UNIVERSIDAD HISPANOAMERICANA

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA INFORMÁTICA

TÍTULO DEL PROYECTO: PROPUESTA DE LA ARQUITECTURA DE LA RED DE COMUNICACIONES DE LA EMPRESA STEINCORP EN ESCAZÚ PARA SU HOMOLOGACIÓN CON LA RED DE LA SEDE CENTRAL EN CARTAGO, APLICANDO MÉTODOS DE DISEÑO DE REDES, PARA EL PRIMER TRIMESTRE DEL 2018

JONATHAN CRUZ HIDALGO

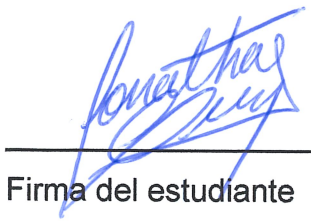
DIRECTORA: YENORY ROJAS HERNÁNDEZ

AGOSTO 2017

DECLARACIÓN JURADA

Yo **Jonathan Cruz Hidalgo**, mayor de edad, portador de la cédula de identidad número **1-1054-0033** egresado de la carrera de **Ingeniería Informática** de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de **Bachillerato en Ingeniería Informática**, juro solemnemente que mi trabajo de investigación titulado: **Propuesta de la arquitectura de la red de comunicaciones de la empresa SteinCorp en Escazú para su homologación con la red de la sede central en Cartago, aplicando métodos de diseño de redes, para el primer trimestre del 2018**, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los **22** días del mes de **agosto** del año dos mil **diecisiete**.



Firma del estudiante

Cédula: 1-1054-0033

CARTA DEL TUTOR

Llorente, 22 de Agosto del 2017

Señora Yenory Rojas Hernández
Directora Ingeniería Informática
Universidad Hispanoamericana

Estimada señora:

El estudiante *Jonathan Cruz Hidalgo*, cédula de identidad número 1-1054-0033, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado PROPUESTA DE LA ARQUITECTURA DE LA RED DE COMUNICACIONES DE LA EMPRESA STEINCORP EN ESCAZÚ PARA SU HOMOLOGACIÓN CON LA RED DE LA SEDE CENTRAL EN CARTAGO, APLICANDO MÉTODOS DE DISEÑO DE REDES, PARA EL PRIMER TRIMESTRE DEL 2018, el cual ha elaborado para optar por el grado académico de Licenciatura.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del *problema*, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	9
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	18
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	27
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	18
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	18
	TOTAL		90

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

Ing. José Roberto Santamaría Sandoval MGP
Cédula identidad N 1-1178-0664
Carné Colegio Profesional N IE-15830.

CARTA DE LECTOR

San José, 22 de Julio del 2017

Ing. Yenory Rojas Hernández PhD.
Ingeniería en Informática
Universidad Hispanoamericana

Estimada señora

El estudiante Jonathan Cruz Hidalgo, cédula de identidad 1-1054-0033, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "Propuesta de la arquitectura de la red de comunicaciones de la empresa Steincorp en Escazú para su homologación con la red de la Sede Central en Cartago, aplicando métodos de diseño de redes, para el primer trimestre del 2018", el cual ha elaborado para obtener su grado de Bachillerato en Ingeniería Informática.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.

Lic. Pedro I. Leiva Chinchilla.
1-1394-0453

CARTA DE REVISIÓN FILOLÓGICA

San José, 24 de octubre de 2017

Señores
Universidad Hispanoamericana
Escuela de Ingeniería Informática

Estimados señores:

El estudiante **Jonathan Cruz Hidalgo** me ha presentado, para efectos de corrección de estilo, en mi calidad de profesional graduado en Filología y Enseñanza del Español, el Proyecto de Graduación denominado **Propuesta de la arquitectura de la red de comunicaciones de la empresa SteinCorp en Escazú para su homologación con la red de la sede central en Cartago, aplicando métodos de diseño de redes, para el primer trimestre del 2018**, el cual ha sido elaborado como parte de los requisitos de la carrera de Ingeniería en Sistemas.

