la rentabilidad real que tendría este proyecto en los próximos tres años:

Las tablas 25 y 26 muestran los valores relacionados a la adquisición de equipos y a las adecuaciones realizadas y planteadas.

Tabla 25 Precios equipos *data center*

Precios equipos

País:	ECUADOR
Cliente:	AKROS
Fecha:	02/10/2012
Asesores:	Edison Cordero/ Franklin Pilapanta/ David Yepez

No. de Parte	Descripción	QYT	P.Lista Unitario	Dcto Exhibith	Dcto Adicional	Dcto Total	P.Unitario con Dcto Adicional	P.TOTAL con Dcto Adicional
	C7000							
507015-B21	HP BLc7000 1PH 6PS 10 Fan FL ROHS ICE	1	$13.369,33	10%	48%	58%	$5.615,12	$5.615,12
J9300A	HP X244 10G XFP SFP+ 1m DAC Cable	8	$1.069,00	28%	35%	63%	$395,53	$3.164,24
438030-B21	HP BLc GbE2c LY 2/3 Switch	3	$1.882,65	10%	48%	58%	$790,71	$2.372,14
	SWITCHES							
JG311A	HP A5500	1	$5.938,92	10%	48%	58%	$2.494,35	$2.494,35
JE069A	HP A5120	1	$3.346,92	10%	55%	65%	$1.171,42	$1.171,42
	SERVERS							
A2626096	DELL R710	1	$6.515,37	15%	8%	23%	$5.016,83	$5.016,83
	STORAGE							
633777-001	HP P4300 G7	2	$3.978,45	10%	58%	68%	$1.273,10	$2.546,21
	LIBRARY							
L2420A	HP MSL 2024	1	$16.953,89	10%	40%	50%	$8.476,95	$8.476,95
	ACCESORIOS							
T5518A	HP 8/8 and 8/24 SAN Switch 8-pt Upgr LTU	1	$3.690,00	10%	48%	58%	$1.549,80	$1.549,80
AJ715A	HP 4Gb Short Wave B-series FC SFP 1 Pack	8	$199,00	10%	48%	58%	$83,58	$668,64
AP768A	HP 42B PCIe 4Gb FC Dual Port HBA	1	$1.780,00	10%	48%	58%	$747,60	$747,60
JD362A	HP A5500 150WAC Power supply	4	$441,72	10%	48%	58%	$185,52	$742,09
JD360B	HP A5500 2Port 10GbE Loc connect module	2	$484,92	10%	48%	58%	$203,67	$407,33
AP860A	HP P2000 600GB 6G SAS 15K 3.5in Ent Hdd	2	$576,78	10%	48%	58%	$242,25	$484,50
503296-B21	HP 460W CS Gold Ht Plg Pwr Supply Kit	3	$260,83	10%	30%	40%	$156,50	$469,49
500662-B21	HP 8GB 2Rx4 PC3-10600R-9 Kit	12	$279,00	10%	48%	58%	$117,18	$1.406,16
507127-B21	HP 300GB 6G SAS 10K 2.5in DP ENT HDD	12	$323,21	10%	48%	58%	$135,75	$1.628,98
613431-B21	HP BLc NC553m DP FlexFabric Adptr Opt	12	$940,80	10%	48%	58%	$395,14	$4.741,63
403619-B21	HP BLc QLogic QMH2462 FC HBA Opt Kit	6	$783,83	10%	48%	58%	$329,21	$1.975,25
UT426E	HP 3y Supp Plus 24 P4300 G2 SAN Soln SVC	2	$2.078,40	18%	35%	53%	$976,85	$1.953,70
	SERVICIOS/CAPACITACION							
UK065E	HP 3y 4h 13x5 BL4xxc Svr Bld HW Support	12	$378,40	18%	35%	53%	$177,85	$2.134,18
UE478E	HP 3y 4h 13x5 c7000 Enclosure HW Supp	1	$827,20	18%	35%	53%	$388,78	$388,78
	ENERGIA							
AP8868	APC PDU 2G, Metered, ZeroU, 10.0kW, 208V	2	$1.117,33	0%	0%	0%	$1.117,33	$2.234,66
ZP24114X	Eaton blade UPS 14KVA	1	$12.364,00	0%	0%	0%	$12.364,00	$12.364,00
	ENFRIAMIENTO							
S362CP	LG S362CP	1	$1.439,00	0%	0%	0%	$1.439,00	$1.439,00
	Subtotal							$66.193,04
	WIRELESS							
DWC-1000	D-link Wireless controller	1	$876,00	20%	0%	20%	$700,80	$700,80
	ROUTER							
C800-K9	Router Cisco 800	2	$1.310,00	15%	0%	15%	$1.113,50	$2.227,00
	Subtotal							$2.927,80
	Total							$69.120,84

Equipos instalados Equipos propuestos para instalar

Tabla 26 Precios adecuaciones *data center*

Precios adecuaciones Data center

País:	ECUADOR
Cliente:	AKROS
Fecha:	02/10/2012
Contacto:	Jaime Cajamarca
Asesores:	Edison Cordero/ Franklin Pilapanta/ David Y

Descripción	Cantidad	Precio unitario/ mensual	Precio total	Descuento	P.Total con Dcto Total
Obra civil					
Remodelacion del Data center (4,5X3,0m)	1	$4.480,00	$4.480,00	0%	$4.480,00
Acometidas por escalerilla	2	$887,50	$1.775,00	0%	$1.775,00
Bypass electrico	1	$549,60	$549,60	0%	$549,60
Tablero de distribuccion electrico	1	$674,80	$674,80	0%	$674,80
Toma a tierra	1	$472,30	$472,30	0%	$472,30
Amarras plasticas 10cm	2	$3,05	$6,10	0%	$6,10
Amarras plasticas 15cm	2	$3,67	$7,34	0%	$7,34
Cinta aislante	1	$2,31	$2,31	0%	$2,31
Velcro 1" x m	1	$3,08	$3,08	0%	$3,08
Mano de obra	1	$3.990,00	$3.990,00	5%	$3.790,50
Rollo cable UTP cat 6A	1	$319,00	$319,00	5%	$303,05
Rollo cable UTP cat 5E	1	$157,00	$157,00	5%	$149,15
Software y/o Tecnología					
Link Aggregation 802.3ad	6	$110,00	$660,00	0%	$660,00
Enlace IRF 10 Gb	1	$354,45	$354,45	0%	$354,45
Etiquetacion cableado	56	$4,39	$245,84	2%	$240,92
Subtotal					**$13.468,60**
Actualizacion Data center Tier II					
Proteccion minima contra eventos	1	$1.400,00	$1.400,00	0%	$1.400,00
Puerta de seguridad	1	$1.600,00	$1.600,00	0%	$1.600,00
Eaton blade UPS 14 KVA (UPS+1)	1	$12.364,00	$12.364,00	0%	$12.364,00
Generador General electric 13Kw	1	$8.362,00	$8.362,00	0%	$8.362,00
APC rack PDU 20A/120V (PDU+1)	1	$727,00	$727,00	0%	$727,00
Emergency power off (EPO)	1	$689,00	$689,00	0%	$689,00
Mano de obra	1	$4.100,00	$4.100,00	5%	$3.895,00
Software y/o Tecnología					
Cloud Computing	36 meses	$2.109,00	$75.924,00	5%	$72.127,80
Instalacion Cloud computing	1	$800,00	$800,00	0%	$800,00
Adquisicion software Visiwave Pro	1	$3.190,00	$3.190,00	0%	$3.190,00
Internet Level 3	36 meses	$769,00	$27.684,00	0%	$27.684,00
Instalacion Internet Level 3	1	$700,00	$700,00	0%	$700,00
Backup Internet Telconet	36 meses	$749,00	$26.964,00	0%	$26.964,00
Instalacion Internet Telconet	1	$669,00	$669,00	0%	$669,00
Capacitacion y/o cursos nuevos equipos y/o tecnologia	4	$2.000,00	$8.000,00	0%	$8.000,00
Subtotal					**$169.171,80**
Total					**$182.640,40**

Equipos y/o tecnologia instalados Equipos y/o tecnologias propuestos para instalar

El periodo de recuperación de la inversión se ha dispuesto en 3 años, basándose en previas experiencias en proyectos anteriores realizados por Akros, tomando en cuenta el índice de depreciación de los equipos (33% anual) y al cambio permanente que la tecnología sufre.

La siguiente tabla 27 muestra el costo total y el beneficio total que tendría en 3 años este proyecto, tomando en cuenta ahorros relacionados con:

- *Mejora de procesos.-* Mejorando los procesos se puede llegar a obtener hasta un 25% de ahorro de gastos en el departamento de TI, acorde a nuevas tecnologías implementadas basadas en calidad & gestión de proyectos, las cuales permitirán eliminar errores, maximizar el uso de activos, facilidad de implementación, minimización de demoras, uso más productivo del personal, etc. Se ha tomado en cuenta los verdaderos gastos anuales del departamento de TI que ascienden a un promedio de $280000 en donde:

  Mejora de procesos= $280000*3años= $840000*0.25%= $210000

- *Eliminación de salarios:* Se estima eliminar 3 salarios con la implementación del data center, teniendo en cuenta un salario básico en el área de TI de $1000 en donde:

  *Eliminación de salarios= $1000*3=*$3000*36meses= $124218

- *Ahorro de energía:* El consumo calculado en el punto 2.3.1 es de 10.04KW/h. En el Ecuador el costo establecido por KW/h redondea los $0.20 centavos en donde se obtendría el siguiente calculo:

  *Ahorro de energía= $10.04*$0.20*1095dias= $52047.36*

- *Ahorro en mantenimientos:* Se tendrá un ahorro en mantenimientos tanto en preventivos como correctivos de $1500 anuales, basado en la experiencia de la empresa Akros, en donde:

  Ahorro de mantenimiento= $1500*3= $4500

Tabla 27 Análisis de comparación costo-beneficio

Análisis de comparación

Costo a 3 años		Beneficio a 3 años	
Instalación adecuaciones Data center	$182.640,41	Mejora de procesos	$210.000,00
Compra equipos Data center	$69.120,85	Eliminación de salarios	$124.218,00
		Ahorro de energía	$52.047,36
		Ahorro mantenimientos de equipos	$4.500,00
Costos totales:	**$ 251.761,25**	**Beneficios totales:**	**$390.765,36**

Por último, la tabla 28 muestra el análisis de finanzas que se realizó a este proyecto, en el cual se puede constatar el tiempo que se necesita para recuperar la inversión, el valor actual neto del proyecto, el flujo de caja, la tasa de descuento, la tabla de amortización, etc.

Como aclaración en la tabla 28, la liquidación de equipos de $15000 se extrajo de experiencias previas en ventas de equipos de tecnología que tuvo Akros.

Tabla 28 Finanzas del análisis costo-beneficio

Costos de Inversión

Precio Adecuaciones	$ 182.640,40
Precio Equipos	$ 69.120,84
Costo del Proyecto	**$ 251.761,25**
Monto del crédito	**$ 251.761,25**
Tasa de interés	12%
Numero de pagos	36
Pago (mensual)	8.362,08 $
Costo total del Proyecto	**$ 301.034,74**

Tabla de amortización

# Pago	Pago Interés	Pago capital	Saldo
1	$ 2.517,61	$ 5.844,46	$ 245.916,79
2	$ 2.459,17	$ 5.902,91	$ 240.013,88
3	$ 2.400,14	$ 5.961,94	$ 234.051,94
4	$ 2.340,52	$ 6.021,56	$ 228.030,38
5	$ 2.280,30	$ 6.081,77	$ 221.948,61
6	$ 2.219,49	$ 6.142,59	$ 215.806,02
7	$ 2.158,06	$ 6.204,02	$ 209.602,01
8	$ 2.096,02	$ 6.266,06	$

Liquidación equipos

Liquidación equipos en 3 años	$ 15.000,00	(Valor aproximado)
Tasa de descuento	12%	(Tasa de interés bancaria real)

Índices financieros

Años para recuperar inversión	2,31	($301.034,74/ $130.255,12= 2,31)

VAN

Valor actual neto 3 años	$10.550,1	$20.082,84	(Formula VAN)

Tasa interna de retorno

Tasa interna de retorno anual	43%		
Tasa interna de retorno 3 años	14%	16%	(Formula TIR)

Flujo de Caja

Beneficios totales= $390.765,3/ 3= $130.255,12

Año 0	Año 1	Año 2	Año 3
-$ 301.034,74	$ 130.255,12	$ 130.255,12	$ 130.255,12
-$ 301.034,74	$ 130.255,12	$ 130.255,12	$ 145.255,12

Sin Liquidación

Con liquidación

			203.335,95
9	$ 2.033,36	$ 6.328,72	$ 197.007,23
10	$ 1.970,07	$ 6.392,00	$ 190.615,23
11	$ 1.906,15	$ 6.455,92	$ 184.159,31
12	$ 1.841,59	$ 6.520,48	$ 177.638,82
13	$ 1.776,39	$ 6.585,69	$ 171.053,13
14	$ 1.710,53	$ 6.651,54	$ 164.401,59
15	$ 1.644,02	$ 6.718,06	$ 157.683,53
16	$ 1.576,84	$ 6.785,24	$ 150.898,29
17	$ 1.508,98	$ 6.853,09	$ 144.045,19
18	$ 1.440,45	$ 6.921,62	$ 137.123,57
19	$ 1.371,24	$ 6.990,84	$ 130.132,73
20	$ 1.301,33	$ 7.060,75	$ 123.071,98
21	$ 1.230,72	$ 7.131,36	$ 115.940,63
22	$ 1.159,41	$ 7.202,67	$ 108.737,96
23	$ 1.087,38	$ 7.274,70	$ 101.463,26
24	$ 1.014,63	$ 7.347,44	$ 94.115,81
25	$ 941,16	$ 7.420,92	$ 86.694,90
26	$ 866,95	$ 7.495,13	$ 79.199,77
27	$ 792,00	$ 7.570,08	$ 71.629,69
28	$ 716,30	$ 7.645,78	$ 63.983,91
29	$ 639,84	$ 7.722,24	$ 56.261,68
30	$ 562,62	$ 7.799,46	$ 48.462,22
31	$ 484,62	$ 7.877,45	$ 40.584,76
32	$ 405,85	$ 7.956,23	$ 32.628,53
33	$ 326,29	$ 8.035,79	$ 24.592,74
34	$ 245,93	$ 8.116,15	$ 16.476,59
35	$ 164,77	$ 8.197,31	$ 8.279,28
36	$ 82,79	$ 8.279,28	$ 0,00

Primeramente, para verificar que la inversión que se realizaría sea rentable, se debe tener en cuenta la proyección de ingresos que se esperan recuperar al final de los 3 años, la cual será de **$390765.36** (tomando como referencia ahorros relacionados con energía, mantenimiento, contratación nuevo personal, etc, al utilizar cloud computing), esperando una tasa de rentabilidad anual del proyecto del **43%** (teniendo como referencia la tasa ofrecida en proyectos previamente realizados). Asimismo, la inversión total más los interés correspondientes del **12%** anual (tomando como referencia la tasa de interés

bancario) sería de **$301034,74** (total entre compra de equipos y adecuaciones). Entonces aplicando la fórmula de B/C quedaría:

$$B/C = VAN / (1+TIR)^2) / VAC / (1+TDD)^2)$$
$$B/C = (\$390765.36 / (1+0.14)^2) / (\$301034,74 / (1+0.12)^2)$$
$$B/C = \$300681.25 / \$239983.05$$
$$B/C = \$1.25$$

Es decir, de los $1.25 existe un margen de ganancia de $0.25 centavos por cada dólar que se invierta, por lo convierte a este proyecto rentable por los próximos 3 años.

CAPÍTULO V

5 Conclusiones y recomendaciones

5.1 Conclusiones

- El uso del estándar TIA-942A proveerá a Akros una serie de recomendaciones para el diseño, funcionamiento e instalación de un *tier* de *data center*, de tal manera que permitirá establecer al departamento de TI el tipo de *data center* que posee, en este caso *tier* I, y lo necesario para actualizarlo a un tier superior, en caso de ser requerido.

- Las mejores prácticas en la gestión de incidencias empleando ITIL, requerirán la creación de una base de datos con los incidentes más comunes que se presenten día a día, permitiendo así bajar los tiempos de respuesta y solución a aquellos problemas cuotidianos o randomicos.

- Akros actualmente al no poseer un departamento de *networking*, se ve en la necesidad de subcontratar a terceros para trabajos de cableado y/o instalación de equipos, lo que implica una desventaja en departamento de TI, ya que no logra ser capacitado debidamente.

- El uso del ciclo de la vida de la red ayudará a Akros a bajar el costo de poseer y operar una red, mejorando su habilidad para responder a condiciones de mercado rápidamente cambiantes y acelerando el acceso a aplicaciones y servicios.

- El portafolio de equipos utilizados en este proyecto se basa completamente en las diferentes líneas comercializadas por la empresa, lo que permitió estar mucho más familiarizado con el uso y funcionamiento de los mismos.

- La administración de los routers de borde dentro de las instalaciones de Akros, permitirá un mejor entendimiento y control sobre la red, ya que se podrá realizar configuraciones y modificaciones según las necesidades de la misma.

- Gracias a la encuesta realizada al departamento de TI, se pudo validar de manera cuantitativa la importancia que poseen los activos de la información dentro de la compañía, lo que finalmente permitirá controlar y asegurar de mejor manera la manipulación de los mismos y al mismo tiempo, evitar daños o pérdidas.

- El método de virtualización actual empleado en Akros mejoró su rendimiento y capacidad, gracias a la adquisición de nuevos equipos, que a su vez permitirán a futuro la utilización de nuevas tecnologías como *cloud computing* dentro de la empresa.

- La realización de un mantenimiento regular y metódico a los equipos, permitirá el alargue de su vida útil y también incrementará su rendimiento diario.

- El uso de los protocolos IP SLA y *Tracks* en los enlaces de un equipo de capa 3 (*router, switch*), identificarán a tiempo los problemas que se pudieran suscitar, permitiendo al administrador de red solucionar dichos inconvenientes rápidamente para evitar pérdidas de paquetes, cuellos de botella, caídas del enlace, etc.

- VisiWave sin duda permitió evidenciar la carencia de intensidad de señal de cada AP en Akros, y al mismo tiempo posibilito la realización de una simulación para situar de mejor manera la ubicación de cada AP y si fuere necesario el incrementar el número de AP´s empleados.

- Toda la compra de tecnología, ya sea de *software* o *hardware* será rentable, siempre y cuando la liquidación de los equipos sea la prevista y la tasa de descuento impuesta por los bancos, no se incremente drásticamente.

- La realización de los laboratorios en GNS3, sin duda permitieron analizar el comportamiento que tendrían los equipos al momento de

poseer un enlace redundante, analizando igualmente sus ventajas y desventajas antes de su utilización.

- Las buenas prácticas propuestas sobre la configuración de políticas del *firewall* TMG de Akros, permitirán un mejor nivel de seguridad dentro y fuera de la red, asegurando así una optimización de los recursos del mismo.

5.2 Recomendaciones

- Se recomienda tomar en cuenta la creación de las nuevas VLAN´s, ya que las mismas permitirán obtener una mejor segmentación por departamentos de toda la red, lo que incrementará la seguridad, mejorará el rendimiento y reducirá costos.

- Se recomienda un crecimiento al enfoque de *networking*, debido a que Akros siendo una empresa con vasta experiencia en el mundo de la tecnología, no posea personal técnico altamente calificado para realizar instalaciones y configuraciones avanzadas de redes.

- Se debe realizar un levantamiento de información en la empresa, para facilitar la implementación procesos, los mismos que permitirán la ejecución de normas y mejores prácticas de una manera más eficientemente

- Se recomienda efectuar talleres de capacitación continua para motivar frecuentemente al personal de TI de Akros, de esta manera se logrará un desempeño más elevado en sus actividades laborales diarias.

- Se sugiere la adquisición de otro enlace de última milla con otro ISP, para de esta manera optimar la disponibilidad y confiabilidad en la red de Akros.

- Realizar un seguimiento de manera frecuente al subneteo y redistribución de VLAN's propuestos, para modificarlos según se vayan dando cambios dentro de ellos.

- Incrementar y fomentar las fortalezas dentro del área de TI, basadas en las recomendaciones dadas por ITIL, para de esta forma mejorar la relación que existe con las diferentes áreas de la empresa.

- Se recomienda incluir las responsabilidades y requisitos de seguridad de la información en el contrato de servicios de *cloud computing*, para mejorar el nivel de disponibilidad del mismo.

- Realizar con frecuencia respaldos de información tanto de servidores como de *host*, para de esta manera evitar pérdidas de información y mantener un esquema de respaldos.

- Es aconsejable dejar un margen de error en los cálculos tanto de compras como de ventas de tecnología, porque las mismas pueden variar su costo sin previo aviso.

- Se recomienda tener en cuenta el crecimiento anual de la empresa, de esta manera se podrá estar un paso adelante en la capacidad de tecnología a utilizarse el año siguiente.

- Es aconsejable correr rutinariamente un analizador de paquetes como Wireshark para asegurar que todo el tráfico que cursa la red es el indicado y no existen paquetes maliciosos.

- Una vez presentado este trabajo de titulación, se recomienda a Akros tomar en cuenta la reubicación de los AP's, para de esta manera mejorar la cobertura inalámbrica dentro de toda la empresa.