He revisado, de acuerdo con los lineamientos de la corrección de estilo señalados por la Universidad, los aspectos de estructura gramatical, acentuación, ortografía, puntuación y los vicios de dicción que se trasladan a lo escrito, y he verificado que se han realizado todas las correcciones indicadas en el documento.

Agradeciendo su atención,

Lic. Henry Rivera Morales
Céd. 1-1195-0430
N° 036633
Colegio de Licenciados y Profesores

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Glosario

AP: Access Point en inglés, su traducción es Punto de Acceso Inalámbrico y su plural es APs, son los dispositivos que se emplean para poder brindar las redes inalámbricas.

Switch: Equipo conmutador de interconexión que opera en la capa de enlace, aquí se conectan los distintos equipos que necesitan acceso mediante los puntos de red.

LAN: Local Area Network, o traducido a Red de Área Local, son las redes que se encuentran comúnmente en las oficinas y casas.

WiFi: Forma de conexión de los dispositivos de forma inalámbrica y utilizan a los APs para poder brindar su servicio.

SSID: El comúnmente llamado Nombre de la Red inalámbrica y es la red inalámbrica a la cual se conectan los equipos.

GUI: Interfaz gráfica de usuario, generalmente por una aplicación o acceso web conectado a la IP del dispositivo.

CLI: Interfaz por líneas de comandos, generalmente se utiliza una aplicación conectada directamente al equipo por un cable consola.

VLan: Red virtual utilizada en conmutadores de capa 2 y 3 para administración y segmentación de subredes.

IP: Número que identifica a un dispositivo en la red, después de una conexión exitosa.

FW: Firewall o dispositivos de seguridad perimetral.

UTM: Traducido como Gestión Unificada de Amenazas, es un dispositivo que incluye una gran variedad de aplicaciones para proteger la seguridad de la red.

DHCP: Servicio que le asigna una IP dinámica a los dispositivos conforme se van conectando y autentificando a la red.

WG: WatchGuard, marca del Firewall y de los APs.

HP: Hewlett-Packard, marca de los conmutadores.

UTP: Cables compuestos de cuatro pares de cable trenzados, usados en los cables de red y otras aplicaciones.

PoE: Alimentación de corriente mediante la red alámbrica.

O365: Office 365, conjunto de aplicaciones como servicio que ofrece Microsoft.

MS: Microsoft Corporación.

CAPÍTULO I

PLANTEAMIENTO DEL TEMA

1.1 DEFINICIÓN DEL PROBLEMA

Con base en los puntos anteriores: ¿De qué manera se puede optimizar y homologar la red de Escazú con la sede central tomando en cuenta la proyección de crecimiento?

El problema de la red de comunicación de la sede en Escazú radica primordialmente en la obsolescencia tecnológica de los equipos de comunicación y su saturación, como resultado están las interrupciones del servicio que generan un impacto económico y el riesgo de afectar la calidad del servicio que se les brinda a los clientes. De modo macro se puede mencionar que el problema principal de la obsolescencia tiene tres impactos diferentes:

A. La incompatibilidad entre los equipos, debido a que los actuales "*Switch*" de comunicación de la sede en Escazú son competencia directa en el mercado en referencia de los equipos *Firewall*. Esto ha dado ciertos problemas a la hora de configuración de VLAN y otras publicaciones, "Los UTM y las plataformas de seguridad NGFW de WatchGuard se diseñaron con la finalidad de simplificar el proceso de añadir tecnologías de reciente aparición" (Vieira, 2015, Párrafo 2).

B. El dimensionamiento que se tomó en cuenta cuando se implementó la sede de Escazú hace más de 5 cinco años, no dio el rendimiento 2 años después, y en los últimos meses está colapsando la red *Wireless*, debido a que hay más usuarios y muchos más sistemas en línea que en sus inicios.

C. La experiencia del usuario que tiene la flexibilidad de trabajar tanto en la sede en Escazú como en la de Cartago, ha impactado al resto de colaboradores con base en sus comentarios cuando comparan una red con la otra.