5.3 Referencias

Acevedo, A. Miranda, F. Núñez , G. Palomino, G. Valdés, C. (2011). Análisis costo-beneficio. Recuperado el 21 de mayo del 2013 de http://es.scribd.com/doc/7883091/Relacion-Beneficio-Costo

Administrator. (2011). *Configuring static route tracking using* IP SLA. Recuperado el 2 de mayo del 2013 de http://ww.firewall.cx/cisco-technical-knowledgebase/cisco-routers/813-cisco-router-ipsla-basic.html

Asesoría en proyecto de infraestructura tecnológica. Recuperado el 11 de marzo del 2013 de http://www.ingeo-electronica.com.ar/data-center.htm

Burbano, E. (2009). Normas y políticas de seguridad informática. Recuperado el 29 de mayo del 2013 de http://es.scribd.com /doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica

CCIE. (2010). Balanceo de carga. Recuperado 28 de abril del 2013 de http://ccie-en-espanol.blogspot.com/2009/05/bgp-balanceo-de-carga-i.html

Cez. (2009). Cableado horizontal. Recuperado el 3 de marzo del 2013 de http://www.cez.com.pe/Cableado%20Estructurado/Estructura%20cableaado%20Horizontal.html

Cortez, G. (2010). ¿Qué es el ancho de banda? ¿Cómo se calcula? Vol. 1, paginas 108, 112. Recuperado el 19 de abril del 2013 de http://www.rnds.com.ar/articulos/065/108w.pdf

Cisco. (2006). Ciclo de vida de la red. Recuperado 22 de abril del 2013 de http://www.cisco.com/web/LA/productos/servicios/docs/Brochure_LCS_062006_SP_Spanish.pdf

Cisco. (2010). CCNP route 642-902 official certificate. (vol 2). Cisco press

Cisco (2010). Operational fundations for Cisco service provider core network. (vol 1). Cisco press.

Definición de PDU. Recuperado el 16 de febrero del 2013 http://www.alegsa.com.ar/Dic/PDU.php

Espino, L. (2009). *Cloud computing* como una red de servicios. Recuperado el 5 de febrero del 2013 de http://www.luisespino.com /pub /cloud_computing_luis_espino.pdf

García, G. (2007). El estándar TIA-942. Recuperado 30 de marzo del 2013 de http://www.areadata.com.ar/pdf/El%20standard%20TIA% 20942%20-vds-11-4.pdf

GNS3. (2013). ¿*What is* GNS3? Recuperado 8 de marzo del 2013 de http://www.gns3.net/

Hewlett packard. (2013). Specifications HP blade system C7000. HP. Recuperado el 20 de diciembre del 2012 de http://h8004.www1.hp. com/products/blades/components/enclosures/c-class/c7000/

Honeynet. Recuperado el 21 de mayo del 2013 de http://www.honeynet.org

HP. (2013). Commands VLAN`s. Recuperado 21 de febrero del 2013 de ftp://ftp.hp.com/pub/networking/software/59679955_14.pdf

HP. (2008). Vignolosa. Recuperado el 12 de enero del 2013 de http://www.vignolosa.com.ar/archivos/PDF/HP/GuiadeHPProLiantySto rageWorksv6.pdf

INEN. (2009). Código de práctica para gestión de la seguridad de la información (1ra edición). Instituto ecuatoriano de normalización.

Jurado, C. (2013). VLAN. Recuperado el 19 de febreo del 2013 de http://www.ciscoredes.com/ccna3/90-vlan.html

Martin Isabel. (2008, mayo). Ventajas y desventajas de la virtualización. Vol. 1, página 1. Recuperado el 12 de enero del 2013 de http://www.techweek.es/virtualizacion/techlabs/1003109005901/ventajas-desventajas-virtualizacion.1.html

Multihoming. Recuperado el 19 de abril del 2013 de http://bibing.us.es/proyectos/abreproy/11359/fichero/BGP%252F9.+Multi homing.pdf

Netgear. (2007). Netgear. Recuperado el 18 de diciembre del 2012 de http://netgear.de/images/Wireless_LAN_White_Paper22-17318.pdf

Network-Core.net. (2010). Atributos BGP. Recuperado el 6 de enero del 2013 de http://www.network-core.net/2010/08/atributos-bgp.html

Power and performance data sheet. Recuperado 25 de enero del 2013 de http://www.dell.com/downloads/global/products/pedge/en/DellPowerEdge-R620-750W-E5-2620-40-Family-Data-Sheet.pdf

Que son los tiers en un centro de datos. El ANSI/TIA-942. Recuperado el 23 de marzo del 2013 de http://www.nubeblog.com/2010/10/11/ que-son-los-tiers-en- un-centro-de-datos-el-ansi-tia-942/

Ramírez, C. Francino, R. 5 requisitos para ser cloud computing. Vol. 1, página 1. Recuperado 4 de febrero del 2013 de http://www.qumulos.com/articulos/5-componentes-para-ser-cloud-computing-2/

Ramírez, P. Donoso, F (2006). Metodología ITIL. Recuperado el 10 de mayo del 2013 de http://es.scribd.com/doc/98107732/ITIL-Proceso

Sarubbi J. (2008). Técnicas de defensa comunes bajo variantes del sistema operativo Unix. Recuperado 1 junio del 2013 de

http://es.scribd.com/doc/7103092/Seguridad-Informatica-Tecnicas-de-defensa-comunes-bajo-variantes-del-sistema-operativo-Unix

TIA/EIA-569A. Recuperado el 20 de mayo del 2013 de http://bibdigital.epn.edu.ec/bitstream/15000/9268/6/Cap%205.pdf

TIA. (2009). Development of standards. TIA. Engineering manual. Recuperado el 9 de junio del 2013 de http://www.tiaonline.org /standards/procedures/manuals/documents/tia_eng_manual-5th_ed ition _102009_final.pdf

T3cnocom. (2008). Wireshark. Recuperado 9 de marzo del 2013 de http://t3cnocom.blogspot.com/2009/08/que-es-el-wireshark.html

Velásquez, E. (2009) ¿Qué es la virtualización?. Recuperado 26 de febrero del 2013 de http://www.tecnologiapyme.com/software /que-es-la-virtualización

ANEXOS

Glosario de términos

- **Servidor DHCP (*dynamic host configuration protocol*).-** Es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP. DHCP permite el uso de servidores DHCP para administrar la asignación dinámica de direcciones IP, a los clientes DHCP de la red.

- **SNMP (*simple network management protocol*).-** Es un protocolo de la capa de aplicación que facilita el intercambio de información entre dispositivos de red, logrando así supervisar el funcionamiento de la red, buscar y resolver los problemas, y planear su crecimiento.

- **NAS (*network access server*).-** Es el punto de entrada que permite a los usuarios o clientes acceder a una red. Un NAS está destinado a actuar como una puerta de entrada para proteger el acceso a un recurso protegido.

- **PPP (*point to point protocol*).** - Permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos computadoras.

- **802.1Q.-** Fue un proyecto de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (*trunking*).

- **Enlace Troncal.-** Es un enlace punto a punto entre dos dispositivos de red, el cual transporta más de una VLAN. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre *switches* y *routers.*

- **PDU (*power distribution unit*).-** Es un dispositivo equipado con múltiples salidas, diseñados para distribuir la energía eléctrica, en los racks.

- ***Outsourcing*=** *Outsourcing*, hace referencia a la fuente externa de suministro de servicios; es decir, la subcontratación de operaciones de una compañía a contratistas externos.

- **Servidor *proxy*.**- Es un equipo intermediario situado entre el sistema del usuario e internet. Puede utilizarse para registrar el uso de internet y también para bloquear el acceso a un sitio *web*.

- **Balanceo de carga por destino.-** Se basa en la dirección IP del *host* destino para encaminar los paquetes. Dadas dos rutas hacia la misma red, los paquetes que vayan hacia un *host* destino de dicha red se reenvían por un camino, mientras que los que van destinados a otro *host* se reenvían por el otro camino. Este balance de carga permite enviar los paquetes ordenados, pero puede ocurrir que la ocupación de los enlaces sea desigual.

- **Balanceo de carga por paquete.-** Consiste en cambiar el camino por el que se reenvían los paquetes cada vez que se envía un paquete, de forma que se consigue una ocupación igual de los recursos de los diferentes enlaces. Sin embargo, los paquetes de un mismo flujo llegarán desordenados al destino debido a los diferentes retardos que sufrirán al seguir diferentes rutas.

- **Dominio de *broadcast.-*** Es un tipo de tráfico que está enfocado a todos los dispositivos que pertenezcan lógicamente a un mismo conjunto.

- **Dominio de colisión.-** Es un segmento físico de una en donde es posible que las tramas puedan colisionar unas con otras. Este dominio se origina en capa 2 y es manejado por *switches.*

- **Rutas estíticas.-** Son rutas IP fijas (configuradas manualmente) las cuales no se modifican ante nuevas actualizaciones en la red.

- **Bucle.-** Un bucle es un tipo de estructura de control que permite repetir una o más sentencias múltiples veces.

- **Latencia.-** Es la suma de retardos temporales dentro de una red.

- **RAID 5.-** Utiliza una división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos de un conjunto. Generalmente, el RAID 5 se implementa con soporte *hardware* para el cálculo de la paridad. RAID 5 necesitará un mínimo de 3 discos para ser implementado.

- **802.1Q.-** Permite a múltiples redes compartir de forma transparente el mismo medio físico, sin dificultades de interferencia entre ellas, lo que se conoce como "*trunking*".

- **NAT (*network address translation*).-** Es un mecanismo utilizado por equipos de capa 3 *(router*), para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

Propuesta comercial N°:	QCO-2013-03-8294 V2
Fecha:	Quito, 28 de marzo de 2013
Razón social:	Akros Soluciones Tecnológicas
Dirección:	Av. República y Almagro
Teléfono:	PBX: (02) 3976800, Ext: 217
Solicitado por:	David Yépez / Sistemas
E-mail:	david.yepez@akroscorp.com

Solución propuesta:

SERVICIOS DE BACKBONE DE INTERNET Y DATOS IP-MPLS PARA QUITO

Servicio	Velocidad	Abono mensual USD	Cargo único instalación USD	Plazo contrato	Ubicación origen	Ubicación destino
BACKBONE DE INTERNET QUITO Incluye: - Ultima milla por fibra óptica propiedad de Level 3 - Backbone de Internet sin compartición 1:1 - 2 salidas internacionales con redundancia automática - Router terminal - 8 IP's	6 Mbps	$769	$700	24 meses	POP GLOBAL CROSSING USA	AKROS QUITO
SERVICIO IP-MPLS DE DATOS QUITO Incluye: - Ultima milla por fibra óptica - Router terminal que entrega una puerta LAN	6 Mbps	$639	$700	24 meses	RED IP-MPLS AKROS	AKROS QUITO
SERVICIO IP-MPLS PARA REDUNDANCIA DE ULTIMA MILLA DE DATOS E INTERNET EN QUITO Incluye: - Ultima milla óptica adicional - Equipo terminal para enrutamiento automático de última milla	6 Mbps	$639	$700	24 meses	RED IP-MPLS AKROS	AKROS QUITO

Observaciones:

- Se debe considerar que la capacidad de última milla se configura a 6 Mbps en Quito.
- El SLA será del 99.8%

Condiciones comerciales:

Instalación:	Los cargos de instalación no incluyen obras civiles en el cliente (adecuaciones, ductería, torres, mástil, energía, entre otros).
Cargo de instalación:	50% del valor a la fecha de la firma de esta propuesta, 50% restante dentro de los cinco días posteriores a la puesta en marcha.
Abono mensual:	Se facturará por adelantado, dentro de los cinco primeros días del mes.
Validez de la propuesta:	La presente oferta es válida por 20 días contados a partir de la fecha de entrega de la misma.
Plazo de instalación:	el plazo estimado para la implementación será de (15) días laborables a partir de la recepción por parte de Global Crossing del contrato firmado.
Propiedad de los equipos:	Los equipos empleados por Global Crossing para la prestación del servicio son propiedad de Global Crossing

Impuestos:

Los precios no incluyen los impuestos de ley correspondientes. Los impuestos serán aplicados de conformidad con la legislación vigente

Requerimientos básicos para la instalación a cargo del cliente:

Espacio exterior:	Los equipos exteriores deben contar con espacio suficiente y adecuado, libre de obstáculos e interferencias.
Espacio interior:	Los equipos de interiores requieren espacio adecuado en racks, protección contra humedad, polvo y otros agentes contaminantes y sistema de aire acondicionado.
Acceso y permisos:	Tramitación y obtención de los permisos correspondientes ante la copropiedad de los edificios para la instalación, cuando corresponda.
Obras civiles:	Obras civiles internas y externas según corresponda al servicio (bases, ductos, canaletas, torres, sistemas de tierra, pararrayos, entre otros).
Energía eléctrica:	Provisión de energía eléctrica regulada, conexión a tierra y sistema de respaldo de energía (UPS) en línea en cada una de las ubicaciones, para protección y correcto funcionamiento de equipos.

Aceptación de la propuesta:

La firma del representante legal o funcionario autorizado en esta oferta comercial, se entenderá como la aceptación de las condiciones y términos contenidas en la misma, en virtud de lo cual la presente oferta comercial se convierte de forma automática en una Orden de Servicios, adenda o anexo modificatorio del contrato principal suscrito entre las partes y por tanto forma parte integrante del mismo.

Contrato principal No.	

Firmas:

CLIENTE
Representante legal o
Funcionario autorizado:
Sello de la compañía

Nombre: _____

GLOBALCROSSING
Consultor: Enrique Altamirano León

Global Crossing

Fecha de aceptación de oferta: _____

Quito, 27 de Marzo del 2013

Señor,

David Yépez, representante de la empresa **Akros soluciones tecnológicas**

De nuestras consideraciones:

Es muy placer poder ayudar a su prestigiosa empresa con nuestras soluciones en servicios de transmisión de Datos e Internet de alta velocidad.

Referencia: Propuesta económica para la trasmisión de datos e internet de alta velocidad.

Solución presentada:

Tipo de servicio	Velocidad	Costo instalación	Mensualidad
Canal simétrico con tecnología IP-MPLS con anillos de fibra que incluye: - Redundancia en Backbone con salidas internacionales. - Monitoreo y reportes mensuales del estado del enlace - 4 IP's - Un Router terminal - Ultima milla utilizando fibra óptica	6000 KBPS	$669	$749
Servicio IP-MPLS para redundancia de última milla en internet y datos incluye: - Enlace por fibra óptica adicional. - Equipo de enrutamiento para la automatización de la última milla.	6000 KBPS	$669	$749
Servicio de radio enlace para redundancia de última milla en internet y datos incluye: - Enlace por medio de RF con repetidoras instaladas - Equipo de radiocomunicación para la redundancia en la última milla (encendido manual)	4000 KBPS	$669	$639

Términos y condiciones:
- Los cargos por instalación no incluyen la obra civil.
- Esta oferta tiene una vigencia de 15 días laborables.
- Se debe cancelar el 50% del valor a la firma del contrato y el resto a la conclusión del mismo.
- Todos los equipos terminales son propiedad absoluta de Telconet.
- Los precios antes mencionados, no incluyen los impuestos de ley correspondientes IVA.
- El tiempo de entrega de la presente propuesta será de 6 días laborables.
- UP Time 99.5%
- Tiempo de respuesta del servicio de 35 minutos.

Adicionales:
- Correo con dominio.
- IP fija en la WAN.
- Protección contra virus para las cuentas aperturadas dentro del dominio del Telconet.
- Soporte técnico especializado 24x7.
- Habilitación del puerto 25.
- Posibilidad de crear VPN hacia otra sucursal.
- Funcionalidades compatibles con VOIP.
- Ejecutivo responsable de la atención a la cuenta.
- Reporte de Up time detallado por web.

Atentamente,
Ing, Yesenia Granja
Asesor ejecutivo
Área corporativa

Tel: +593 23963100
Email: yesenia.granja@telconet.ec
Dirección: Av. 12 octubre y F. Salazar Edif. Concord

SURATEL
TRANSMISION DE DATOS

Transmisión de Datos con un alto nivel de Capacidad y Calidad

Quito, 25 de Marzo del 2013

Sr.
David Yépez, Akros soluciones tecnológicas

Presente.-

REF: PROPUESTA ECONOMICA DE TRASMISIÒN DE DATOS E INTERNET

De nuestras consideraciones:

Es muy grato para el **GRUPO TVCABLE - SURATEL**, presentar a su distinguida Empresa, nuestras Soluciones en Servicios de Transmisión de Datos e Internet:

SOLUCIONES EN COMUNICACION

Ventajas del Internet Corporativo: Acceso de alta velocidad al Internet, conexión de alta disponibilidad y provisión de ancho de banda, posibilidad de crear VPN hacia sucursales, aplicaciones voz IP, Ejecutivo de cuenta asignado, soporte especializado y monitoreo 24horas.

Tecnología IP/MPLS, ETHERNET SWITCH y SDH a nivel de Backbone con red de anillos 1Gb, STM-16 y STM1, acceso a Usuario con Servicios IPVPN, Ethernet Switched, Clear Channel y Frame Relay.

SURATEL es consciente que usted no se puede permitir que su servicio de Transmisión de Datos le falle. Esta es la razón por la que **SURATEL** muestra su compromiso a través del Service Level Agreement (SLA), que proporciona contoda certeza la disponibilidad y el rendimiento de su enlace. Provisto siempre de un backup en nuestros nodos y redundancia de última milla (opcional). A continuación detallamos las ventajas de nuestros planes PREMIUM.

CALIDAD DEL SERVICIO PREMIUM:

- Disponibilidad del enlace anual 99.5%
- Tiempo de respuesta a pedidos de servicio: 30 Minutos.
- Tiempo máximo de resolución de problemas de enlace final: 2 horas
- Tiempo máximo de resolución de problemas de red troncal: 4 horas
- Soporte técnico: 24 horas al día. Técnico asignado al cliente
- Supervisión del enlace 24 horas por parte del cliente y reportes mensuales por parte de nosotros.
- Ejecutivos responsables asignados a su cuenta. Atención cliente, Técnico, Cobranzas, Comercial.

SERVICIOS OFERTADOS

- **CABLENET IP – INTERNET CORPORATIVO**
- Tecnología **IP/MPLS** a nivel de Ultima Milla (aumento de Velocidad para nuestros clientes)
- Enlace directo desde el cliente hasta nuestro Nodo con salida Internacional por Fibra Optica.
- Diferenciación de Servicios a nivel de Ultima Milla: Permite priorizar (QoS) el tráfico de la aplicación del Cliente, respecto a la navegación y otras aplicaciones del usuario final (voz) sobre el Internet
- Administración del Tráfico de cada usuario
- Monitoreo 24 horas por parte del cliente y reportes mensuales enviados por Técnico Responsable de su cuenta.
- Redundancia en Backbone con protección 1 + 1 a nivel de túneles IP
- Redundancia en Ultima Milla (opcional)
- Canal dedicado desde el nodo más cercano hasta el cliente, última milla propia (SURATEL)

Solución : CARACTERISTICAS DSL / CANAL SIMÉTRICO: Por la naturaleza de las aplicaciones que realizan se dispone de gran ancho de banda en troncales y salida Internacional, disponemos de aumento de velocidad para clientes directos de SURATEL sin congestiones, es por ello que su canal estaría libre de congestiones, garantizándoles siempre los **6000kbps.**

Canal: **6000/6000Kbps. (INTERNET CABLENET IP CORPORATIVO CNET)**

Instalación: **$150,00**
Renta Mensual:

$549,90 1,1

Este es un canal dedicado, que garantiza el 100% de la velocidad contratada

Última milla: Alámbrico SURATEL
Up Time anual: 99.5%
Equipos: CTUR
Tecnología: IPMPLS CON AUMENTOS CONTINUOS DE VELOCIDAD

Redundancia : CARACTERISTICAS DSL / CANAL SIMÉTRICO: Por la naturaleza de las aplicaciones que realizan se dispone de gran ancho de banda en troncales y salida Internacional, disponemos de aumento de velocidad para clientes directos de SURATEL sin congestiones, es por ello que su canal estaría libre de congestiones, garantizándoles siempre los **6000kbps.**

Canal: **6000/6000Kbps. (REDUNDANCIA INTERNET CABLENET IP CORPORATIVO CNET)**

Instalación: **$150,00**
Renta mensual:

$549,90 1,1

Este es un canal dedicado, que garantiza el 100% de la velocidad contratada

Ultima milla: Alámbrico SURATEL
Up Time anual: 99.5%
Equipos: CTUR
Tecnología: IPMPLS CON AUMENTOS CONTINUOS DE VELOCIDAD

Opciones de pago por instalación:

- Puede diferirla a 12 meses con intereses con tarjeta de crédito.
- En caso de tener la última milla con SURATEL, pero el servicio con otro proveedor, el costo de instalación es CERO
- Pago contra factura
- Todos los precios no incluyen IVA

SERVICIOS ADICIONALES:

- Incluye Última Milla Corporativa + Internet Corporativo
- Correo con Dominio nombre@tvcable.net.ec

GRUPO TVCABLE
Más para tu vida

Propuesta de Housing en Datacenter Quito o Guayaquil de Telconet

Cliente: AKROS

Atención a: Ing. David Yépez

Elaborado por: Cecilia Chinacalle

Fecha: 30-03-2013.