Ahora se desarrollarán a detalle los problemas presentados en la red gracias al Diagrama de Ishikawa representado en la siguiente figura:

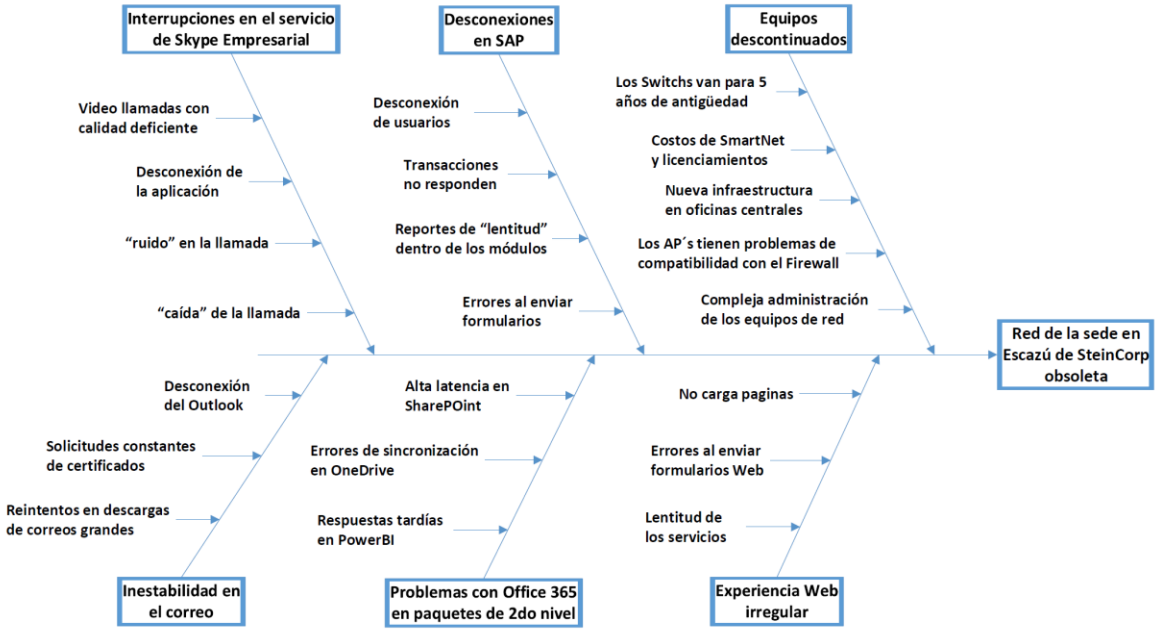


Figura 1: Diagrama de Ishikawa

Fuente: Diseño propio.

- **Equipos descontinuados:** El principal problema con el que lidian los usuarios de la red de la sede en Escazú es consecuencia de que los "Switch" y "access point" cumplirán en el 2017 los cinco años, además de estar instalado un "switch"

3Com del que ignoramos su antigüedad. Además, se debe indicar que los equipos instalados representan un costo anual de $3500 en “smart net” y licenciamiento del “Wireless Controler”, gasto innecesario para equipos sin valor en libros.

Cabe mencionar que los equipos de red de la compañía en Escazú ya quedaron obsoletos en comparación a la nueva red implementada en la sede central de Cartago, a esto se le agrega que los Puntos de Acceso Inalámbrico actuales son incompatibles con el *firewall* de la organización. Lo anterior limita las características propias y recarga en procesos a este dispositivo, situación que no sucede en la red de Cartago, ya que los “APs” son compatibles y este funciona como Controlador de Redes Inalámbricas, situación que logra trasladar los procesos del filtrado Web a los AP, liberando de procesamiento y memoria al equipo central.

En la figura que sigue, se muestra la ventana gráfica del Controlador de Redes Inalámbricas con el cual cuenta el dispositivo de seguridad perimetral, y se distinguen los Puntos de Acceso Inalámbricos de los cuales está constituida la red, todo esto al mismo costo de inversión adicional.

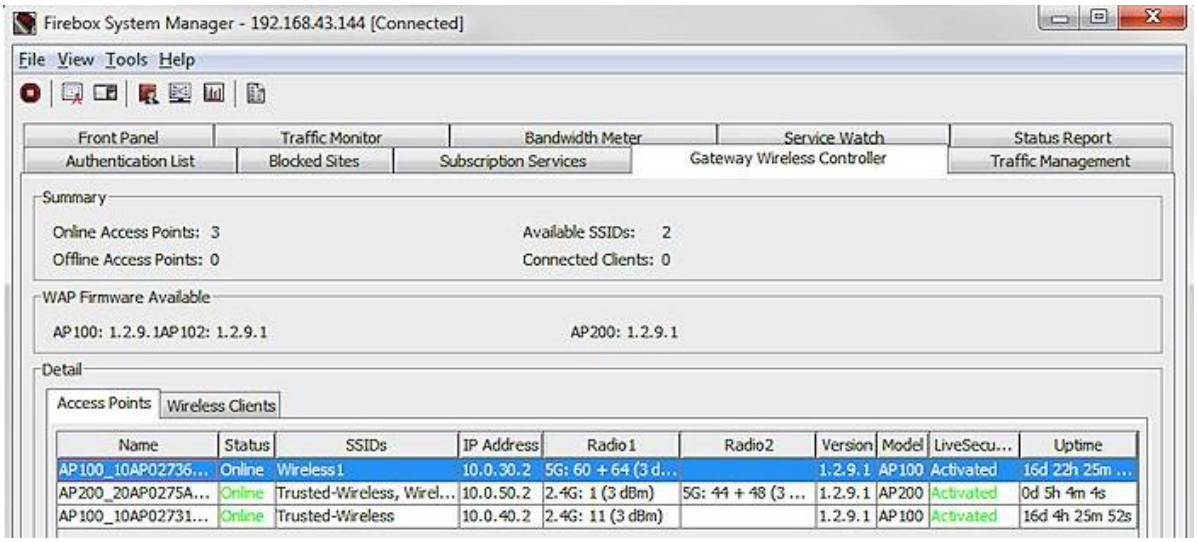


Figura 2*:* Controlador Inalámbrico WatchGuard

Fuente: Imagen tomada de la aplicación, propiedad de SteinCorp

La tecnología existente en Escazú es complicada de administrar, lo que incrementa la dependencia del departamento de proveedores certificados y a su vez el mantenimiento a un costo mayor, en comparación a la tecnología ya instalada en Cartago. Adicionalmente están los conmutadores HP, que "…(son) compatible(s) con una amplia gama de interfaces de gestión con GUI web, línea de comandos (CLI) y SNMP con puertos de micro USB o consola" (HP), lo que facilita su administración, y su sencillez logra implementaciones en menor tiempo.

- **Interrupciones en el servicio de Skype Empresarial:** Como consecuencia de la red obsoleta de SteinCorp en Escazú, cuando se realiza una video llamada por Skype, inclusive entre la misma red, la calidad es deficiente, se "pixelea" o se desfasa el video en relación con el audio. También se presentan casos de

desconexión abrupta de la aplicación de Skype Empresarial debido a que se da una saturación de la red y los AP se reinician.

Para contrarrestar este problema, se ha recomendado el uso de la conexión alámbrica en el escritorio, aunque esta no debe ser la regla, ya que estamos en la era de la movilidad. Las laptops más modernas no cuentan con el conector RJ45 y aunque esté conectado al cable, se ha reportado interferencia o pequeños cortes momentáneos entre 2 y 7 segundos en medio de una llamada, incluso algunas llamadas se cortan definitivamente.

- **Desconexiones del cliente de SAP y sus servicios:** La experiencia con esta aplicación ha generado mucha inconformidad, ya que hay reportes de usuarios que están trabajando dentro de un módulo y se desconectan o cuando se completa un formulario y se aplica la transacción, retorna un error y deben volver a digitar toda la información, esta es una recurrencia que genera grandes pérdidas anuales en minutos de productividad total.

Adicionalmente, otro reporte de los usuarios es que cuando trabajan dentro de los mandantes, módulos o transacciones, SAP tarda considerablemente en responder. Esta herramienta en particular se ve muy afectada y es de suma importancia en esta sede, ya que los mayores consumidores son del departamento de finanzas, pilar de la organización.

- **Inestabilidad en el cliente de Outlook:** Los problemas del cliente de Outlook son comunes y asociados a la latencia de la red, como lo son no refrescar los correos, desconectarse, reiniciar la descarga de algún correo de considerable tamaño (más de 5mb). Adicional al error de desconexión, de forma frecuente aparece la ventada de aceptación de certificado de seguridad, esto es causado cuando la herramienta se desconecta y conecta automáticamente.