Precio de la Solución

Número de Unidades Us Iniciales: Rack Estándar: 21 Unidades (compartido)

Costo de Alquiler	($150 c/unidad)	$1000,00
Costo de 12.5 KVAs (hasta 15 Kvas: $280 c/u) en el Rack		$ 780,00
Costo de conectividad Datos Local 1 Mbps		$ 129.00
Costo de conectividad Internet desde DC 1 Mbps		$ 120.00
Soporte Manos Remotas (Manos Remotas Predefinidas (8 Interacciones de hasta 5 min)		$ 80.00
Total Mensual		**$ 2109.00**
Costo Instalación para 21 Us. Standard (Incluye instalación eléctrica)		$ 660,00
Costo Instalación Conectividad Datos 1 Mbps		$ 70,00
Costo Instalación Conectividad Internet desde DC		$ 70,00
Total Instalación		**$ 800,00**
Fecha de Implementación en DC /UIO:	**15 días después de la firma del contrato**	
Tiempo mínimo de contratación:		3 años

Innovación y Garantía de Calidad

- **GNS3**

1. Implementación del enlace de backup utilizando BGP, PRB y Local preference con routers de los proveedores en Akros.

Tarea 1

Realizar las configuraciones correspondientes en el router de Akros_Level3, para su comunicación con los routers Akros_Telconet y Level3 utilizando los siguientes comandos:

Pasos	Comando	Propósito
1	Akros_Level3>enable	Ingresa al modo privilegiado
2	Akros_Level3#conf ter	Ingresa al modo de configuración global
3	Akros_Level3 (config)#inter lo 0	Ingresa al modo de configuración de la interfaz
4	Akros_Level3 (config-if)#ip add 10.5.93.1 255.255.255.0	Coloca una IP a la interfaz
5	Akros_Level3 (config-if)#exit	Regresa al modo de configuración global
6	Akros_Level3 (config)#inter fa 0/0	Ingresa al modo de configuración de la interfaz
7	Akros_Level3 (config-if)#ip add 182.168.20.10 255.255.255.0	Coloca una IP a la interfaz
8	Akros_Level3 (config-if)#no shut	Activa la interfaz
9	Akros_Level3 (config-if)#exit	Regresa al modo de configuración global
10	Akros_Level3 (config)#inter fa 1/0	Ingresa al modo de configuración de la interfaz
11	Akros_Level3 (config-if)#ip add 182.167.20.10 255.255.255.0	Coloca una IP a la interfaz
12	Akros_Level3 (config-if)#no shut	Activa la interfaz
13	Akros_Level3 (config-if)#exit	Regresa al modo de configuración global
14	Akros_Level3 (config)#router bgp 11	Ingresa al modo de configuración
15	Akros_Level3 (config-router)#no sync	Deshabilita la sincronización entre BGP e IGP.
16	Akros_Level3 (config-router)#bgp log-neighbor-changes	Habilita el registro de BGP
17	Akros_Level3 (config-router)#network 10.5.93.0 mask 255.255.255.0 Akros_Level3 (config-router)#network 10.5.94.0 mask 255.255.255.0	Da a conocer a BGP la red interna del router
18	Akros_Level3 (config-router)#neighbor	Establece vecindad con la

	182.168.20.11 remote-as 10 Akros_Level3 (config-router)#neighbor 182.167.20.11 remote-as 11	red de los routers vecinos
19	Akros_Level3 (config-router)#neighbor 182.167.20.11 next-hop-self	Habilita el siguiente salto en la tabla de BGP
20	Akros_Level3 (config-router)#neighbor 182.168.20.11 route-map AS-10-INCOMING in	Establece una mapa de rutas para los anuncios de entrada
21	Akros_Level3 (config-router)#neighbor 182.168.20.11 route-map AS-10-OUTGOING out	Establece una mapa de rutas para los anuncios de salida
22	Akros_Level3 (config-router)#no auto-summary	Deshabilita el proceso de agregación automática
23	Akros_Level3 (config-router)#exit	Regresa al modo de configuración global
24	Akros_Level3 (config)#ip as-path access-list 1 permit ^10$	Crea una lista de acceso o (ACL) IP para admitir rutas originadas del AS mencionado
25	Akros_Level3 (config)#access list 50 permit 10.5.94.0 0.0.0.255 Akros_Level3 (config)#access list 60 permit 10.5.93.0 0.0.0.255	Agrega una ACL como control de tráfico en el equipo
26	Akros_Level3 (config)#route-map AS-10-INCOMING permit 50	Permite el ingreso de tráfico del AS 10 por la ACL 50
27	Akros_Level3 (config-route-map)#match as-path 1	Une el AS con la ACL
28	Akros_Level3 (config-route-map)#set local-preference 200	Añade una preferencia al enlace. Un camino con preferencia mayor se convierte en enlace principal
29	Akros_Level3 (config-route-map)# exit	Regresa al modo de configuracion global
30	Akros_Level3 (config)#route-map AS-10-OUTGOING permit 50	Permite el ingreso de tráfico del AS 10 por la ACL 50
31	Akros_Level3 (config-route-map)# match ip address 50	Distribuye cualquier ruta que tenga la dirección de destino IP permitida en la ACL
32	Akros_Level3 (config-route-map)# set as-path prepend 11	Manipula el atributo as-path de BGP a través del AS local
33	Akros_Level3 (config-route-map)#exit	Regresa al modo de configuración global
34	Akros_Level3 (config)#route-map AS-10-OUTGOING permit 60	Permite la salida de tráfico del AS 10 por la ACL 60
35	Akros_Level3 (config-route-map)#match ip address 60	Distribuye cualquier ruta que tenga la dirección de destino IP permitida en la ACL
36	Akros_Level3 (config-route-map)#exit	Regresa al modo de configuración global
37	Akros_Level3 (config)#ip as-path access-list 50 permit ^$	Permite recibir todas las rutas originadas por los distintos AS

38	Akros_Level3 (config)#route-map localonly permit 50	Filtra las rutas recibidas por un ISP para que no sean anunciadas hacia el otro ISP
39	Akros_Level3 (config-route-map)#match as-path 50	Une el AS con la ACL
40	Akros_Level3 (config-route-map)#end	Regresa al modo de configuración privilegio
41	Akros_Level3#sh running-config	Muestra la configuración del router
42	Akros_Level3#sh ip bgp	Despliega las entradas de BGP en una tabla de ruteo
43	Akros_Level3#sh ip bgp all summary	Despliega el estado de las conexiones establecidas por BGP
44	Akros_Level3# sh ip as-path-access-list	Despliega el contenido actual del AS con relación a la ACL
45	Akros_Level3#ping 182.168.20.11 Akros_Level3#ping 182.167.20.11 Akros_Level3#ping 10.5.94.1 Akros_Level3#ping 10.5.96.1 Akros_Level3#ping 10.5.95.1 source 10.5.93.1	Verifica la conexión entre los enlaces
46	Akros_Level3#wr	Guarda la configuración realizada

Configuraciones finales router Akros_Level3

Akros_Level3#sh running-config

```
interface Loopback0
 ip address 10.5.93.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 182.168.20.10 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 182.167.20.10 255.255.255.0
 duplex auto
 speed auto
!
router bgp 11
 no synchronization
 bgp log-neighbor-changes
 network 10.5.93.0 mask 255.255.255.0
 network 10.5.94.0 mask 255.255.255.0
 neighbor 182.167.20.11 remote-as 11
 neighbor 182.167.20.11 next-hop-self
 neighbor 182.168.20.11 remote-as 10
 neighbor 182.168.20.11 route-map AS-10-INCOMING in
 neighbor 182.168.20.11 route-map AS-10-OUTGOING out
 no auto-summary
!
no ip http server
no ip http secure-server
```

```
ip classless
!
ip as-path access-list 1 permit ^10$
ip as-path access-list 50 permit ^$
!
access-list 50 permit 10.5.93.0 0.0.0.255
access-list 60 permit 10.5.94.0 0.0.0.255
!
route-map AS-10-INCOMING permit 50
 match as-path 1
 set local-preference 200
!
route-map AS-10-OUTGOING permit 50
 match ip address 50
 set as-path prepend 11
!
route-map AS-10-OUTGOING permit 60
 match ip address 60
!
route-map localonly permit 50
 match as-path 50
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
Akros_Level3#sh ip bgp
BGP table version is 15, local router ID is 10.5.93.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.5.93.0/24     0.0.0.0                  0         32768 i
*>i10.5.94.0/24     182.167.20.11            0    100      0 i
*> 10.5.95.0/24     182.168.20.11            0             0 10 i
*>i10.5.96.0/24     182.167.20.11            0    100      0 9 i
*                   182.168.20.11                          0 10 9 i
Akros_Level3#sh ip bgp all summary
For address family: IPv4 Unicast
BGP router identifier 10.5.93.1, local AS number 11
BGP table version is 15, main routing table version 15
4 network entries using 468 bytes of memory
5 path entries using 260 bytes of memory
6/4 BGP path/bestpath attribute entries using 744 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1544 total bytes of memory
BGP activity 6/2 prefixes, 10/5 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
182.167.20.11   4    11      54      63       15    0    0 00:04:23        2
182.168.20.11   4    10      67      62       15    0    0 00:42:09        2
Akros_Level3#sh ip  as-path-access-list
```

AS path access list 1
permit ^10$
AS path access list 50
permit ^$
Akros_Level3#ping 182.168.20.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.168.20.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/105/124 ms
Akros_Level3#ping 182.167.20.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.167.20.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/105/122 ms
Akros_Level3#ping 10.5.94.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.167.20.11, timeout is 3 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/105/127 ms
Akros_Level3#ping 10.5.96.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.167.20.11, timeout is 3 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/105/127 ms
Akros_Level3#ping 10.5.95.1 source 10.5.93.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.167.20.11, timeout is 3 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/105/128 ms

Pruebas de redundancia

Akros_Level3(config)#interface fastEthernet 1/0
Akros_Level3(config-if)#shutdown
Akros_Level3(config-if)#
*Mar 1 00:25:38.003: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state to administratively down
*Mar 1 00:25:39.003: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to down
*Mar 1 00:28:16.387: %BGP-5-ADJCHANGE: neighbor 182.167.20.11 Down BGP Notification sent
*Mar 1 00:28:16.387: %BGP-3-NOTIFICATION: sent to neighbor 182.167.20.11 4/0 (hold time expired) 0 bytes
Akros_Telconet#ping 10.5.95.1 source 10.5.94.1 repeat 200
Type escape sequence to abort.
Sending 200, 100-byte ICMP Echos to 10.5.95.1, timeout is 2 seconds:
Packet sent with a source address of 10.5.94.1
!!!
!!!.....
..... !!!!!!!!!!!!!!!!
Level3#ping 10.5.94.1 source 10.5.95.1 repeat 200
Type escape sequence to abort.
Sending 200, 100-byte ICMP Echos to 10.5.94.1, timeout is 2 seconds:
Packet sent with a source address of 10.5.95.1
!!!
!!!.....
.....!!!!!!!!!!
Telconet#ping 10.5.93.1 source 10.5.96.1 repeat 200

```
Type escape sequence to abort.
Sending 200, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
Packet sent with a source address of 10.5.96.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
.....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Tarea 2

Realizar las configuraciones correspondientes en el router de Akros_Telconet, para su comunicación con los routers de Akros_level3 y Telconet utilizando los siguientes comandos:

Pasos	Comando	Propósito
1	Akros_Telconet>enable	Ingresa al modo privilegiado
2	Akros_Telconet #conf ter	Ingresa al modo de configuración global
3	Akros_Telconet (config)#inter lo 0	Ingresa al modo de configuración de la interfaz
4	Akros_Telconet (config-if)#ip add 10.5.94.1 255.255.255.0	Coloca una IP a la interfaz
5	Akros_Telconet (config-if)#exit	Regresa al modo de configuración global
6	Akros_Telconet (config)#inter fa 0/0	Ingresa al modo de configuración de la interfaz
7	Akros_Telconet (config-if)#ip add 182.169.20.10 255.255.255.0	Coloca una IP a la interfaz
8	Akros_Telconet (config-if)#no shut	Activa la interfaz
9	Akros_Telconet (config-if)#exit	Regresa al modo de configuración global
10	Akros_Telconet (config)#inter fa 1/0	Ingresa al modo de configuración de la interfaz
11	Akros_Telconet (config-if)#ip add 182.167.20.11 255.255.255.0	Coloca una IP a la interfaz
12	Akros_Telconet (config-if)#no shut	Activa la interfaz
13	Akros_Telconet (config-if)#exit	Regresa al modo de configuración global
14	Akros_Telconet (config)#router bgp 11	Ingresa al modo de configuración
15	Akros_Telconet (config-router)#no sync	Deshabilita la sincronización entre BGP e IGP.
16	Akros_Telconet (config-router)#bgp log-neighbor-changes	Habilita el registro de BGP
17	Akros_Telconet (config-router)#network 10.5.93.0 mask 255.255.255.0 Akros_Telconet (config-router)#network 10.5.94.0 mask 255.255.255.0	Da a conocer a BGP la red interna del router
18	Akros_Telconet (config-router)#neighbor 182.169.20.11 remote-as 9	Establece vecindad con la red de los routers vecinos

	Akros_Telconet (config-router)#neighbor 182.167.20.10 remote-as 11	
19	Akros_Telconet (config-router)#neighbor 182.167.20.10 next-hop-self	Habilita el siguiente salto en la tabla de BGP
20	Akros_Telconet (config-router)#neighbor 182.169.20.11 route-map AS-9-INCOMING in	Establece una mapa de rutas para los anuncios de entrada
21	Akros_Telconet (config-router)#neighbor 182.169.20.11 route-map AS-9-OUTGOING out	Establece una mapa de rutas para los anuncios de salida
22	Akros_Telconet (config-router)#no auto-summary	Deshabilita el proceso de agregación automática
23	Akros_Telconet (config-router)#exit	Regresa al modo de configuración global
24	Akros_Telconet (config)#ip as-path access-list 1 permit ^9$	Crea una lista de acceso o (ACL) IP para admitir rutas originadas del AS mencionado
25	Akros_Telconet (config)#access list 50 permit 10.5.93.0 0.0.0.255 Akros_Telconet (config)#access list 60 permit 10.5.94.0 0.0.0.255	Agrega una ACL como control de tráfico en el equipo
26	Akros_Telconet (config)#route-map AS-9-INCOMING permit 50	Permite el ingreso de tráfico del AS 10 por la ACL 50
27	Akros_Telconet (config-route-map)#match as-path 1	Une el AS con la ACL
28	Akros_Telconet (config-route-map)#set local-preference 150	Añade una preferencia al enlace. Un camino con preferencia mayor se convierte en enlace principal
29	Akros_Telconet (config-route-map)#exit	Regresa al modo de configuración global
30	Akros_Telconet (config)#route-map AS-9-OUTGOING permit 50	Permite la salida de tráfico del AS 10 por la ACL 50
31	Akros_Telconet (config-route-map)#match ip address 50	Distribuye cualquier ruta que tenga la dirección de destino IP permitida en la ACL
32	Akros_Telconet (config-route-map)#set as-path prepend 11	Manipula el atributo as-path de BGP a través del AS local
33	Akros_Telconet (config-route-map)#exit	Regresa al modo de configuración global
34	Akros_Telconet (config)#route-map AS-9-OUTGOING permit 60	Permite la salida de tráfico del AS 10 por la ACL 60
35	Akros_Telconet (config-route-map)#match ip address 60	Distribuye cualquier ruta que tenga la dirección de destino IP permitida en la ACL
36	Akros_Telconet (config-route-map)#exit	Regresa al modo de configuración global
37	Akros_Telconet (config)#ip as-path access-list 50 permit ^$	Permite recibir todas las rutas originadas por los distintos AS
38	Akros_Telconet (config)#route-map localonly permit	Filtra las rutas recibidas por

	50	un ISP para que no sean anunciadas hacia el otro ISP
39	Akros_Telconet (config-route-map)#match as-path 50	Une el AS con la ACL
40	Akros_Telconet (config-route-map)#end	Regresa al modo de configuración privilegio
41	Akros_Telconet #sh running-config	Muestra la configuración del router
42	Akros_Telconet #sh ip bgp	Despliega las entradas de BGP en una tabla de ruteo
43	Akros_Telconet #sh ip bgp all summary	Despliega el estado de las conexiones establecidas por BGP
44	Akros_Telconet # sh ip as-path-access-list	Despliega el contenido actual del AS con relación a la ACL
45	Akros_Telconet #ping 182.169.20.11 Akros_Telconet #ping 182.167.20.10 Akros_Telconet #ping 10.5.93.1 Akros_Telconet #ping 10.5.96.1 Akros_Telconet #ping 10.5.95.1 source 10.5.94.1	Verifica la conexión entre los enlaces
46	Akros_Telconet #wr	Guarda la configuración realizada

Configuraciones finales router Akros_Telconet

Akros_Telconet#sh running-config

```
interface Loopback0
 ip address 10.5.94.1 255.255.255.0
!
interface FastEthernet1/0
 ip address 182.167.20.11 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
router bgp 11
 no synchronization
 bgp log-neighbor-changes
 network 10.5.93.0 mask 255.255.255.0
 network 10.5.94.0 mask 255.255.255.0
 neighbor 182.167.20.10 remote-as 11
 neighbor 182.167.20.10 next-hop-self
 neighbor 182.169.20.11 remote-as 9
 neighbor 182.169.20.11 route-map AS-10-INCOMING in
 neighbor 182.169.20.11 route-map AS-10-OUTGOING out
 no auto-summary
!
no ip http server
```

```
no ip http secure-server
ip classless
!
ip as-path access-list 1 permit ^9$
ip as-path access-list 50 permit ^$
!
access-list 50 permit 10.5.93.0 0.0.0.255
access-list 60 permit 10.5.94.0 0.0.0.255
!
route-map AS-9-OUTGOING permit 50
 match ip address 50
 set as-path prepend 11
!
route-map AS-9-OUTGOING permit 60
 match ip address 60
!
route-map AS-9-INCOMING permit 50
 match as-path 1
 set local-preference 150
!
route-map localonly permit 50
 match as-path 50!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Akros_Telconet#sh ip bgp

```
BGP table version is 15, local router ID is 10.5.94.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i10.5.93.0/24     182.167.20.10            0    100      0 i
*> 10.5.94.0/24     0.0.0.0                  0         32768 i
*>i10.5.95.0/24     182.167.20.10            0    100      0 10 i
*                   182.169.20.11                          0 9 10 i
*> 10.5.96.0/24     182.169.20.11            0             0 9 i
```

Akros_Telconet#sh ip bgp all summary

```
For address family: IPv4 Unicast
BGP router identifier 10.5.94.1, local AS number 11
BGP table version is 15, main routing table version 15
4 network entries using 468 bytes of memory
5 path entries using 260 bytes of memory
6/4 BGP path/bestpath attribute entries using 744 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1544 total bytes of memory
BGP activity 6/2 prefixes, 10/5 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
182.167.20.10   4    11     113     121       15    0    0 01:03:04        2
182.169.20.11   4     9     125     120       15    0    0 01:40:52        2
```

Akros_Telconet#sh ip as-path-access-list

AS path access list 1
   permit ^9$
AS path access list 50
   permit ^$
Akros_Telconet#ping 182.169.20.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.169.20.11, timeout is 3 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 94/105/124 ms
Akros_Telconet#ping 182.167.20.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.167.20.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 95/103/122 ms
Akros_Telconet#ping 10.5.93.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/48 ms
Akros_Telconet#ping 10.5.96.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/49 ms
Akros_Telconet#ping 10.5.95.1 source 10.5.94.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/37/49 ms

Pruebas de redundancia

Akros_Level3(config)#interface fastEthernet 1/0
Akros_Level3(config-if)#shutdown
Akros_Level3(config-if)#
*Mar 1 01:48:53.439: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state to administratively down
*Mar 1 01:48:54.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to down
*Mar 1 01:51:38.907: %BGP-5-ADJCHANGE: neighbor 182.167.20.11 Down BGP Notification sent
*Mar 1 01:51:38.907: %BGP-3-NOTIFICATION: sent to neighbor 182.167.20.11 4/0 (hold time expired) 0 bytes
Akros_Telconet#ping 10.5.95.1 source 10.5.94.1 repeat 220
Type escape sequence to abort.
Sending 220, 100-byte ICMP Echos to 10.5.95.1, timeout is 2 seconds:
Packet sent with a source address of 10.5.94.1
!!!
!!!
!!!
Level3#ping 10.5.94.1 source 10.5.95.1 repeat 220
Type escape sequence to abort.
Sending 220, 100-byte ICMP Echos to 10.5.94.1, timeout is 2 seconds:
Packet sent with a source address of 10.5.95.1
!!!
!!!
!!!
Telconet#ping 10.5.93.1 source 10.5.96.1 repeat 220

```
Type escape sequence to abort.
Sending 220, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
Packet sent with a source address of 10.5.96.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!.....................................................................
.....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Tarea 3

Realizar las configuraciones correspondientes en el router de Level3, para su comunicación con el router de Akros_level3 utilizando los siguientes comandos:

Pasos	Comando	Propósito
1	Level3>enable	Ingresa al modo privilegiado
2	Level3#conf ter	Ingresa al modo de configuración global
3	Level3 (config)#inter lo 0	Ingresa al modo de configuración de la interfaz
4	Level3 (config-if)#ip add 10.5.95.1 255.255.255.0	Coloca una IP a la interfaz
5	Level3(config-if)#exit	Regresa al modo de configuración global
6	Level3(config)#inter fa 0/0	Ingresa al modo de configuración de la interfaz
7	Level3 (config-if)#ip add 182.168.20.11 255.255.255.0	Coloca una IP a la interfaz
8	Level3 (config-if)#no shut	Activa la interfaz
9	Level3(config-if)#exit	Regresa al modo de configuración global
10	Level3(config)#inter fa 1/0	Ingresa al modo de configuración de la interfaz
11	Level3 (config-if)#ip add 182.170.20.10 255.255.255.0	Coloca una IP a la interfaz
12	Level3 (config-if)#no shut	Activa la interfaz
13	Level3(config-if)#exit	Regresa al modo de configuración global
14	Level3(config)#router bgp 10	Ingresa al modo de configuración
15	Level3(config-router)#no sync	Deshabilita la sincronización entre BGP e IGP.
16	Level3 (config-router)#bgp log-neighbor-changes	Habilita el registro de BGP
17	Level3(config-router)#network 10.5.95.0 mask 255.255.255.0	Da a conocer a BGP la red interna del router
18	Level3 (config-router)#neighbor 182.168.20.10 remote-as 11	Establece vecindad con la red de los routers vecinos
19	Level3 (config-router)#neighbor 182.170.20.11 remote-as 9	Establece vecindad con la red de los routers vecinos
20	Level3 (config-router)#neighbor 182.168.20.10 next-hop-self	Habilita el siguiente salto en la tabla de BGP
21	Level3 (config-router)#end	Regresa al modo de

		configuración privilegio
22	Level3#sh running-config	Muestra la configuración del router
23	Level3#sh ip bgp	Despliega las entradas de BGP en una tabla de ruteo
24	Level3#sh ip bgp all summary	Despliega el estado de las conexiones establecidas por BGP
25	Level3#ping 182.168.20.10 Level3#ping 182.170.20.11 Level3#ping 10.5.93.1 Level3#ping 10.5.96.1 Level3#ping 10.5.94.1 source 10.5.95.1	Verifica la conexión entre los enlaces
26	Level3#wr	Guarda la configuración realizada

Configuraciones finales router Level3

Level3#sh running-config

```
interface Loopback0
 ip address 10.5.95.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 182.168.20.11 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 182.170.20.10 255.255.255.0
 duplex auto
 speed auto
!
router bgp 10
 no synchronization
 bgp log-neighbor-changes
 network 10.5.95.0 mask 255.255.255.0
 neighbor 182.168.20.10 remote-as 11
 neighbor 182.170.20.11 remote-as 9
 no auto-summary
!
ip http server
no ip http secure-server
ip classless
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Level3#sh ip bgp

```
BGP table version is 12, local router ID is 10.5.95.1
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  10.5.93.0/24     182.170.20.11                          0 9 11 i
*>                  182.168.20.10            0             0 11 i
*> 10.5.94.0/24     182.168.20.10                          0 11 i
*                   182.170.20.11                          0 9 11 i
*> 10.5.95.0/24     0.0.0.0                  0         32768 i
*  10.5.96.0/24     182.168.20.10                          0 11 9 i
*>                  182.170.20.11            0             0 9 i
Level3#show ip bgp all summary
For address family: IPv4 Unicast
BGP router identifier 10.5.95.1, local AS number 10
BGP table version is 12, main routing table version 12
4 network entries using 468 bytes of memory
7 path entries using 364 bytes of memory
7/4 BGP path/bestpath attribute entries using 868 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1796 total bytes of memory
BGP activity 4/0 prefixes, 16/9 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
182.168.20.10   4    11     146     150       12    0    0 02:03:50        3
182.170.20.11   4     9     146     146       12    0    0 02:03:54
Level3#ping 182.168.20.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.168.20.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/74/100 ms
Level3#ping 182.170.20.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.170.20.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/29/40 ms
Level3#ping 10.5.93.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/36 ms
Level3#ping 10.5.96.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/29/43 ms
Level3#ping 10.5.94.1 source 10.5.95.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/29/39 ms
```

Tarea 4

Realizar las configuraciones correspondientes en el router de Telconet, para su comunicación con el router de Akros_Telconet utilizando los siguientes comandos:

Pasos	Comando	Propósito
1	Telconet>enable	Ingresa al modo privilegiado
2	Telconet #conf ter	Ingresa al modo de configuración global
3	Telconet (config)#inter lo 0	Ingresa al modo de configuración de la interfaz
4	Telconet (config-if)#ip add 10.5.96.1 255.255.255.0	Coloca una IP a la interfaz
5	Telconet (config-if)# exit	Regresa al modo de configuración global
6	Telconet (config)#inter fa 0/0	Ingresa al modo de configuración de la interfaz
7	Telconet (config-if)#ip add 182.169.20.11 255.255.255.0	Coloca una IP a la interfaz
8	Telconet (config-if)#no shut	Activa la interfaz
9	Telconet (config-if)#exit	Regresa al modo de configuración global
10	Telconet (config)#inter fa 1/0	Ingresa al modo de configuración de la interfaz
11	Telconet (config-if)#ip add 182.170.20.11 255.255.255.0	Coloca una IP a la interfaz
12	Telconet (config-if)#no shut	Activa la interfaz
13	Telconet (config-if)#exit	Regresa al modo de configuración global
14	Telconet (config)#router bgp 9	Ingresa al modo de configuración
15	Telconet (config-router)#no sync	Deshabilita la sincronización entre BGP e IGP.
16	Telconet (config-router)#bgp log-neighbor-changes	Habilita el registro de BGP
17	Level3(config-router)#network 10.5.96.0 mask 255.255.255.0	Da a conocer a BGP la red interna del router
18	Telconet (config-router)#neighbor 182.169.20.10 remote-as 11	Establece vecindad con la red de los routers vecinos
19	Level3 (config-router)#neighbor 182.170.20.10 remote-as 10	Establece vecindad con la red de los routers vecinos
20	Telconet (config-router)#neighbor 182.169.20.10 next-hop-self	Habilita el siguiente salto en la tabla de BGP
21	Telconet (config-router)#end	Regresa al modo de configuración privilegio
22	Telconet #sh running-config	Muestra la configuración del router
23	Telconet #sh ip bgp	Despliega las entradas de

		BGP en una tabla de ruteo
24	Telconet #sh ip bgp all summary	Despliega el estado de las conexiones establecidas por BGP
25	Telconet #ping 182.169.20.10 Telconet #ping 182.170.20.10 Telconet #ping 10.5.94.1 Telconet #ping 10.5.96.1 Telconet #ping 10.5.93.1 source 10.5.96.1	Verifica la conexión entre los enlaces
26	Telconet #wr	Guarda la configuración realizada

Configuraciones finales router Telconet

Telconet#sh running-config

```
interface Loopback0
 ip address 10.5.96.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 182.169.20.11 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 182.170.20.11 255.255.255.0
 duplex auto
 speed auto
!
router bgp 9
 no synchronization
 bgp log-neighbor-changes
 network 10.5.96.0 mask 255.255.255.0
 neighbor 182.169.20.10 remote-as 11
neighbor 182.170.20.10 remote-as 10
 no auto-summary
!
ip http server
no ip http secure-server
ip classless
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Telconet#sh ip bgp

```
BGP table version is 12, local router ID is 10.5.96.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.5.93.0/24     182.169.20.10                          0 11 i
```

```
*                    182.170.20.10                    0 10 11 i
*  10.5.94.0/24      182.170.20.10                    0 10 11 i
*>                   182.169.20.10          0         0 11 i
*  10.5.95.0/24      182.169.20.10                    0 11 10 i
*>                   182.170.20.10          0         0 10 i
*> 10.5.96.0/24     0.0.0.0                0        32768 i
Telconet#show ip bgp all summary
For address family: IPv4 Unicast
BGP router identifier 10.5.96.1, local AS number 9
BGP table version is 12, main routing table version 12
4 network entries using 468 bytes of memory
7 path entries using 364 bytes of memory
7/4 BGP path/bestpath attribute entries using 868 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
BGP activity 4/0 prefixes, 16/9 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
182.169.20.10   4    11     160     164       12    0    0 02:17:15        3
182.170.20.10   4    10     160     160       12    0    0 02:17:18        3
Telconet#ping 182.169.20.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.169.20.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 65/74/100 ms
Telconet#ping 182.170.20.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.170.20.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/29/32 ms
Telconet#ping 10.5.95.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.95.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/44 ms
Telconet#ping 10.5.94.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.95.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/35/46 ms
Telconet#ping 10.5.93.1 source 10.5.96.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.95.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 34/32/48 ms
```

2. Implementación del enlace de backup utilizando rutas estáticas, IP SLA y Track con un router propietario de Akros

Tarea 1

Realizar las configuraciones correspondientes en el router de NAP, para su comunicación con el router Akros utilizando los siguientes comandos:

Pasos	Comando	Propósito
1	NAP>enable	Ingresa al modo privilegiado

2	NAP #conf ter	Ingresa al modo de configuración global
3	NAP (config)#inter lo 0	Ingresa al modo de configuración de la interfaz
4	NAP (config-if)#ip add 10.5.93.1 255.255.255.0	Coloca una IP a la interfaz
5	NAP (config-if)#exit	Regresa al modo de configuración global
6	NAP (config)#inter fa 0/0	Ingresa al modo de configuración de la interfaz
7	NAP s (config-if)#ip add 182.168.20.10 255.255.255.0	Coloca una IP a la interfaz
8	NAP (config-if)#no shut	Activa la interfaz
9	NAP (config-if)#exit	Regresa al modo de configuración global
10	NAP (config)#inter fa 1/0	Ingresa al modo de configuración de la interfaz
11	NAP (config-if)#ip add 182.169.20.10 255.255.255.0	Coloca una IP a la interfaz
12	NAP (config-if)#no shut	Activa la interfaz
13	NAP (config-if)#exit	Regresa al modo de configuración global
14	NAP (config)#ip route 0.0.0.0 0.0.0.0 182.168.20.11 NAP (config)#ip route 10.5.96.0 255.255.255.0 182.169.20.11	Añade rutas estáticas
15	NAP (config)#ip sla monitor 1	Ingresa a la administración del ip sla
16	NAP (config-sla-monitor)#type echo protocol iplcmpEcho 10.5.94.1 source-ip 10.5.93.1	Habilita el envío de paquetes ICMP a través de la IP de destino y el enlace de origen
17	NAP (config-sla-monitor-echo)#frequency 3	Setea la velocidad en que se repite el envío de paquetes ICMP al siguiente salto
18	NAP (config-sla-monitor-echo)#timeout 999	Establece la cantidad de tiempo (milisegundos) en que IP sla esperara una respuesta de su paquete de solicitud
19	NAP (config-sla-monitor-echo)#threshold 500	Determina el umbral ascendente que almacena el historial de operación de IP sla
20	NAP (config-sla-monitor-echo)#exit	Regresa al modo de configuración global
21	NAP (config)#ip sla monitor schedule 1 start-time now life forever	Configura los parámetros de programación para la operación de IP sla
22	NAP (config-router)#end	Regresa al modo privilegio
23	NAP #sh running-config	Muestra la configuración del router

24	NAP #sh ip sla monitor statistics	Muestra la cantidad de intentos acertados y fallidos que tiene la interface monitoreada
25	NAP #sh ip route	Despliega la información de la tabla de ruteo
26	NAP #ping 10.5.95.1 NAP #ping 10.5.96.1 NAP #ping 10.5.94.1	Verifica la conexión entre los enlaces
27	NAP #wr	Guarda la configuración realizada

Configuraciones finales router Akros

NAP #sh running-config

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 10.5.94.1 source-ipaddr 10.5.93.1
 timeout 999
 threshold 500
 frequency 3
ip sla monitor schedule 1 life forever start-time now
!
no ftp-server write-enable
!
interface Loopback0
 ip address 10.5.93.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 182.168.20.10 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 182.169.20.10 255.255.255.0
 duplex auto
 speed auto
!
no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 182.168.20.11
ip route 10.5.96.0 255.255.255.0 182.169.20.11
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

NAP #sh ip sla monitor statistics

```
Akros#sh ip sla monitor statistics
```

Round trip time (RTT) Index 1
      Latest RTT: 72 ms
Latest operation start time: *05:16:38.314 UTC Fri Mar 1 2002
Latest operation return code: OK
Number of successes: 906
Number of failures: 5
Operation time to live: Forever
NAP #ping 10.5.95.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.95.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/28/36 ms
NAP #ping 10.5.96.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.96.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/36/52 ms
NAP #ping 10.5.94.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.96.1, timeout is 3 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 29/39/52 ms

Tarea 2

Realizar las configuraciones correspondientes en el router de Level3, para su comunicación con los routers Akros, Telconet y NAP utilizando los siguientes comandos:

Pasos	Comando	Propósito
1	Level3>enable	Ingresa al modo privilegiado
2	Level3#conf ter	Ingresa al modo de configuración global
3	Level3(config)#inter lo 0	Ingresa al modo de configuración de la interfaz
4	Level3 (config-if)#ip add 10.5.95.1 255.255.255.0	Coloca una IP a la interfaz
	Level3(config-if)#exit	Regresa al modo de configuración global
	Level3(config)#inter fa 0/0	Ingresa al modo de configuración de la interfaz
	Level3 (config-if)#ip add 182.168.20.11 255.255.255.0	Coloca una IP a la interfaz
	Level3 (config-if)#no shut	Activa la interfaz
	Level3(config-if)#exit	Regresa al modo de configuración global
	Level3(config)#inter fa 1/0	Ingresa al modo de configuración
	Level3 (config-if)#ip add 182.167.20.10 255.255.255.0	Da a conocer a BGP la red interna del router
	Level3 (config-if)#no shut	Establece vecindad con la red de los routers vecinos

	Level3(config-if)#exit	Regresa al modo de configuración privilegio
	Level3(config)#inter fa 2/0	Ingresa al modo de configuración de la interfaz
	Level3 (config-if)#ip add 182.170.20.10 255.255.255.0	Coloca una IP a la interfaz
	Level3 (config-if)#no shut	Activa la interfaz
	Level3(config-if)#exit	Regresa al modo de configuración global
	Level3 (config)#ip sla monitor 5	Ingresa a la administración del ip sla
	Level3 (config-sla-monitor)#type echo protocol iplcmpEcho 182.167.20.11 source-ip 182.167.20.10	Habilita el envío de paquetes ICMP a través de la IP de destino y el enlace de origen
	Level3 (config-sla-monitor-echo)#frequency 3	Setea la velocidad en que se repite el envío de paquetes ICMP al siguiente salto
	Level3 (config-sla-monitor-echo)#timeout 999	Establece la cantidad de tiempo (milisegundos) en que IP sla esperara una respuesta de su paquete de solicitud
	Level3 (config-sla-monitor-echo)#threshold 500	Determina el umbral ascendente que almacena el historial de operación de IP sla
	Level3 (config-sla-monitor-echo)#exit	Regresa al modo de configuración global
	Level3 (config)#ip sla monitor schedule 5 start-time now life forever	Configura los parámetros de programación para la operación de IP sla
	Level3 (config)#track 5 rtr 5 reachability	Realiza un rastreo de las operaciones de IP sla
	Level3 (config)#delay down 10 up 5	Permite crear un tiempo de espera antes de que el track sea ejecutado
	Level3 (config)#ip route 0.0.0.0 0.0.0.0 182.167.20.11 track 5	Crea una ruta estática para forzarla a funcionar mientras el argumento track este operativo
	Level3 (config)#ip route 0.0.0.0 0.0.0.0 182.170.20.11 100	Añade una ruta estática y le da una distancia administrativa mayor para convertirla en enlace de backup
	Level3 (config)#ip route 10.5.93.0 255.255.255.0 182.168.20.10	Añade una ruta estática
	Level3 (config)#end	Regresa al modo de configuración privilegio

	Level3#sh running-config	Muestra la configuración del router
	Level3#sh ip sla monitor statistics	Muestra la cantidad de intentos acertados y fallidos que tiene la interface monitoreada
	Level3#sh ip route	Despliega la tabla de rutas
	Level3 #sh track 5	Despliega la actividad de los objetos monitoreados
	Level3 #sh ip route track-table	Muestra la tabla de rastreo configurada
	Level3#ping 10.5.93.1 Level3#ping 10.5.94.1	Verifica la conexión entre los enlaces
	Level3#wr	Guarda la configuración realizada

Configuraciones finales router Level3

Level3#sh running-config

```
ip sla monitor 5
 type echo protocol ipIcmpEcho 182.167.20.11 source-ipaddr 182.167.20.10
 timeout 999
 threshold 500
 frequency 3
ip sla monitor schedule 5 life forever start-time now
!
no ftp-server write-enable
!
track 5 rtr 5 reachability
 delay down 10 up 5
!
no crypto isakmp ccm
!
interface Loopback0
 ip address 10.5.95.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 182.168.20.11 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 182.167.20.10 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 ip address 182.170.20.10 255.255.255.0
 duplex auto
 speed auto
!
no ip http server
no ip http secure-server
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 182.167.20.11 track 5
ip route 0.0.0.0 0.0.0.0 182.170.20.11 100
ip route 10.5.93.0 255.255.255.0 182.168.20.10
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
Level3#sh ip sla monitor statistics
Round trip time (RTT)   Index 5
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: *05:42:53.594 UTC Fri Mar 1 2002
Latest operation return code: Timeout
Number of successes: 68
Number of failures: 788
Operation time to live: Forever
end
Level3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 182.170.20.11 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 2 subnets
C       10.5.95.0 is directly connected, Loopback0
S       10.5.93.0 [1/0] via 182.168.20.10
     182.170.0.0/24 is subnetted, 1 subnets
C       182.170.20.0 is directly connected, FastEthernet2/0
     182.168.0.0/24 is subnetted, 1 subnets
C       182.168.20.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [100/0] via 182.170.20.11ping 10.5.93.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/36/64 ms
Level3#sh track 5
Track 5
  Response Time Reporter 5 reachability
  Reachability is Down
    17 changes, last change 00:55:08
  Delay up 5 secs, down 10 secs
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
Level3#sh ip route track-table
 ip route 0.0.0.0 0.0.0.0 182.167.20.11 track 5 state is [up]
Level3#ping 10.5.94.1
Type escape sequence to abort.
```

Sending 5, 100-byte ICMP Echos to 10.5.94.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/40/64 ms
Level3#ping 10.5.93.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.94.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 26/45/61 ms

Tarea 3

Realizar las configuraciones correspondientes en el router de Telconet, para su comunicación con el router de Akros, Lvel3 y NAP utilizando los siguientes comandos:

Pasos	Comando	Propósito
1	Telconet>enable	Ingresa al modo privilegiado
2	Telconet #conf ter	Ingresa al modo de configuración global
3	Telconet (config)#inter lo 0	Ingresa al modo de configuración de la interfaz
4	Telconet (config-if)#ip add 10.5.96.1 255.255.255.0	Coloca una IP a la interfaz
	Telconet (config-if)#exit	Regresa al modo de configuración global
	Telconet (config)#inter fa 0/0	Ingresa al modo de configuración de la interfaz
	Telconet (config-if)#ip add 182.169.20.11 255.255.255.0	Coloca una IP a la interfaz
	Telconet (config-if)#no shut	Activa la interfaz
	Telconet (config-if)#exit	Regresa al modo de configuración global
	Telconet (config)#inter fa 1/0	Ingresa al modo de configuración de la interfaz
	Telconet (config-if)#ip add 182.166.20.10 255.255.255.0	Coloca una IP a la interfaz
	Telconet (config-if)#no shut	Activa la interfaz
	Telconet (config-if)#exit	Regresa al modo de configuración global
	Telconet (config)#inter fa 2/0	Ingresa al modo de configuración de la interfaz
	Telconet (config-if)#ip add 182.170.20.11 255.255.255.0	Coloca una IP a la interfaz
	Telconet (config-if)#no shut	Activa la interfaz
	Telconet (config-if)#exit	Regresa al modo de configuración global
	Telconet (config)#ip route 10.5.93.0 255.255.255.0 182.169.20.10 Telconet (config)#ip route 10.5.94.0 255.255.255.0	Añade rutas estática

	182.166.20.11 Telconet (config)#ip route 10.5.95.0 255.255.255.0 182.170.20.10	
	Telconet #sh running-config	Muestra la configuración del router
	Telconet #sh ip route	Despliega la tabla de rutas
	Telconet #ping 10.5.93.1 Telconet #ping 10.5.94.1	Verifica la conexión entre los enlaces
	Telconet #wr	Guarda la configuración realizada

Configuraciones finales router Telconet

Telconet#sh run