- **Problemas con otras aplicaciones en Office365**: Con lo referente a la experiencia de SharePoint, se detecta una alta latencia en los tiempos de respuesta, al navegar entre las páginas o al trabajar con archivos. La cantidad de errores de sincronización de OneDrive es considerable, el mayor indicador de ese problema, por parte de Microsoft, son problemas de latencia en medio de la sincronización.

La experiencia de “PowerBI” no es la óptima, existe latencia cuando se refrescan los reportes. En la figura de a continuación se muestra un pequeño diagrama de los factores que pueden afectar la comunicación con Office365.

Figura 3*:* Principales factores que afectan al rendimiento de red

Fuente: Web de Microsoft Support

- **Experiencia en la navegación web irregular:** Este es otro de los casos comunes, el error 404 al cargar páginas web, aunque después de 2 o 3 presiones sobre F5, carga correctamente. Otros casos son al completar un formulario web y darle “enviar”, da error, y además la experiencia de navegación se siente con poca velocidad.

1.2 JUSTIFICACIÓN DEL PROYECTO

Con base en toda la problemática que se explicó en la introducción, la renovación de los equipos debe ser algo prioritario para la organización, ya que implica una mejora real en la experiencia y productividad de los colaboradores de la sede de la compañía en Escazú, esto tomando como referencia el caso de éxito en la implementación de la nueva red en Cartago.

“Las redes más modernas mejoran las TI y el rendimiento del negocio” (T-Systems International GmbH, 2016). Un problema real es la obsolescencia de los actuales equipos que están llegando al final de su vida útil, y como consecuencia, se están incrementando los costos de mantenimiento por sus frecuentes fallas. De forma colateral, esto causa descontento en los colaboradores que delegan la responsabilidad y presión al departamento de TI, en un círculo de buscar culpables.

Como caso de éxito se tiene la renovación completa de todos los equipos de la red de la sede central en Cartago, a esta fecha se lleva una inversión de $54.000 de un presupuesto de $100.000. Adicional a esto, cuando surge un nuevo requerimiento

de red de algún país, esta red se implementa tomando en cuenta a los requisitos y estándares de la sede central, para con esto homologar poco a poco los países con base en Cartago. Así nace una razón más que sustenta la importancia de actualizar la red de la sede en Escazú y homologarla a los estándares de “casa matriz”.

“Los efectos de las redes obsoletas son claros, desde el alto nivel de latencia a las tasas de transferencia de datos irregulares” (T-Systems International GmbH, 2016), sumado a la tecnología e inversión, se puede citar como otra justificación la importancia de las oficinas de Escazú en relación con la cantidad de colaboradores, esto coloca a esta sede como la segunda más grande, superada solo por la sede central. Es en Escazú donde se concentra el “Core Administrativo” de la organización, punto central de los directivos, recursos humanos, ventas y otros departamentos claves para la empresa, por ello la prioridad de ajustar y brindar el servicio que exigen esos puestos.

Desde un punto de vista técnico, se debe indicar una justificación clave como la disminución de los procesos en el firewall y delegar parte de los procesos de seguridad a la red WiFi, “Los puntos de acceso inalámbricos de WatchGuard superan este desafío extendiendo la mejor seguridad UTM de su clase, desde el firewall WatchGuard hasta la WLAN” (WatchGuard), ya que la tecnología que presenta este dispositivo al integrar varias tareas de seguridad de red en un mismo dispositivo (como lo son las VPNs entre sitios y de usuarios, protección perimetral, filtrado de contenido, control de amenazas persistentes avanzadas, el filtrado web por usuario, entre otras) incluyendo un Controlador Inalámbrico con puntos de acceso de la misma marca. Esto ha ayudado

a delegar los procesos de seguridad a los APs, liberando de esa carga al “firewall” y así permitiendo un mejor rendimiento del hardware y prolongar su vida útil, como lo identifica la hoja de características del dispositivo. Esta tecnología de controlador inalámbrico integrada “ayuda a obtener grandes ahorros, sin costos adicionales de hardware de controlador, sin cargos de ubicación de AP ni de licencia de software del controlador” (WatchGuard).