```
interface Loopback0
 ip address 10.5.96.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 182.169.20.11 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 182.166.20.10 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2/0
 ip address 182.170.20.11 255.255.255.0
 duplex auto
 speed auto
!
no ip http server
no ip http secure-server
ip classless
ip route 10.5.93.0 255.255.255.0 182.169.20.10
ip route 10.5.94.0 255.255.255.0 182.166.20.11
ip route 10.5.95.0 255.255.255.0 182.170.20.10
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Telconet#sh ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 4 subnets
S       10.5.95.0 [1/0] via 182.170.20.10
S       10.5.94.0 [1/0] via 182.166.20.11
S       10.5.93.0 [1/0] via 182.169.20.10
C       10.5.96.0 is directly connected, Loopback0
     182.170.0.0/24 is subnetted, 1 subnets
C       182.170.20.0 is directly connected, FastEthernet2/0
     182.169.0.0/24 is subnetted, 1 subnets
C       182.169.20.0 is directly connected, FastEthernet0/0
     182.166.0.0/24 is subnetted, 1 subnets
C       182.166.20.0 is directly connected, FastEthernet1/0
 Telconet#ping 10.5.93.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/30/36 ms
Telconet#ping 10.5.94.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.94.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/33/40 ms
```

Tarea 4

Realizar las configuraciones correspondientes en el router de Akros, para su comunicación con los routers NAP, Telconet y Level3 utilizando los siguientes comandos:

Pasos	Comando	Propósito
1	Akros>enable	Ingresa al modo privilegiado
2	Akros #conf ter	Ingresa al modo de configuración global
3	Akros (config)#inter lo 0	Ingresa al modo de configuración de la interfaz
4	Akros (config-if)#ip add 10.5.94.1 255.255.255.0	Coloca una IP a la interfaz
	Akros (config-if)#exit	Regresa al modo de configuración global
	Akros (config)#inter fa 0/0	Ingresa al modo de configuración de la interfaz
	Akros (config-if)#ip add 182.167.20.11 255.255.255.0	Coloca una IP a la interfaz
	Akros (config-if)#no shut	Activa la interfaz
	Akros (config-if)#exit	Regresa al modo de configuración global

	Akros (config)#inter fa 1/0	Ingresa al modo de configuración
	Akros (config-if)#ip add 182.166.20.11 255.255.255.0	Da a conocer a BGP la red interna del router
	Akros (config-if)#no shut	Establece vecindad con la red de los routers vecinos
	Akros (config-if)#exit	Regresa al modo de configuración privilegio
	Akros (config)#ip sla monitor 5	Ingresa a la administración del ip sla
	Akros (config-sla-monitor)#type echo protocol iplcmpEcho 182.167.20.10 source-ip 182.167.20.11	Habilita el envío de paquetes ICMP a través de la IP de destino y el enlace de origen
	Akros (config-sla-monitor-echo)#frequency 3	Setea la velocidad en que se repite el envío de paquetes ICMP al siguiente salto
	Akros (config-sla-monitor-echo)#timeout 999	Establece la cantidad de tiempo (milisegundos) en que IP sla esperara una respuesta de su paquete de solicitud
	Akros (config-sla-monitor-echo)#threshold 500	Determina el umbral ascendente que almacena el historial de operación de IP sla
	Akros (config-sla-monitor-echo)#exit	Regresa al modo de configuración global
	Akros (config)#ip sla monitor schedule 5 start-time now life forever	Configura los parámetros de programación para la operación de IP sla
	Akros (config)#track 5 rtr 5 reachability	Realiza un rastreo de las operaciones de IP sla
	Akros (config)#delay down 10 up 5	Permite crear un tiempo de espera antes de que el track sea ejecutado
	Akros (config)#ip sla monitor 2	Ingresa a la administración del ip sla
	Akros (config-sla-monitor)#type echo protocol iplcmpEcho 10.5.93.1 source-ip 10.5.94.1	Habilita el envío de paquetes ICMP a través de la IP de destino y el enlace de origen
	Akros (config-sla-monitor-echo)#frequency 3	Setea la velocidad en que se repite el envío de paquetes ICMP al siguiente salto
	Akros (config-sla-monitor-echo)#timeout 999	Establece la cantidad de tiempo (milisegundos) en que IP sla esperara una respuesta de su paquete de solicitud
	Akros (config-sla-monitor-echo)#threshold 500	Determina el umbral

		ascendente que almacena el historial de operación de IP sla
	Akros (config-sla-monitor-echo)#exit	Regresa al modo de configuración global
	Akros (config)#ip sla monitor schedule 2 start-time now life forever	Configura los parámetros de programación para la operación de IP sla
	Akros (config)#ip route 0.0.0.0 0.0.0.0 182.167.20.10 track 5	Crea una ruta estática para forzarla a funcionar mientras el argumento track este operativo
	Akros (config)#ip route 0.0.0.0 0.0.0.0 182.166.20.10 100	Añade una ruta estática y le da una distancia administrativa mayor para convertirla en enlace de backup
	Akros (config)#end	Regresa al modo de configuración privilegio
	Akros #sh running-config	Muestra la configuración del router
	Akros #sh ip sla monitor statistics	Muestra la cantidad de intentos acertados y fallidos que tiene la interface monitoreada
	Akros #sh ip route	Despliega la tabla de rutas
	Akros #sh track 5	Despliega la actividad de los objetos monitoreados
	Akros #sh ip route track-table	Muestra la tabla de rastreo configurada
	Akros #ping 10.5.93.1 Akros #ping 10.5.95.1 Akros #ping 10.5.96.1	Verifica la conexión entre los enlaces
	Akros #traceroute 10.5.93.1	Verifica el número de saltos antes de llegar al destino
	Akros #wr	Guarda la configuración realizada

Configuraciones finales router NAP

Akros #sh run

```
ip sla monitor 2
 type echo protocol ipIcmpEcho 10.5.93.1 source-ipaddr 10.5.94.1
 timeout 999
 threshold 500
 frequency 3
ip sla monitor schedule 2 life forever start-time now
ip sla monitor 5
 type echo protocol ipIcmpEcho 182.167.20.10 source-ipaddr 182.167.20.11
 timeout 999
```

```
 threshold 500
 frequency 3
ip sla monitor schedule 5 life forever start-time now
!
no ftp-server write-enable
!
track 5 rtr 5 reachability
 delay down 10 up 5
!
no crypto isakmp ccm
!
interface Loopback0
 ip address 10.5.94.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 182.167.20.11 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 182.166.20.11 255.255.255.0
 duplex auto
 speed auto
!
no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 182.167.20.10 track 5
ip route 0.0.0.0 0.0.0.0 182.166.20.10 100
ip route 10.5.96.0 255.255.255.0 182.166.20.10
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
Akros #sh ip sla monitor statistics
Round trip time (RTT)   Index 2
        Latest RTT: 60 ms
Latest operation start time: *07:05:21.086 UTC Fri Mar 1 2002
Latest operation return code: OK
Number of successes: 105
Number of failures: 0
Operation time to live: Forever
Round trip time (RTT)   Index 5
        Latest RTT: 20 ms
Latest operation start time: *07:05:21.094 UTC Fri Mar 1 2002
Latest operation return code: OK
Number of successes: 105
Number of failures: 0
Operation time to live: Forever
Akros #sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is 182.167.20.10 to network 0.0.0.0

    10.0.0.0/24 is subnetted, 1 subnets
C       10.5.94.0 is directly connected, Loopback0
    182.166.0.0/24 is subnetted, 1 subnets
C       182.166.20.0 is directly connected, FastEthernet1/0
    182.167.0.0/24 is subnetted, 1 subnets
C       182.167.20.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 182.167.20.10
Akros #sh track 5
Track 5
  Response Time Reporter 5 reachability
  Reachability is Up
    20 changes, last change 01:01:31
  Delay up 5 secs, down 10 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 36
  Tracked by:
    STATIC-IP-ROUTING 0
Akros #sh ip route track-table
 ip route 0.0.0.0 0.0.0.0 182.167.20.10 track 5 state is [up]
Akros #ping 10.5.93.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/60/68 ms
Akros #ping 10.5.95.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.95.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/29/36 ms
Akros #ping 10.5.96.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.96.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/33/48 ms
Akros #traceroute 10.5.93.1
Type escape sequence to abort.
Tracing the route to 10.5.93.1
  1 182.167.20.10 40 msec 28 msec 28 msec
  2 182.168.20.10 56 msec *  56 msec
```

Pruebas de redundancia

```
Level3(config)#inter fa1/0
Level3(config-if)#shutdown
Level3(config-if)#
*Mar  1 07:18:54.194: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state to
administratively down
```

```
*Mar 1 07:18:55.194: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0, changed state to down
Level3#sh ip route track-table
 ip route 0.0.0.0 0.0.0.0 182.167.20.11 track 5 state is [down]

Akros #ping 10.5.93.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.5.93.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.....!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 91 percent (91/100), round-trip min/avg/max = 48/68/92 ms
Akros #sh ip route track-table
ip route 0.0.0.0 0.0.0.0 182.167.20.10 track 5 state is [down]
Akros #traceroute 10.5.93.1
Type escape sequence to abort.
Tracing the route to 10.5.93.1
  1 182.166.20.10 40 msec 24 msec 28 msec
  2 182.169.20.10 76 msec *  100 msec
```

La utilización del software GNS3 en ambas emulaciones, ha permitido demostrar algunos de los beneficios que conlleva poseer un enlace de respaldo, empleando diferentes técnicas (BGP, PRB, IP SLA). Estos beneficios tales como mayor disponibilidad de la red, mejoramiento en la confiabilidad de la entrega de paquetes, medición del rendimiento de la red, creación de políticas de enrutamiento, etc, permitirán a la empresa Akros estar 24/7 conectado con sus clientes, mejorando de igual manera la velocidad y la comunicación de las diferentes actividades diarias que hacen uso del internet.

- **WIRESHARK**

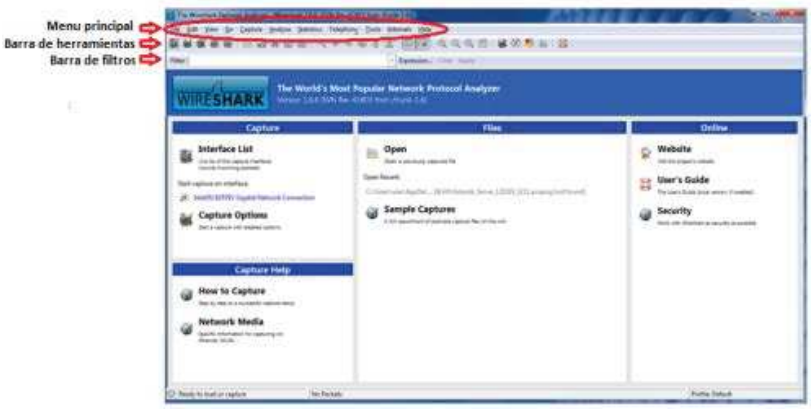
El *software* libre Wireshark, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones. Es muy utilizado como herramienta didáctica ya que permite ver todo el tráfico que pasa a través de una red, aplicar filtros para observar los paquetes de un protocolo concreto o examinar un archivo de captura previamente salvado en disco. Entre sus características de funcionamiento se puede encontrar:

- Disponible para Linux, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red sea esta alámbrica o inalámbrica.

- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Permite hacer un filtro que cumpla con un criterio previamente definido.
- Permite obtener estadísticas y gráficas mediante el uso de colores que identifican el filtro especificado.

Debido a temas de seguridad y confidencialidad, no es factible analizar la red real de Akros. Lo que se realizó, son dos ejemplos utilizando una dirección IP alternativa (10.5.93.0 /24), en donde se simulará un ataque DoS y una infección por virus, los mismos que serán analizados por Wireshark.

El primer paso para el uso de esta herramienta es ejecutarla (instalación previamente realizada) como se muestra en la siguiente figura:



La interfaz principal de Wireshark cuenta con varias secciones que se describen a continuación:

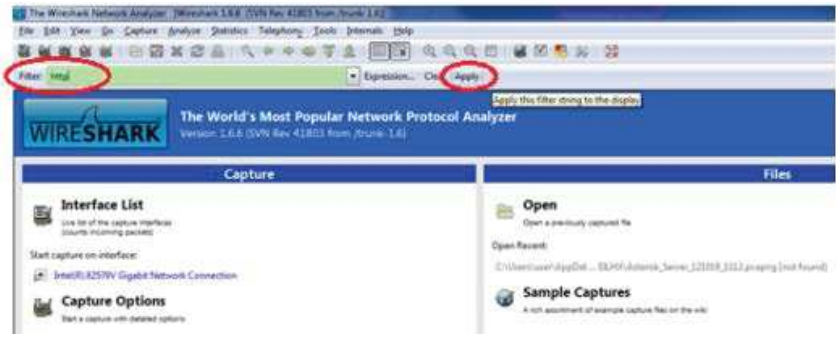
- *Menú principal*, la misma que contiene los siguientes sub menús:

  - ✓ ***File*****,** manipulación de archivos.
  - ✓ ***Edit*****,** funciones de los paquetes y configuración de interfaz de usuario.
  - ✓ ***View,*** configurar el despliegue de la pantalla capturada.

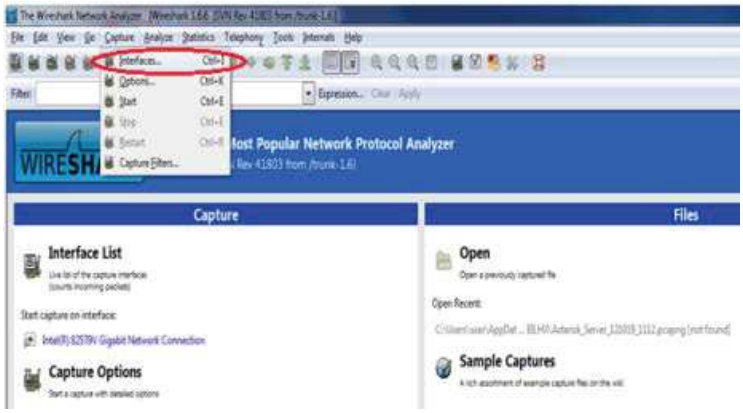
- ✓ ***Go*****,** desplazamiento entre los paquetes.
- ✓ ***Analyze*****,** manipulación de filtros, habilitación de protocolos.
- ✓ ***Stadistics,*** estadísticas de captura.
- ✓ ***Help,*** menú de ayuda.

- *Barra de herramientas principal*, permite el acceso rápido a las funciones más utilizadas.
- *Barra de herramientas para* filtros, donde se aplica el filtro que se desea aplicar a los paquetes que están siendo capturados.

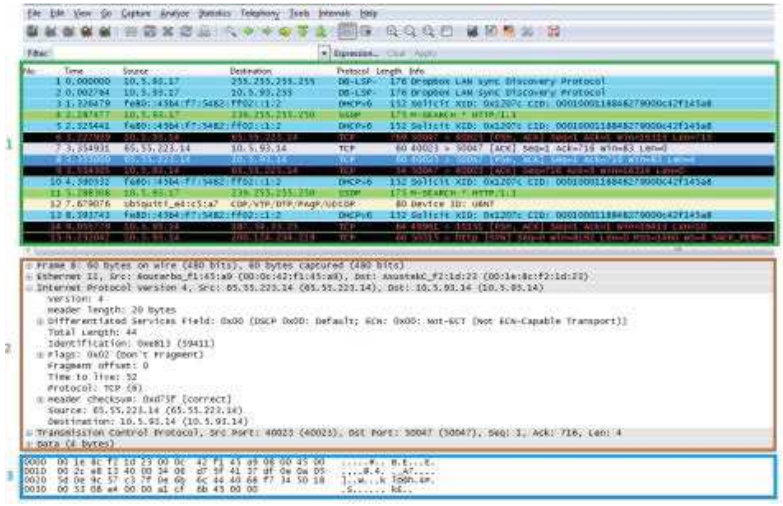
En la opción *filter*, se puede colocar el tipo de protocolo que se desea analizar en la red y posteriormente se presiona *apply,* tal como se muestra la siguiente figura:



Una vez colocado el protocolo específico que se desea analizar, (si no se quiere analizar un protocolo específico, se puede analizar todo el tráfico) se dará *click* sobre la opción capture para posteriormente señalar la sub opción interfaces, de este modo se empezará la captura del tráfico, tal como se muestra en la siguiente figura:



Una vez que el tráfico comienza a ser capturado (ver figura inferior), existen tres zonas muy importantes a tomar en cuenta las cuales se verán a continuación:

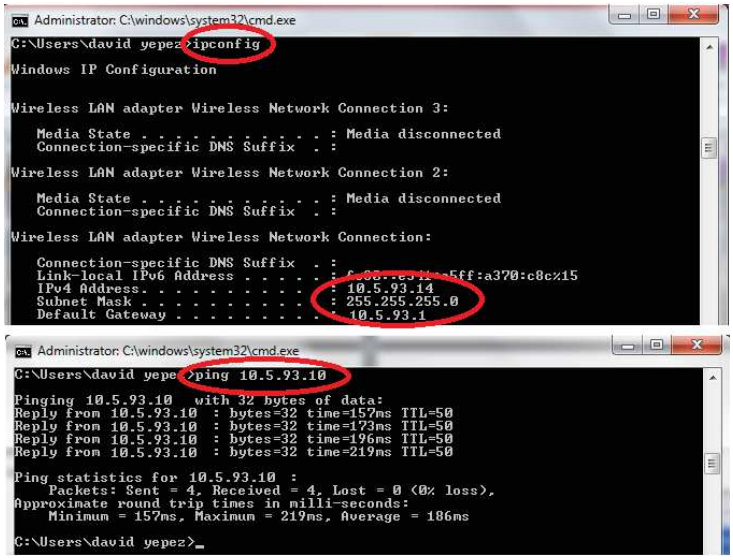


- La zona 1 corresponde a la lista de visualización de todos los paquetes que se están capturando en tiempo real. Saber interpretar correctamente los datos proporcionados en esta zona (tipo de protocolo, números de secuencia, *flags*, marcas de tiempo, puertos, etc.) permitirá deducir el problema sin tener que realizar una auditoría minuciosa.

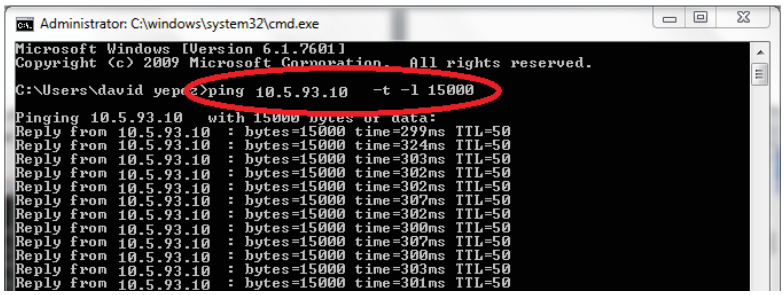
- La zona 2 permite desglosar por capas cada una de las cabeceras de los paquetes seleccionados, lo que facilitará moverse por cada uno de los campos de las mismas.

- Por último, la zona 3 representa en formato hexadecimal el paquete en bruto, es decir, tal y como fue capturado por la tarjeta de red.

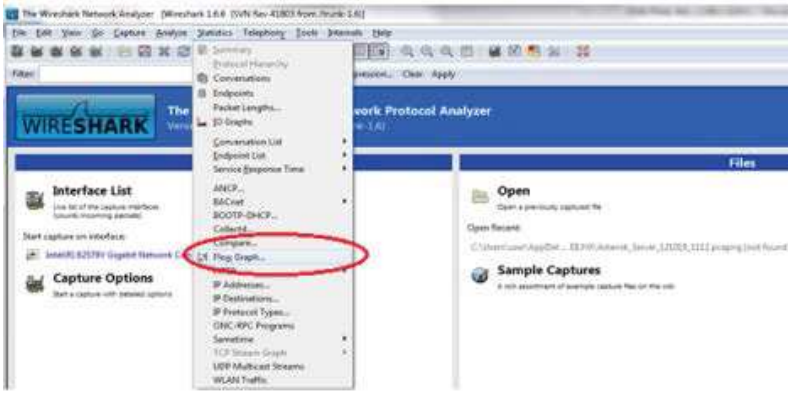
En el primer ejemplo, se simulará un ataque de denegación de servicio (DoS). Una manera muy común utilizada para ejecutar ataques DoS, es por medio de la ventana de CMD de Windows. Como primer paso, se colocan 2 PC's dentro de la misma red. Después, se procede a asignar direcciones IP (PC1: 10.5.93.14 / PC2: 10.5.93.10). Luego, se realiza un ping desde la 10.5.93.14 hacia la 10.5.93.10 para verificar que hay conectividad, tal como lo muestra la siguiente figura:



Posteriormente, se comienza a realizar el ataque DoS, utilizando para ello 2 características muy importantes del comando ping. El –t, que realiza un *ping* infinito a una determinada IP y el –l que determina el tamaño del *buffer* que en este caso será 15000, tal como lo indica la siguiente figura. Para acelerar el proceso de solicitudes de ping hacia la IP 10.5.93.10, se pueden abrir varias ventanas CMD simultáneamente y realizar el mismo proceso.



Una vez generado el ataque por un periodo de tiempo, arrancamos el programa Wireshark, en donde existe una opción que permite capturar el diagrama de flujo a través de la red. Esto se realiza dando *click* en el menú *statistics,* para posteriormente dar *click* en la sub opción *flow graph* (figura inferior). Una vez activada la opción *flow graph*, se procede a verificar los *flag* SYN, que no son más que un conjunto de señalizaciones de cabecera IP.

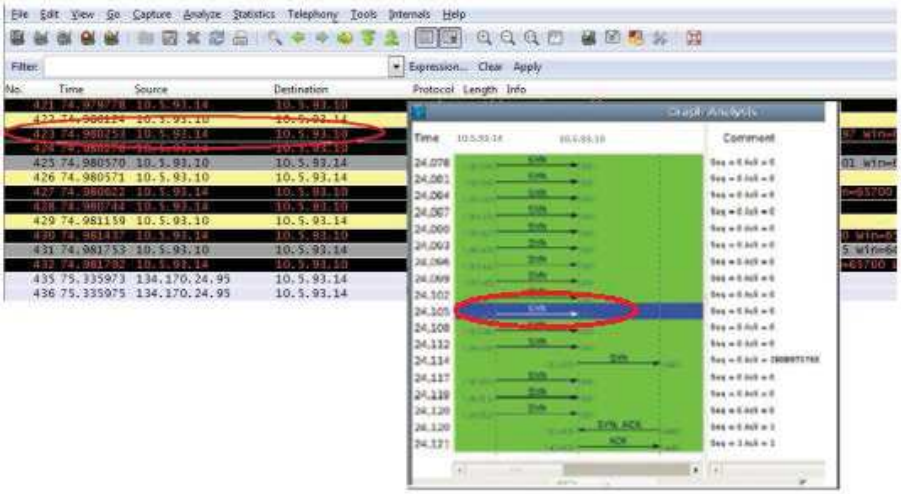


Inmediatamente se nota que existe una gran cantidad de segmentos TCP con el *flag* SYN activados desde la misma IP 10.5.93.14, que no reciben respuesta alguna. Esta opción *flow graph* facilitará seguir el comportamiento de conexiones TCP, ya que, describe de forma muy intuitiva mediante flechas, el origen y destino de cada paquete, resaltando los *flags* activos que intervienen en cada sentido de la conexión, tal como lo indica la siguiente figura.

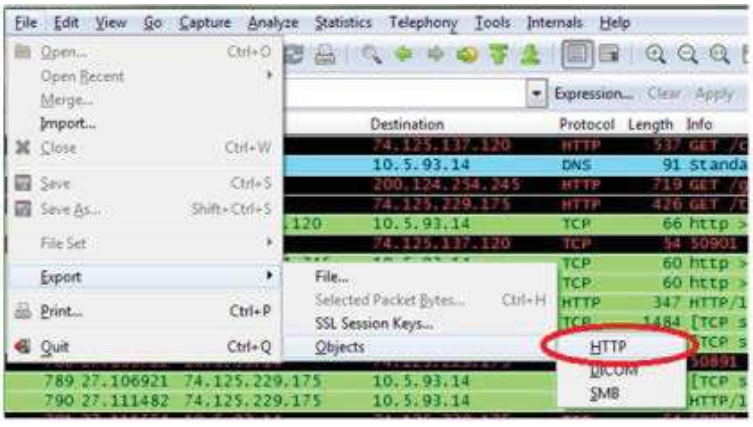
En este caso en particular se observa que, en un intervalo muy corto de tiempo, existen numerosos intentos de conexión por parte de la dirección IP 10.5.93.14 hacia la dirección 10.5.93.10, situación algo inusual. El PC destino ha tratado de resolver la MAC de la máquina origen en numerosas ocasiones, pero al no recibir ninguna respuesta y carecer de la dirección física del *host*, no se puede enviar un ACK-SYN al mismo para continuar con el establecimiento de la conexión.

Esto conlleva que TCP/IP de la maquina destino 10.5.93.10 tenga que esperar un tiempo determinado por cada conexión, durante el cual seguirán llegando más paquetes que irán creando nuevas conexiones. Por cada conexión que se intente establecer se creará una estructura en memoria que es usada por

TCP/IP del sistema operativo para identificar cada una de las conexiones y que, con un número muy elevado, pueden terminar con los recursos de la máquina produciendo que el equipo deje de contestar más solicitudes de conexión.

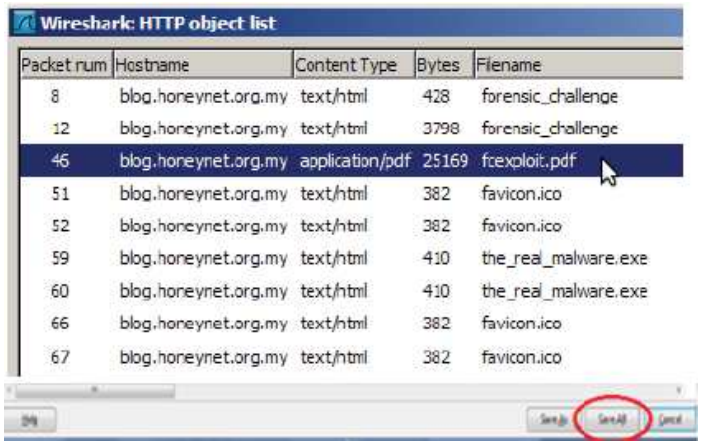


El segundo ejemplo realizado, un PC entra a la página *web* www.honeynet.org, en donde procede a descargar un archivo cualquiera .pdf. Para estar seguros que dicho archivo no contenta ningún tipo de infección, se ejecuta Wireshark y se realiza una captura de trafico HTTP de la red. Se identifican qué archivos se han descargado aprovechando la utilidad de exportar objetos, seleccionando la opción *file*, después la sub opción *export, objects* y finalmente HTTP, como lo muestra la siguiente figura:



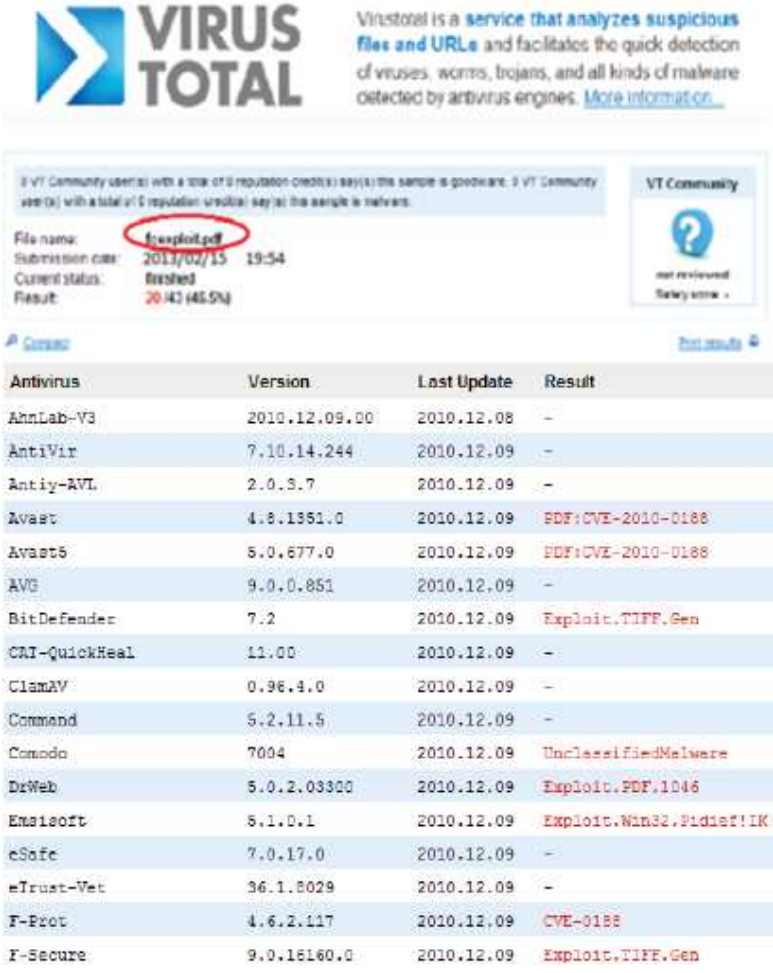
Después, aparece la ventana con todas las peticiones HTTP detectadas en el exportador de objetos. Aislando los archivos conocidos, se centra la atención en el archivo .pdf descargado recientemente. Se selecciona dicho archivo

sospechoso (paquete 46 "*fcexploit.pdf")*, tal como se muestra en la siguiente figura.



Posteriormente, se procede a descargar (dando click en el botón *save all*) el fichero seleccionado "*fcexploit.pdf*", almacenándolo en el disco duro local. Se supone que este archivo es malicioso por lo que habrá que tener cuidado de no abrirlo o ejecutarlo, pero ya se tiene una posible muestra del *malware* que se podrá analizar con un antivirus o enviarla a que sea analizada *online*.

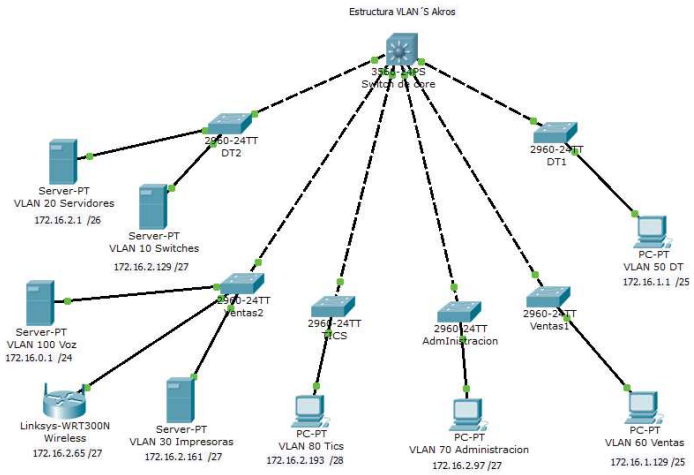
Finalmente, se debe analizar el archivo con un antivirus local instalado, o mejor aún, con un motor de búsqueda online de firmas de virus el cual posee un mayor campo de análisis de archivos infectados. Un muy buen motor de búsqueda de virus online es "Virus total¨. Su ubicación web es *www.virustotal.com*. En la figura inferior, se muestra la página de inicio, en donde se puede seleccionar el archivo a ser examinado. Posteriormente, en la figura 6.18, se despliega el resultado obtenido en el fichero descargado, el mismo que fue positivo, indicando el nombre del virus, por lo que es posible buscar información específica para eliminarlo y, paralelamente, informar al proveedor de antivirus para que genere una firma de detección en caso de no detectarlo.



Antivirus	Version	Last Update	Result
AhnLab-V3	2010.12.09.00	2010.12.08	-
AntiVir	7.10.14.244	2010.12.09	-
Antiy-AVL	2.0.3.7	2010.12.09	-
Avast	4.8.1351.0	2010.12.09	PDF:CVE-2010-0188
Avast5	5.0.677.0	2010.12.09	PDF:CVE-2010-0188
AVG	9.0.0.851	2010.12.09	-
BitDefender	7.2	2010.12.09	Exploit.TIFF.Gen
CAT-QuickHeal	11.00	2010.12.09	-
ClamAV	0.96.4.0	2010.12.09	-
Command	5.2.11.5	2010.12.09	-
Comodo	7004	2010.12.09	UnclassifiedMalware
DrWeb	5.0.2.03300	2010.12.09	Exploit.PDF.1046
Emsisoft	5.1.0.1	2010.12.09	Exploit.Win32.Pidief!IK
eSafe	7.0.17.0	2010.12.09	-
eTrust-Vet	36.1.8029	2010.12.09	-
F-Prot	4.6.2.117	2010.12.09	CVE-0188
F-Secure	9.0.16160.0	2010.12.09	Exploit.TIFF.Gen

➢ REDISTRIBUCIÓN DE VLAN'S

Diagrama de topología



Objetivos de aprendizaje

Al completar esta práctica de laboratorio se podrá:

- Configurar la topología física.
- Configurar la topología lógica.
- Verificar la conectividad en la red.
- Crear subredes que se ajusten a los requisitos de la empresa.
- Crear VLAN´s
- Crear los enlaces de *trunk*
- Agregar puertos de *switch* a una VLAN.
- Realizar ping entre el switch_core y cada uno de los *switches* de distribución.

Escenario

En esta práctica de laboratorio se diseñará y configurará una red la cual verificara la conectividad a través de los distintos dispositivos de red. Esto requiere la creación y la asignación de bloques de subredes y VLAN's. El *switch* de core estará directamente conectado a los diferentes *switches* de distribución los cuales estarán divididos por las distintas VLAN's.

Tarea 1

Realizar las configuraciones básicas en *switch* Ventas1 utilizando los siguientes comandos:

Pasos	Comando	Propósito
1	Ventas1#configure terminal	Entra al modo de configuración global
2	Ventas1 (config)#vlan 90	Crea la VLAN 90
3	Ventas1(config-vlan)#name management	Asigna un nombre a la VLAN
4	Ventas1(config-vlan)#exit	Regresa al modo global
5	Ventas1 (config)# interface fa 0/20	Ingresa al modo de configuración de la interfaz
6	Ventas1(config-if)#switchport trunk native vlan 90	Asigna una VLAN de administración a una interface
7	Ventas1(config-vlan)#exit	Regresa al modo global
8	Ventas1(config)#interface vlan 90	Ingresa al modo VLAN
9	Ventas1(config-if)#ip address 172.16.2.214 255.255.255.240	Coloca una dirección IP a la VLAN
10	Ventas1(config-if)#exit	Regresa al modo global
11	Ventas1 (config)#vlan 60	Crea la VLAN 60
12	Ventas1 (config-vlan)#name ventas	Asigna un nombre a la VLAN
13	Ventas1(config)#inter fa 0/1	Ingresa al modo de configuración de la interfaz
14	Ventas1(config-if)#switchport mode access	Coloca a la interfaz en modo de acceso
15	Ventas1(config-if)#switchport access vlan 60	Permite el paso de la VLAN por la interfaz
16	Ventas1(config-if)#no shutdown	Activa la interfaz
17	Ventas1(config-vlan)#exit	Regresa al modo global
18	Ventas1(config)#interface vlan 60	Ingresa a la interfaz de la VLAN
19	Ventas1(config-if)#ip address 172.16.1.130 255.255.255.128	Coloca una dirección IP a la VLAN
20	Ventas1(config-if)#end	Regresa al modo privilegiado
21	Ventas1#sh running-config	Corre la configuración interna del switch
22	Ventas1#sh vlan brief	Muestra la configuración de las VLAN´s creadas
23	Ventas1#sh interface trunk	Despliega la información sobre todas las interfaces de Trunk
24	Ventas1#sh ip interface brief	Despliega en detalle la configuración de cada interface
25	Ventas1#ping 172.16.1.131	Permite verificar la conectividad entre 2 puntos
26	Ventas1 #wr	Guarda la configuración realizada

NOTA: Todos los pasos anteriores, se deben ejecutar en cada uno de los *switches* de distribución, cambiando el número de VLAN, Interfaces y sus IP´s asignadas.

Configuraciones finales switch Ventas1

```
Ventas1#sh running-config
Building configuration...
Current configuration : 1168 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Ventas1
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/20
switchport trunk native vlan 90
switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan60
 ip address 172.16.1.130 255.255.255.128
!
interface Vlan90
 ip address 172.16.2.214 255.255.255.240
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
Ventas1# sh vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig1/1, Gig1/2
60   ventas                           active    Fa0/1
90   management                       active
```

```
1002 fddi-default                active
1003 token-ring-default          active
1004 fddinet-default             active
1005 trnet-default               active
Ventas1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/20      1-1005

Port        Vlans allowed and active in management domain
Fa0/20      1,60,90
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      60
Ventas1#sh ip interface brief
  Interface              IP-Address      OK? Method Status                Protocol
Vlan60                 172.16.1.130    YES manual up                    up
Vlan90                 172.16.2.214    YES manual up                    up
Ventas1#ping 172.16.1.131
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.131, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/28/32 ms
```

Tarea 2

Realizar la creación de las VLAN´s en el *switch* de core con sus respectivas IP´s. Además, crear los enlaces de *Trunk* para la comunicación entre *switches*.

Pasos	Comando	Propósito
1	Switch_core#config terminal	Entra al modo de configuración global
2	Switch_core (config)#vlan 90	Crea la VLAN 90
3	Switch_core(config-vlan)#name management	Asigna un nombre a la VLAN
4	Switch_core(config-vlan)#exit	Regresa al modo global
5	Switch_core(config)#interface fa 0/20	Ingresa al modo de configuración de la interfaz
6	Switch_core(config-if)#switchport trunk native vlan 90	Asigna una VLAN de administracion a una interface
7	Switch_core(config-vlan)#exit	Regresa al modo global
8	Switch_core(config)#interface vlan 90	Ingresa al modo VLAN
9	Switch_core (config-if)#ip address 172.16.2..209 255.255.255.240	Coloca una dirección IP a la VLAN
10	Switch_core(config-if)#exit	Regresa al modo global
11	Switch_core(config)#vlan 60	Crea la VLAN 60
12	Switch_core(config-vlan)#name ventas	Asigna un nombre a la VLAN
13	Switch_core(config-vlan)#exit	Regresa al modo global
14	Switch_core (config)#interface vlan 60	Ingresa a la interfaz de la VLAN
15	Switch_core (config-if)#ip address 172.16.1.131	Coloca una dirección IP a la

	255.255.255.128	VLAN
16	Switch_core(config-if)#exit	Regresa al modo global
17	Switch_core(config)# interface fa 0/20	Ingresa al modo de configuración de la interfaz
18	Switch_core(config-if)#switchport trunk encapsulation dot1q	Protocolo usado para interconectar switches y routers
19	Switch_core(config-if)# switchport mode trunk	Establece el puerto troncal para intercomunicar switches
20	Switch_core(config-if)#end	Regresa al modo privilegiado
21	Switch_core#sh running-config	Corre la configuración interna del switch
22	Switch_core #sh vlan brief	Muestra la configuración de las VLAN´s creadas
23	Ventas1#sh interface trunk	Despliega la información sobre todas las interfaces de Trunk
24	Ventas1#sh ip interface brief	Despliega en detalle la configuración de cada interface
25	Ventas1#ping 172.16.1.129	Permite verificar la conectividad entre 2 puntos
26	Switch_core #wr	Guarda la configuración realizada

NOTA: Todos los pasos anteriores, se deben ejecutar a cada interfaz conectada desde el *switch* de core hacia los switches de distribución, cambiando en cada enlace el número asignado de cada VLAN y su respectiva dirección IP.

Configuraciones finales switch_core

Switch_core#sh running-config
Building configuration...
Current configuration : 2069 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch_core
!
spanning-tree mode pvst
!
interface FastEthernet0/4
switchport trunk encapsulation dot1q
switchport trunk native vlan 90
switchport mode trunk
!
interface FastEthernet0/8

```
switchport trunk encapsulation dot1q
switchport trunk native vlan 90
switchport mode trunk
!
interface FastEthernet0/12
switchport trunk encapsulation dot1q
switchport trunk native vlan 90
switchport mode trunk
!
interface FastEthernet0/16
switchport trunk encapsulation dot1q
switchport trunk native vlan 90
switchport mode trunk
!
interface FastEthernet0/20
switchport trunk encapsulation dot1q
switchport trunk native vlan 90
switchport mode trunk
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport trunk native vlan 90
switchport mode trunk
!
interface Vlan10
 ip address 172.16.2.131 255.255.255.224
!
interface Vlan20
 ip address 172.16.2.3 255.255.255.192
!
interface Vlan30
 ip address 172.16.2.163 255.255.255.224
!
interface Vlan40
 ip address 172.16.2.67 255.255.255.224
!
interface Vlan50
 ip address 172.16.1.3 255.255.255.128
!
interface Vlan60
 ip address 172.16.1.131 255.255.255.128
!
interface Vlan70
 ip address 172.16.2.99 255.255.255.224
!
interface Vlan80
 ip address 172.16.2.195 255.255.255.240
!
interface Vlan90
 ip address 172.16.2.209 255.255.255.240
!
interface Vlan100
 ip address 172.16.0.3 255.255.255.0
!
ip classless
!
line con 0
line vty 0 4
```

```
 login
!
end
Switch_core#sh vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                                Fa0/22, Fa0/23, Gig0/1, Gig0/2
10   switches                         active
20   servidores                       active
30   impresoras                       active
40   wireless                         active
50   DT                               active
60   ventas                           active
70   administracion                   active
80   tics                             active
90   management                       active
100  voz                              active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch_core#sho interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/4       on           802.1q         trunking      90
Fa0/8       on           802.1q         trunking      90
Fa0/12      on           802.1q         trunking      90
Fa0/16      on           802.1q         trunking      90
Fa0/20      on           802.1q         trunking      90
Fa0/24      on           802.1q         trunking      90
Port        Vlans allowed on trunk
Fa0/4       1-1005
Fa0/8       1-1005
Fa0/12      1-1005
Fa0/16      1-1005
Fa0/20      1-1005
Fa0/24      1-1005
Port        Vlans allowed and active in management domain
Fa0/4       1,10,20,30,40,50,60,70,80,90,100
Fa0/8       1,10,20,30,40,50,60,70,80,90,100
Fa0/12      1,10,20,30,40,50,60,70,80,90,100
Fa0/16      1,10,20,30,40,50,60,70,80,90,100
Fa0/20      1,10,20,30,40,50,60,70,80,90,100
Fa0/24      1,10,20,30,40,50,60,70,80,90,100
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/4       1,10,20,30,40,50,60,70,80,90,100
Fa0/8       1,10,20,30,40,50,60,70,80,90,100
Fa0/12      1,10,20,30,40,50,60,70,80,90,100
Fa0/16      1,10,20,30,40,50,60,70,80,90,100
Fa0/20      1,10,20,30,40,50,60,70,80,90,100
Fa0/24      1,10,20,30,40,50,60,70,80,90,100
Switch_core#sh ip interface brief
    Interface              IP-Address      OK? Method Status                Protocol
     Vlan10                172.16.2.131    YES manual up                    up
     Vlan20                172.16.2.3      YES manual up                    up
```