Por último, pero no menos importante, el ahorro en renovaciones y mantenimiento es otra justificación, ya que al adquirir los equipos nuevos se libera a la organización del pago de horas de mantenimiento anuales. La nueva tecnología que se propone instalar es mucho más fácil de mantener y la curva de aprendizaje se reduce considerablemente, además el equipo de colaboradores está entrenado en los dispositivos de Cartago, lo que significa que mucho del trabajo que realizaba el proveedor certificado ahora se puede ejecutar con el equipo propio de TI. Esto libera horas de soporte reactivo y lo traslada a nuevos proyectos, además que los costos por “smartnet” desaparecen, las renovaciones por licenciamiento se reducen considerablemente y el licenciamiento del “Wireless Controler” desaparece completamente.

Otra justificación real es el consumo de la red. En la inauguración de la sede de Escazú en el 2013, solo 60 colaboradores concurrentes estaban en la oficina, para estos inicios del 2017 se cuenta con 120 colaboradores y sus BYOD (“*Bring your own device*”, traducción: trae tu propio dispositivo) que era un término en aquel momento

alejado de la realidad que lo es hoy en día, y existe una proyección de crecimiento de recurso humano del 14%.

En resumen, la justificación de este proyecto se centra en los ahorros que se verán reflejados en la compra de los equipos, así como en su mantenimiento, desaparición de garantías anuales, licenciamientos y tiempos de espera, ya que gran parte del trabajo lo puede realizar el personal del departamento de TI. Paralelo a esto se obtiene la mejora de la red para el soporte de una mayor cantidad de usuarios y dispositivos concurrentes.

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 OBJETIVO GENERAL

- Proponer la arquitectura de red de comunicaciones de la empresa SteinCorp en Escazú para su homologación con la red de la sede central en Cartago.

1.3.2 OBJETIVOS ESPECÍFICOS

- Diagnosticar la situación actual de la red de comunicaciones de la empresa en su sede de Escazú evaluando los equipos existentes para la definición de las brechas a nivel técnico y operativo.

- Establecer los requerimientos que la empresa necesita evaluando proveedores y alcances para la identificación de los equipos de su nueva red de comunicaciones en la sede de Escazú.

- Diseñar la arquitectura necesaria estimando los requerimientos con el diagnóstico para un dimensionamiento real de la nueva red de comunicaciones de la empresa en su sede de Escazú.

- Establecer un plan piloto comparando la situación actual de la red con la diseñada en esta propuesta para demostrar la necesidad del proyecto en SteinCorp de su sede de Escazú.

1.4 MARCO DE REFERENCIA EMPRESARIAL Y CONTEXTUAL

Laboratorios Stein nace en 1980 como una compañía costarricense dedicada a la producción y comercialización de medicamentos para uso humano. En los últimos 5 años cambia su nombre a SteinCorp, con este nuevo nombre pretende conocer en su nuevo giro de negocio corporativo, buscando la ampliación a nivel regional de sus productos y una forma más corporativa de ejercer las tomas de decisiones. Esto es reforzado por alianzas estratégicas de distribución genial con grandes farmacéuticas mundiales y consolidando en su nuevo laboratorio las tecnologías de vanguardia con certificaciones que buscan abrir aún más su mercado regional.

Su misión es contribuir en forma sostenible con la salud y calidad de vida de las personas, ofreciendo un amplio acceso a productos de clase mundial, apegados a las mejores prácticas de la industria y con un servicio de excelencia dentro de un marco ético y de respeto por el ambiente. Su visión es ser una empresa farmacéutica líder en los mercados en que opera, siendo innovadora, globalizada, con una oferta accesible de productos de calidad y orientada a la salud integral de las personas. Su objetivo es buscar la excelencia en el servicio al cliente, el enfoque que se está imprimiendo en la organización es una realidad en el corto, mediano y largo plazo.

Para SteinCorp es la convicción de saber escuchar al cliente y dar el servicio en tiempo y calidad, bajo una premisa de la mejora continua, que se traduce en el día a

día en la búsqueda de la excelencia. Más allá de atender una queja es comprender, que una queja es un reto para la mejora y para el crecimiento de la organización.