```
Vlan30          172.16.2.163    YES manual up                    up
Vlan40          172.16.2.67     YES manual up                    up
Vlan50          172.16.1.3      YES manual up                    up
Vlan60          172.16.1.131    YES manual up                    up
Vlan70          172.16.2.99     YES manual up                    up
Vlan80          172.16.2.195    YES manual up                    up
Vlan90          172.16.2.209    YES manual up                    up
Vlan100         172.16.0.3      YES manual up                    up
Switch_core#ping 172.16.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/7/10 ms
Switch_core#ping 172.16.2.129
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/10 ms
Switch_core#ping 172.16.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/9/10 ms
Switch_core#ping 172.16.2.65
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.65, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/7/10 ms
Switch_core#ping 172.16.2.161
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.161, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/7/10 ms
Switch_core#ping 172.16.2.193
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.193, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/10 ms
Switch_core#ping 172.16.2.97
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.97, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/7/10 ms
Switch_core#ping 172.16.1.129
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/9/10 ms
Switch_core#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/6/10 ms
```

NOTA: Debido a que los *switches* que posee Akros son HP, se creará a continuación una tabla comparativa de comandos entre HP y Cisco

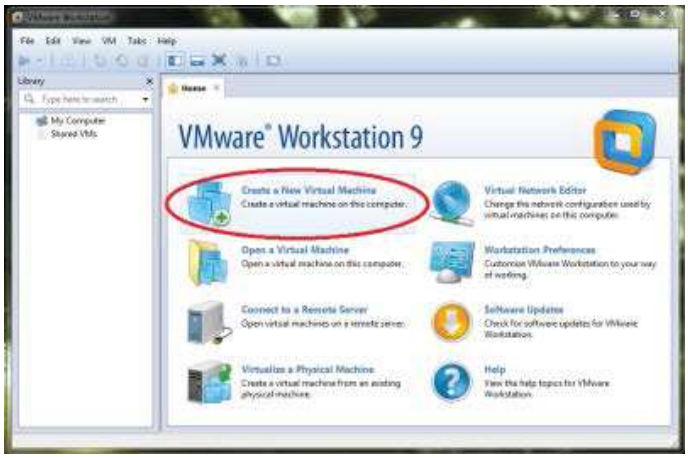
CISCO	HP	FUNCION
cisco#config terminal	<HP> system-view	Entra al modo de configuración global
cisco(config)#vlan “# vlan”	[HP] vlan id “# vlan”	Crea una VLAN
cisco(config)#name “nombre VLAN”	[HP-vlan] description “nombre VLAN”	Asigna un nombre a la VLAN
cisco (config)#exit	[HP] exit	Regresa al modo de configuración privilegiado
cisco(config)#end	[HP] quit	Regresa al modo de configuración anterior
cisco(config)#interface fa “# interface”	[HP] interface fa “# interface”	Ingresa a la interfaz deseada
cisco(config-if)#ip address “dirección IP”	[HP-Vlan-interface] ip address “dirección IP”	Asigna una dirección IP a una interfaz
cisco(config)#interface vlan “# vlan”	[HP] interface vlan-interface “# vlan”	Ingresa a la VLAN deseada
cisco(config-if)#no shutdown	[HP] enable	Activa la interfaz
cisco(config-if)#switchport encapsulation dot1q	[HP] tagged trk1	Protocolo usado para interconectar switches y routers
cisco(config-if)#switchport mode trunk	[HP] trunk “# interface” trk1	Establece el puerto troncal para intercomunicar switches
cisco(config-if)#switchport mode access	HP] access “# interface”	Coloca a la interfaz en modo de acceso
cisco(config-if)#switchport access vlan “# VLAN”	[HP] port trunk permit vlan “# vlan”	Permite el paso de la VLAN por la interfaz
cisco(config-if)#switchport trunk native vlan “”# VLAN	[HP] port trunk native permit vlan ”# vlan”	Asigna una VLAN de administración a una interface
cisco#sh running-config	[HP]display current-configuration	Muestra la configuración interna del switch
cisco#sh vlan brief	[HP]display vlan brief	Muestra la configuración de las VLAN´s creadas
cisco#wr	[HP] wr memory	Guarda la configuración realizada

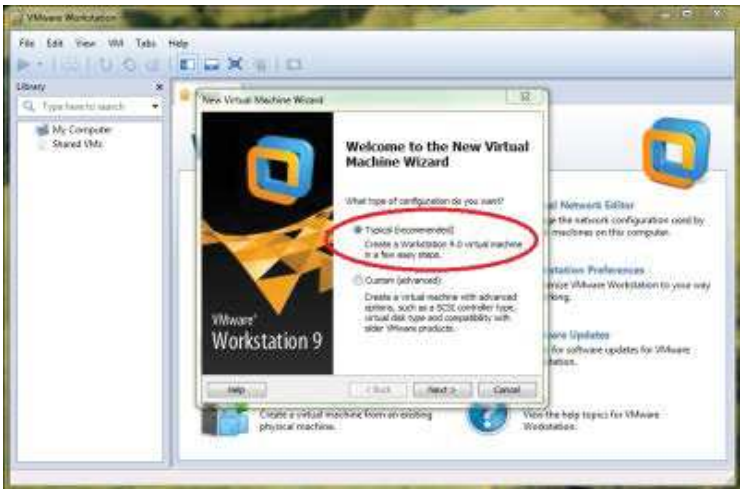
➢ VIRTUALIZACIÓN DEL SISTEMA OPERATIVO WINDOWS SERVER 2003

A continuación se mostrará cómo se realiza una virtualización de plataforma, en donde se instalará y configurará el SO windows XP utilizando el *software* Vmware *workstation* 9, el mismo que necesita los siguientes requerimientos mínimos para su funcionamiento:

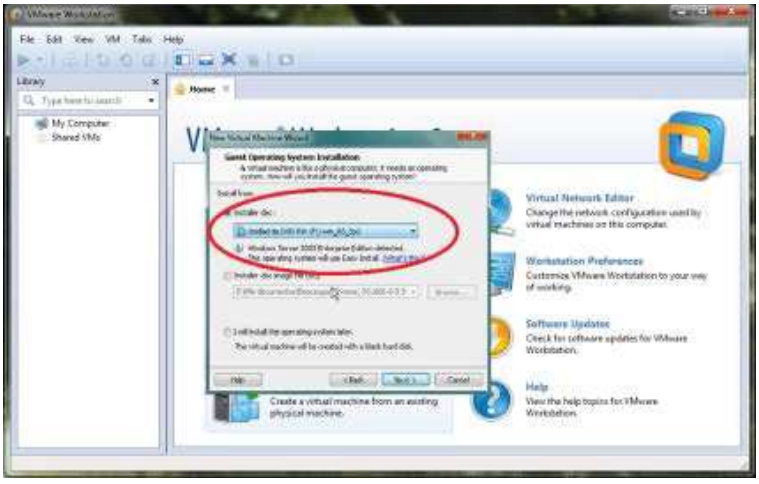
- Velocidad del procesador: 1Ghz
- Sistema operativo: Windows 2000, XP, 7, 8, server. Linux Centos, Ubuntu, Redhat *enterprice*.
- Espacio en disco: 7-60Gb dependiendo del SO a virtualizar.
- Memoria RAM: 2Gb

Como primer paso, se debe ejecutar el programa VMware wokstation 9 en una estación de trabajo. Una vez el programa este corriendo, se procede a la creación de una nueva máquina virtual, para posteriormente escoger la instalación típica tal como lo indican las siguientes figuras:

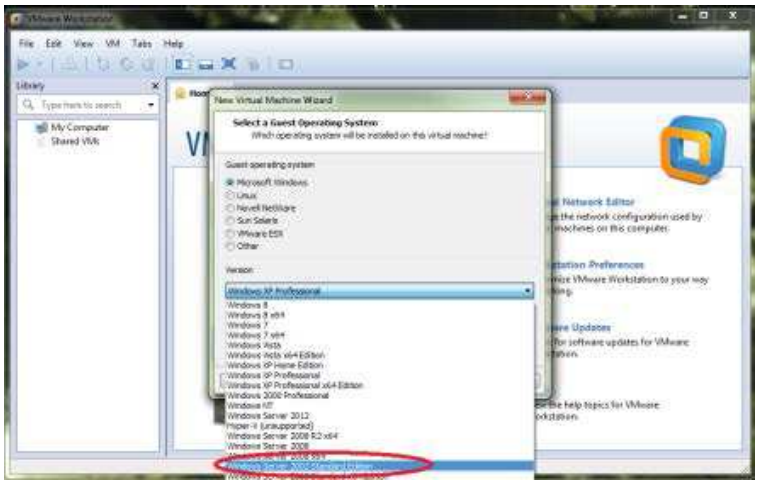




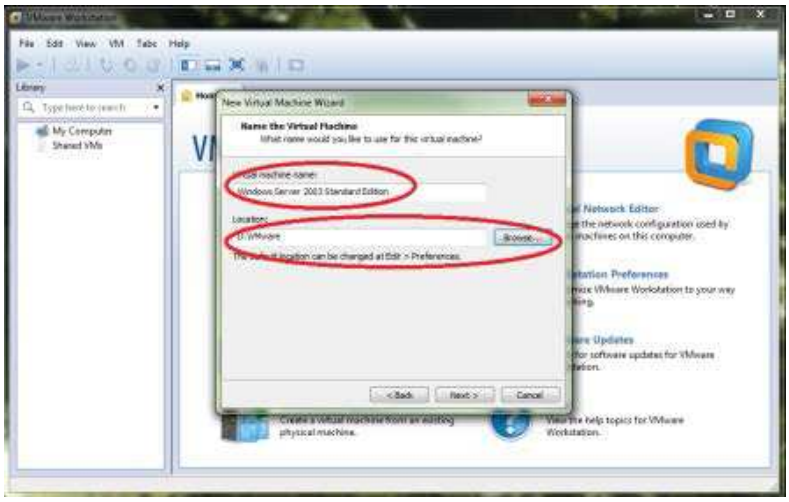
Una vez escogida la configuración típica, se procede a seleccionar el origen de la imagen que se desea virtualizar. Existen 2 opciones: Desde una imagen .ISO o desde un cd. Para este ejemplo se seleccionará desde un cd, tal como lo muestra la siguiente figura:



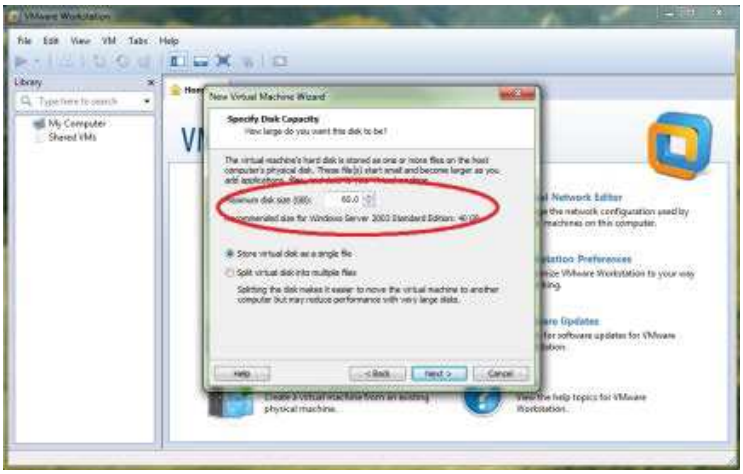
Vmware debe asegurarse que SO es el que contiene el cd, por lo que pide la especificación del mismo, como se ve en la siguiente figura:



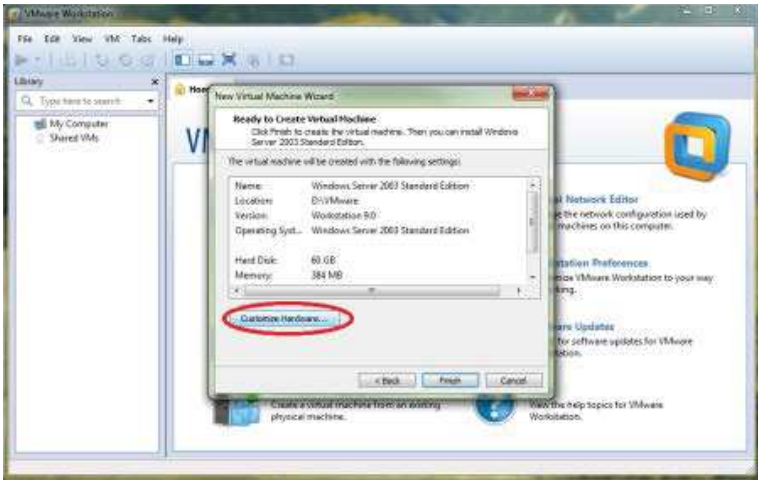
Posteriormente, se elige un nombre a la nueva máquina virtual (Windows server 2003 *standard edition*) y la ubicación donde se guardara (D:/Vmware), tal como lo muestra la siguiente figura:



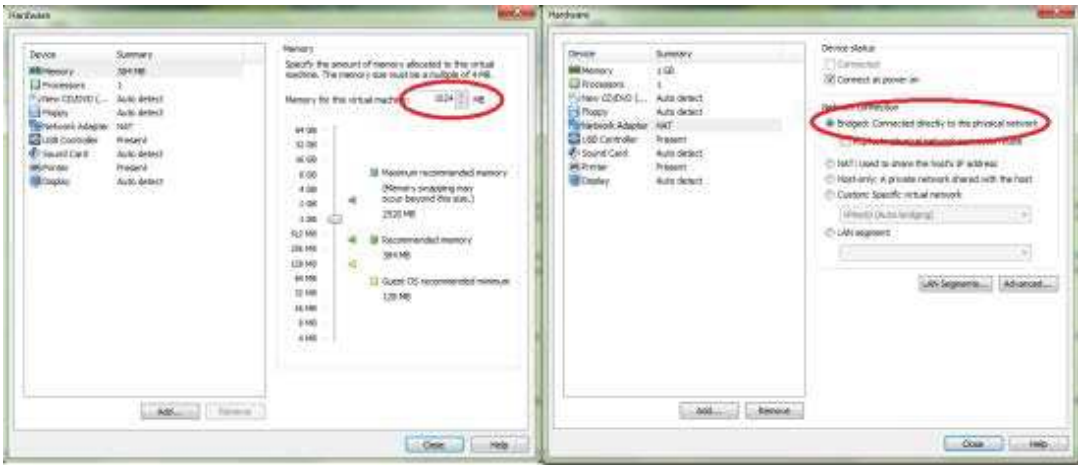
Una vez seleccionado el nombre y la ubicación, se continúa con la elección de la capacidad de disco duro que será destinada para la máquina virtual. Lo mínimo recomendado son 40Gb, pero en este caso se dejará 60Gb para el futuro crecimiento de la máquina virtual. Además se puede escoger si se desea dividir el disco en diferentes archivos o en uno solo, lo que permitirá la movilización de la máquina virtual de una computadora a otra sin problemas como se visualizará en la siguiente figura:



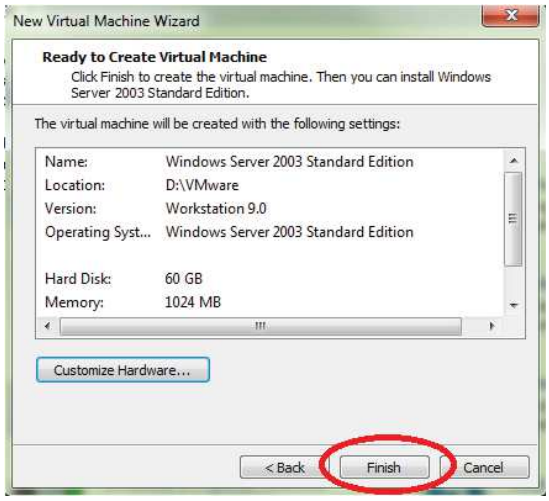
Teniendo seleccionada la capacidad del disco, se da un click en el botón *next* se para proceder a personalizar la máquina virtual según las necesidades del usuario. Esto se consigue dando *click* en el botón personalizar *hardware* como se muestra en la siguiente figura:



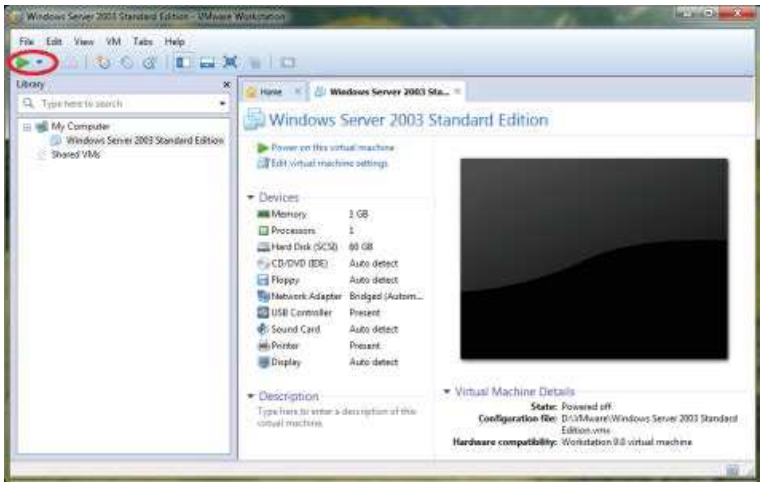
Una vez dentro de la opción personalizar *hardware*, hay que tener en cuenta 2 cosas muy importantes. La elección del tamaño de la memoria RAM que no deberá sobrepasar el 50% de la memoria física del equipo, ya que puede disminuir el rendimiento del mismo, y la elección de “puente” entre la tarjeta de red de la máquina física con la tarjeta de red de la máquina virtual (ver la siguiente figura).

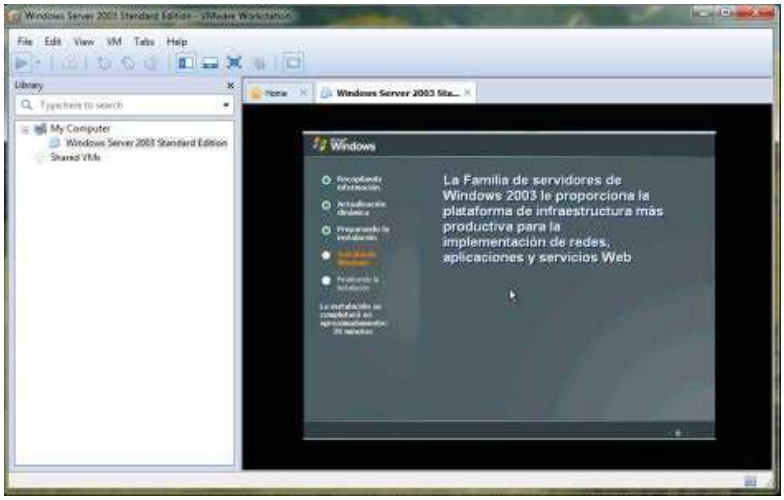


Como siguiente paso, se cierra la ventana de personalización de *hardware* y se culmina la creación de la máquina virtual dando click en el botón finalizar, como se aprecia en la siguiente figura:

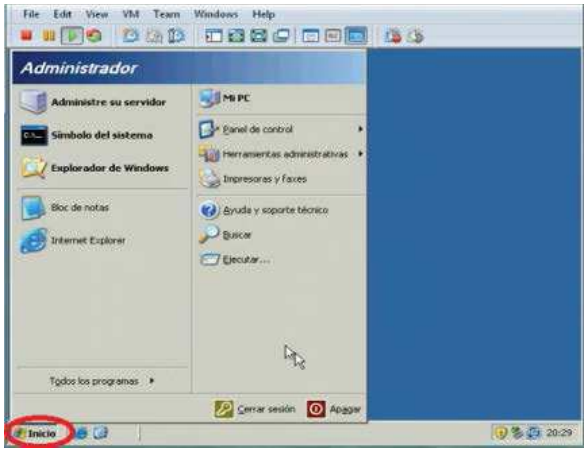


Una vez finalizada la creación de la máquina virtual, se procede al encendido de la misma, en donde el SO comenzará a cargar todos sus componentes. Este proceso puede tomar varios minutos, dependiendo de las características operativas de la maquina física, tal como se aprecia en las siguientes figuras:





Finalmente, la máquina virtual está completamente cargada (ver la siguiente figura), y despliega un escritorio idéntico al de Windows server 2003, en donde se encontraran todas las funciones y características de un SO real, con la ventaja que aquí se puede cargar cualquier *software* y no hay necesidad de adquirir un equipo físico para cada aplicativo.



- **ENCUESTA AL DEPARTAMENTO DE TI**

Los siguientes cuadros, muestran las encuestas cuantitativas realizadas en el departamento de TI de Akros, con el fin de medir la importancia que poseen los activos de la información dentro de la compañía. Se realizaron 8 encuestas similares, de las cuales se han seleccionado 3 a manera de ejemplo.

Encuestas de activos de la información al TI

Nombre: Mauricio Guaño

Cedula: 1516987043

Fecha: 22-05-2013

La siguiente encuesta tiene como intención la recopilación de información del departamento de TI, acerca de los activos de la información que posee Akros, para de esta manera tener una mejor concepción de la importancia de los mismos.

Las siguientes preguntas poseen 10 opciones en donde se entiende que 1 es bajo, 5 medio y 10 alto.

1. Cree usted que la informacion o datos generados en la empresa son de vital importancia para la misma?										
1	2	3	4	5	6	7	8	9	10	
☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Confidencialidad
☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Disponibilidad
☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Integridad
2. Cree usted que las aplicaciones adquiridas e implementadas en la empresa son importante para la misma?										
☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Confidencialidad
☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Disponibilidad
☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Integridad
3. Cree usted que toda persona dentro de la empresa deba tener acceso a los Activos de la información?										
☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Confidencialidad
☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Disponibilidad
☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Integridad
4. Cree usted que los servicios administrativos y de comercialización de productos son de importancia para la empresa?										
☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	Confidencialidad
☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	Disponibilidad
☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	Integridad
5. Cree usted que los equipos de tecnología afectan la productividad de la empresa?										
☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Confidencialidad
☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Disponibilidad
☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	Integridad
6. Cree usted que las instalaciones actuales de la empresa poseen algun benefio para la misma?										
☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	Confidencialidad
☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	Disponibilidad
☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	Integridad
7. Cree usted que otros activos que no se mencionarón anteriormente y que brindan soporte a los sistemas de la información son vitales para la empresa?										
☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	Confidencialidad
☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	Disponibilidad
☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	Integridad

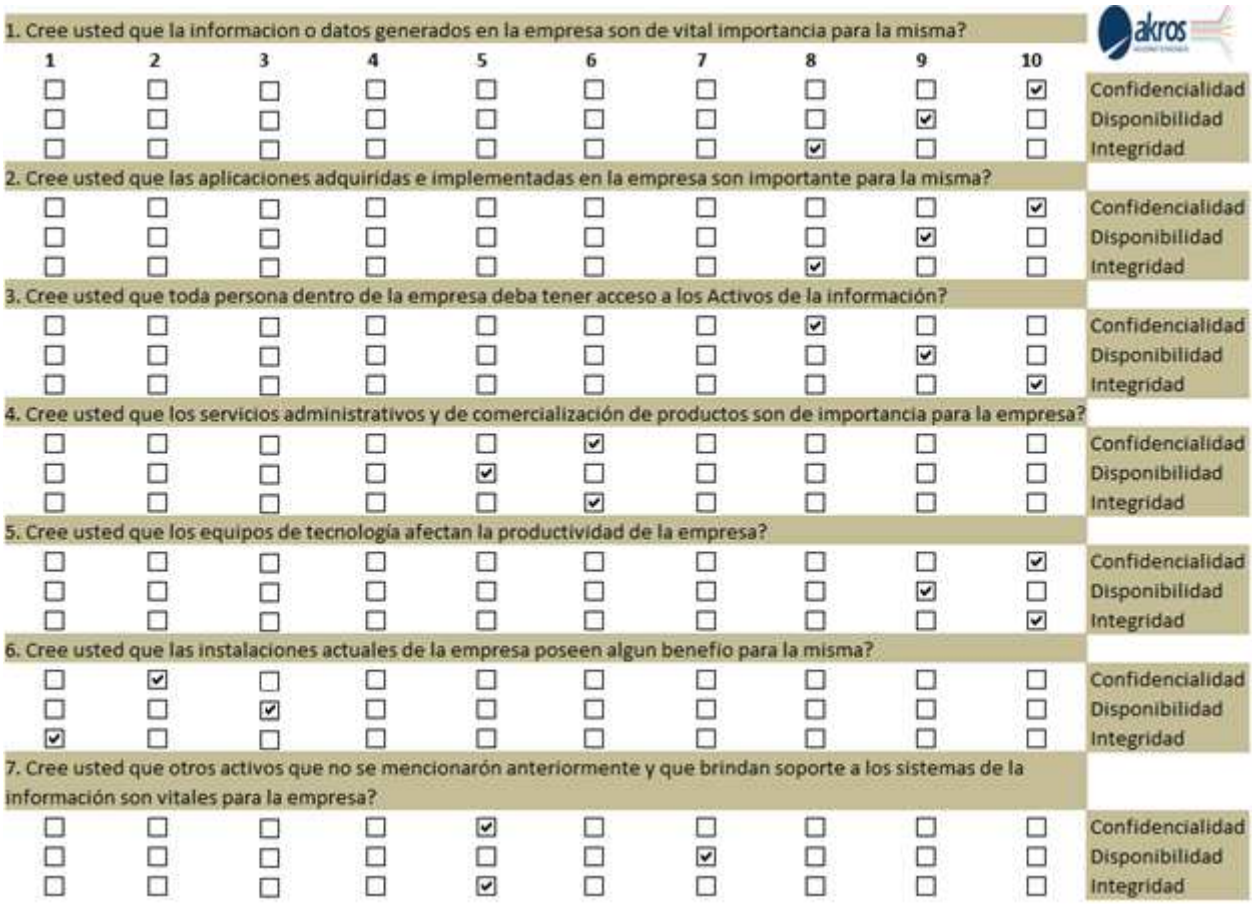
Nombre: Lupe plaza

Cedula: 1719638596

Fecha: 22-05-2013

La siguiente encuesta tiene como intención la recopilación de información del departamento de TI, acerca de los activos de la información que posee Akros, para de esta manera tener una mejor concepción de la importancia de los mismos.

Las siguientes preguntas poseen 10 opciones en donde se entiende que 1 es bajo, 5 medio y 10 alto.



	1	2	3	4	5	6	7	8	9	10	
1. Cree usted que la informacion o datos generados en la empresa son de vital importancia para la misma?											
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Confidencialidad
	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Disponibilidad
	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	Integridad
2. Cree usted que las aplicaciones adquiridas e implementadas en la empresa son importante para la misma?											
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Confidencialidad
	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Disponibilidad
	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	Integridad
3. Cree usted que toda persona dentro de la empresa deba tener acceso a los Activos de la información?											
	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	Confidencialidad
	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Disponibilidad
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Integridad
4. Cree usted que los servicios administrativos y de comercialización de productos son de importancia para la empresa?											
	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	Confidencialidad
	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	Disponibilidad
	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	Integridad
5. Cree usted que los equipos de tecnología afectan la productividad de la empresa?											
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Confidencialidad
	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Disponibilidad
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Integridad
6. Cree usted que las instalaciones actuales de la empresa poseen algun beneficio para la misma?											
	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	Confidencialidad
	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	Disponibilidad
	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	Integridad
7. Cree usted que otros activos que no se mencionarón anteriormente y que brindan soporte a los sistemas de la información son vitales para la empresa?											
	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	Confidencialidad
	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	Disponibilidad
	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	Integridad

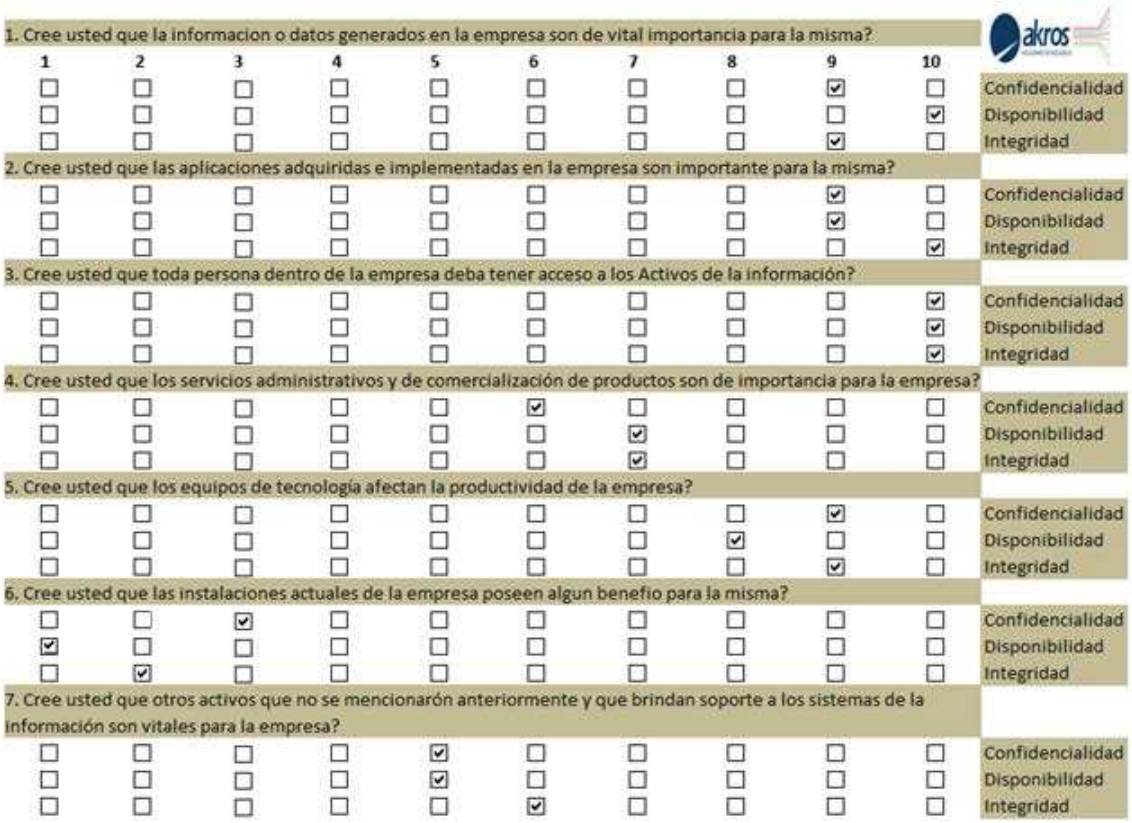
Nombre: Jaime Cajamarca

Cedula: 1836689573

Fecha: 22-05-2013

La siguiente encuesta tiene como intención la recopilación de información del departamento de TI, acerca de los activos de la información que posee Akros, para de esta manera tener una mejor concepción de la importancia de los mismos.

Las siguientes preguntas poseen 10 opciones en donde se entiende que 1 es bajo, 5 medio y 10 alto.



	1	2	3	4	5	6	7	8	9	10	
1. Cree usted que la informacion o datos generados en la empresa son de vital importancia para la misma?											
	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Confidencialidad
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Disponibilidad
	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Integridad
2. Cree usted que las aplicaciones adquiridas e implementadas en la empresa son importante para la misma?											
	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Confidencialidad
	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Disponibilidad
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Integridad
3. Cree usted que toda persona dentro de la empresa deba tener acceso a los Activos de la información?											
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Confidencialidad
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Disponibilidad
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	Integridad
4. Cree usted que los servicios administrativos y de comercialización de productos son de importancia para la empresa?											
	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	Confidencialidad
	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	Disponibilidad
	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	Integridad
5. Cree usted que los equipos de tecnología afectan la productividad de la empresa?											
	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Confidencialidad
	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	Disponibilidad
	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	Integridad
6. Cree usted que las instalaciones actuales de la empresa poseen algun benefio para la misma?											
	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	Confidencialidad
	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	Disponibilidad
	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	Integridad
7. Cree usted que otros activos que no se mencionarón anteriormente y que brindan soporte a los sistemas de la información son vitales para la empresa?											
	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	Confidencialidad
	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	Disponibilidad
	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	Integridad

Estas encuestas fueron realizadas a las 8 personas que conforman el departamento de TI de Akros, en donde las opiniones totales se resumen en la siguiente tabla:

	1	2	3	4	5	6	7	8	9	10	
Confiabilidad								I	III	IIII	1ra pregunta
Disponibilidad							I	II	III	II	1ra pregunta
Integridad								III	III	II	1ra pregunta
Confiabilidad									IIIIII	II	2da pregunta
Disponibilidad								III	IIII	I	2da pregunta
Integridad								IIII	II	II	2da pregunta
Confiabilidad							I	III		IIII	3ra pregunta
Disponibilidad								II	IIIII	I	3ra pregunta
Integridad								I	II	IIIII	3ra pregunta
Confiabilidad				I	I	IIIIII					4ta pregunta
Disponibilidad					IIIII	II					4ta pregunta
Integridad						IIII	III	I			4ta pregunta
Confiabilidad								I	III	IIII	5ta pregunta
Disponibilidad								II	III	III	5ta pregunta
Integridad								III	II	III	5ta pregunta
Confiabilidad	I	II	III	II							6ta pregunta
Disponibilidad	III		III	II							6ta pregunta
Integridad	II	IIII	II								6ta pregunta
Confiabilidad					III	II	III				7ma pregunta
Disponibilidad				I	IIII	I	II				7ma pregunta
Integridad					I	IIIIII	I				7ma pregunta

En la primera pregunta, la opinión general del departamento de TI sugiere que los datos generados dentro de Akros son muy importantes para la misma, y deberían ser resguardados adecuadamente.

En la segunda pregunta, de igual manera toda aplicación adquirida por Akros debe ser solamente empleada para los fines que fue adquirida, y debe ser manipulada por personal autorizado.

En la tercera pregunta, la mayoría de personas están de acuerdo que los activos de la información deben estar a la disponibilidad de todo el personal.

En la cuarta pregunta, la opinión general del departamento de TI está de acuerdo que los servicios administrativos y de comercialización en referencia a los activos de la información tienen un impacto moderado sobre los mismos.

En la quinta pregunta, se evidencia que todo equipo de tecnología afecta directamente a la productividad de la empresa, desde la perspectiva de TI.

En la sexta pregunta, se corrobora que las actuales instalaciones que posee Akros, no producen un beneficio significativo para la misma.

En la séptima pregunta, haciendo referencia a otros activos de la información que no fueron mencionados en esta encuesta, el personal de TI no cree que

sean de vital importancia por el momento para la empresa, sin embargo tampoco descartan su impacto a futuro sobre el beneficio de Akros.

- **MANUAL BÁSICO DE PROCEDIMIENTOS PARA EL DEPARTAMENTO DE TI**

El siguiente documento está enfocado a las actividades y funciones que se deben respetar dentro del departamento de TI de Akros, así como en las diferentes instalaciones o asistencias a clientes fuera de la empresa, para de esta manera asegurar la seguridad de la información y ejecutar mejores prácticas en caso de incidencias.

1 Responsabilidad por los activos

- Designar una persona dentro del departamento de TI a cargo de los activos de la empresa, para que esta responda inmediatamente en caso de cualquier incidente.
- En caso de pérdida o daño de algún activo, la persona a cargo deberá realizar un informe del hecho ocurrido, para buscar rápidamente una solución.
- Definir y revisar periódicamente las restricciones y clasificaciones del acceso a áreas restringidas dentro de la empresa.
- Definir el uso del correo electrónico y de internet con todos los usuarios, realizando capacitaciones y charlas.
- Documentar e identificar todos los activos ya sean estos físicos (equipos) o intangibles (reputación e imagen).
- Elaborar un proceso para el etiquetado de los activos.

2 Seguridad física

- Definir claramente los perímetros de seguridad con sus respectivas ubicaciones.
- Establecer un área de recepción con personal para poder controlar el acceso físico al lugar.
- Colocar sistema biométrico en las puertas, para controlar el acceso de personal no autorizado.

- Instalar sistemas de seguridad ya sean CCTV o alarmas para salvaguardar la integridad de un área restringida.
- El *data center* debe estar físicamente separado de lugares donde terceras personas tengan acceso.
- Se debe poseer un registro con fecha y hora para el ingreso o salida del personal de las áreas de alta sensibilidad para la empresa.
- Exigir ya sea a empleados o visitantes, el uso de alguna identificación visible para su identificación.
- Retirar o bloquear inmediatamente los derechos de acceso a los usuarios que cambien de función o dejen la empresa.
- Tener sistemas de incendios probados periódicamente, para evitar problemas al momento de un siniestro real.

3 Seguridad de equipos

- Los equipos informáticos se deben ubicar de tal modo que se logre minimizar el acceso innecesario a las áreas de trabajo.
- Los equipos que manejen información sensible, deberán estar ubicados de tal forma que se reduzca el riesgo de visualización de la información por personas no autorizadas.
- Los equipos de *networking* deberán estar aislados físicamente de los demás equipos, para reducir el nivel general de protección, y así concentrarlos en una sola area.
- No se podrá comer, beber, fumar en las cercanías de los equipos, ya que los mismos pueden sufrir daños debido a residuos alimenticios.
- Aplicar protección contra rayos, para minimizar el sobre voltaje en los equipos.
- En caso de falla tecnológica en el equipo, el usuario deberá reportar inmediatamente al departamento de TI, para su respectiva revisión.
- En caso de entrega de equipos fuera de la empresa, la persona a cargo deberá realizar un acta de entrega/recepción constatando el buen estado del activo, de esta manera se reduce en un futuro el posible reclamo del cliente final.

- En caso de entrega a domicilio de equipos recién adquiridos por el cliente, se deberá asegurarlos en caso de robo o accidente, de esta manera se minimiza el costo de reponer un equipo nuevo.
- Antes de ingresar un equipo dañado al taller técnico, el mismo deberá ser inspeccionado por personal calificado, para constatar el estado en el que ingresa.

4 Seguridad del cableado

- Las líneas de energía eléctrica y de telecomunicación deberían ser subterráneas, cuando sea posible, o tener protección alterna adecuada.
- El cableado de red deberá estar protegido contra interceptación no autorizada o daño, por ejemplo utilizando conductos y evitando rutas por áreas públicas.
- Los cables de energía deberían estar separados de los cables de telecomunicación para evitar interferencias, utilizando para esto de preferencia escalerillas.
- No exceder la distancia recomendada por el fabricante del cable (90m por lo general).
- No dejar cables desconectados o tendidos en el suelo ya que estos se pueden dañar al ser pisoteados.
- No doblar o halar los cables de manera brusca.
- No utilizar cables pelados o en mal estado, ya que estos podrían causar interferencias en la red.
- Se debe identificar todos los cables de red y energia para evitar errores de manejo.
- Es recomendable utilizar un plano del cableado para evitar errores.

5 Seguridad de los medios de almacenamiento

- Antes de ingresar a un medio de almacenamiento, este debe ser analizado por el antivirus para evitar propagación de troyanos, gusanos, *spam*, etc.

- Bajo ninguna circunstancia se dejarán sin custodia los medios de almacenamiento, o copias de seguridad de los sistemas.
- Todo medio de almacenamiento deberá ser documentado e inventariado en un registro específico.
- La ubicación física de los medios de almacenamiento deberá estar lejos del polvo, humedad, o cualquier contacto con material o químicos.
- La llave de seguridad que pertenece a los medios de almacenamiento debe estar bajo supervisión de la gerencia.

6 Mantenimiento de equipos

- Los mantenimientos deberán estar acorde con los intervalos y descripciones del proveedor.
- Solamente personal de mantenimiento previamente calificado, debería realizar esta actividad.
- En caso de mantenimiento fuera de la oficina, revisar por lo menos por dos personas que todo el material necesario este completo.
- Hacer cumplir los tiempos previamente acordados entre la empresa y el cliente.
- En caso de requerir más tiempo del establecido previamente, comunicarse directamente con el ejecutivo de cuenta a cargo del mantenimiento para que este informe respectivamente al cliente.
- Antes de empezar el mantenimiento, apagar el equipo y desconectarlo de la toma eléctrica para evitar descargas eléctricas.
- Retirar partes sensibles (discos duros, ventiladores, memorias) durante la ejecución del mantenimiento.
- No realizar el mantenimiento sobre alfombras o superficies que puedan acumular estática.
- Hacer uso de productos antiestáticos y de ser posible manipular el equipo utilizando guantes de caucho.
- Mantener registro de todas las fallas reales o sospechosas encontradas durante el mantenimiento.

- Si el equipo llega a salir de la empresa debido a su respectivo mantenimiento, por ningún motivo se lo debe dejar sin custodia.
- Una vez concluido el mantenimiento, entregar un informe al usuario final, para que este tenga conocimiento del trabajo que se realizó al equipo.

7 Monitoreo

- Identificar el ID del usuario.
- Identificar fecha, hora y detalles de los registros de inicio y de cierre.
- Chequear cambios en la configuración del sistema.
- Registrar el acceso a páginas web.
- Revisar los registros de fallas para garantizar que estas se han resuelto eficazmente.

8 Contraseñas para usuarios

- Exigir a los usuarios firmar una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo.
- Suministrar una contraseña temporal a un usuario, cuando es nuevo o cambio de área en una empresa.
- Las contraseñas temporales, deben ser entregadas personalmente, nunca ser enviadas por correo u otros medios de comunicación.
- Las contraseñas temporales, deben ser cambiadas inmediatamente por el usuario.
- Las contraseñas nunca deben ser almacenadas dentro de un computador sin contar con un formato de protección.
- No utilizar las mismas contraseñas de la empresa para propósitos personales.
- No incluir contraseñas en ningún proceso de registro automático

9 Vinculación de personal

- Conocer bien los antecedentes, referencias personales y laborales, con el fin de determinar que no genera una amenaza para la empresa.

- El contrato de vinculación debe incluir cláusulas de confidencialidad asociadas a la protección de la información y a los delitos contenidos en la ley.
- El contrato de vinculación debe informar en qué condiciones se auditara el correo electrónico institucional del empleado, así como los activos que le sean asignados.
- Informar a los empleados que el acceso a internet solo estará disponible para fines profesionales
- Notificar los derechos, responsabilidades y deberes que asumen en cada cargo en cuanto a la seguridad del equipo y la información contenida en este.

10 Procedimientos contra incidentes

- En el caso de daño de equipos fuera de la oficina, determinar las fallas, ya sean estas de *hardware* o de *software*. Resolver la falla si es factible, caso contrario se debe generar un informe técnico especificando el problema y la parte o partes a ser remplazadas.
- Una vez detectado el problema, informar al cliente, haciéndole conocer las partes afectadas, o en su caso informándole acerca de los requerimientos mínimos de operatividad del equipo afectado, para que en el futuro no tenga el mismo problema.
- En caso de no poder comunicarse con la oficina para informar que el mantenimiento y/o asistencia técnica ha concluido, colocar esta observación en el informe final.
- En el caso de *hackeo* al equipo, verificar si se ha producido una violación de la confidencialidad y la integridad a los documentos más importantes.
- En el caso de configuración de nuevos equipos, de preferencia desempaquetarlos en presencia del cliente, explicándole los componentes del equipo, para posteriormente proceder a la respectiva configuración.

- En el caso de sacar respaldos, se debe tener mucho cuidado de no pasar por alto ningún documento y/o archivo, ya que esto puede ocasionar problemas futuros con el usuario final.

11 Capacitación de usuarios

- Realizar una explicación adecuada de las aplicaciones corporativas que utiliza la compañía.
- Explicación de las políticas y normas de seguridad que la empresa posee.
- Explicación y/o aclaración de las áreas restringidas que posee la empresa.
- Realización de práctica de informes de asistencias técnicas creados para los clientes finales.
- Hacer énfasis en el uso apropiado de los servicios de Internet.
- Como evitar la entrada de virus y otros códigos dañinos.
- Reconocer las técnicas más frecuentes de ingeniería social, para evitar ser víctimas de este tipo de engaños.
- Como gestionar los soportes informáticos, los equipos y los dispositivos portátiles.
- Como reaccionar ante determinados incidentes que puedan comprometer la seguridad de la información o el acceso a los recursos del sistema.

Con la puesta en marcha de este manual básico de procedimientos para el departamento de TI de Akros, se podrá empezar a tener un mayor dominio sobre los activos de la información, permitiendo así a cada usuario tener un control muy elevado sobre los mismos.

Por otro lado, esta manual también permitirá al departamento de TI mejorar la seguridad, confidencialidad e integridad de cada uno de los activos de la información que posee la empresa, de este modo se reducirán fallas humanas al momento de manejar y operar los activos.