Crecer de la mano de la exportación es el paso de ser una empresa familiar a una organización que da lugar a la creación de la Corporación Stein, los ha llevado a cruzar fronteras y romper barreras en el campo farmacéutico, apoyados en un grupo de talentosos colegas que brindan día a día su mejor esfuerzo en la consecución de este logro. En los próximos cinco años, SteinCorp pretende crecer en el portafolio de productos de las líneas cardio-metabólico, gastroenterología y ginecología, así como el desarrollo de una nueva línea en Neurociencias.

“Con éxito enfrentamos el reto de romper las barreras que impone la diversidad social y cultural en materia de salud” (Waserstein, 2016). Para lograr todo este crecimiento, la organización está comprometida a crecer en la inversión en el talento humano, apoyándose de la remodelación y ampliación de la planta y consolidando la posición de privilegio en el mercado centroamericano, Ecuador y República Dominicana. Es en este crecimiento en infraestructura, maquinaria y talento humano que este proyecto se basa, en consolidar la experiencia de los colaboradores de la organización en sus dos sedes de Costa Rica, para una experiencia en redes satisfactoria y que erradique los errores. Siempre se vela por la salud de las personas, la prioridad de la organización.

En SteinCorp se posee un efectivo sistema que permite administrar y mejorar la calidad de los productos y servicios, ya que se cuentan con políticas claras, responsabilidades y líneas de autoridad bien definidas; es una empresa que se esfuerza por mantener una infraestructura moderna y un excelente ambiente de trabajo. La decisión de mejorar impone satisfacer las necesidades de los clientes, para SteinCorp el mejoramiento continuo es una norma. Hablar de Stein es hablar de gestión de calidad.

Se nace como una compañía costarricense dedicada a la producción y comercialización de medicamentos para uso humano; y de ser un laboratorio que atendía únicamente al mercado nacional, se evoluciona a una Corporación que abarca distintos ámbitos del quehacer farmacéutico. En SteinCorp no se habla de negocio, sino de compromiso, y este es el de la producción y comercialización de medicamentos para uso humano.

En resumen, Laboratorios Stein nace en 1980 como una compañía costarricense dedicada a la producción y comercialización de medicamentos para uso humano. Gracias al compromiso de sus colaboradores en la década de los noventa ya contaba con operaciones en toda el área centroamericana, desde Guatemala hasta Panamá, región con una población superior a los 38 millones de habitantes; así continúa creciendo a pasos agigantados gracias a su gran calidad, y en el 2004 inicia operaciones en Ecuador y en el 2008 en República Dominicana. Se ha evolucionado de

una empresa familiar a una corporación con presencia en Centroamérica, República Dominicana y Ecuador, además de sus conexiones con Sudamérica y la India.

1.5 ALCANCES Y LIMITACIONES

1.5.1 ALCANCES

- El primer entregable del proyecto será la documentación en donde se resuma de forma puntal y concreta un diagnóstico de la situación actual de la red en la sede de Escazú, así como el inventario de equipos y su comparación con los ya actualizados e instalados en la sede de Cartago, los cuales serán la base de la homologación.

- Posterior a dicho trabajo como segundo entregable se tendrá la documentación en donde se establezcan los requerimientos de la empresa para la nueva red de comunicaciones, y en donde se identificarán los equipos necesarios y proveedores que podrán participar según ofertas, además un cuadro comparativo de los precios de todas las ofertas recibidas.

- El tercer entregable será el diseño de la arquitectura necesaria para el correcto funcionamiento de la red, con base en un diagrama en “Microsoft Visio” donde se identifiquen los equipos en cada piso, sus zonas, IP de administración según la

“VLan” con un usuario / contraseña para implementación, todo debidamente documentado.

- Después de establecer un plan piloto que demuestre la necesidad del proyecto, el cual será presentado a Gerencia de TI como un “Demo”, el cuarto y último alcance del proyecto será el informe escrito del “Demo”, la documentación de la propuesta y una presentación resumen en formato financiero en MS PowerPoint para exponerla al Director Financiero de SteinCorp, para la aprobación del proyecto.

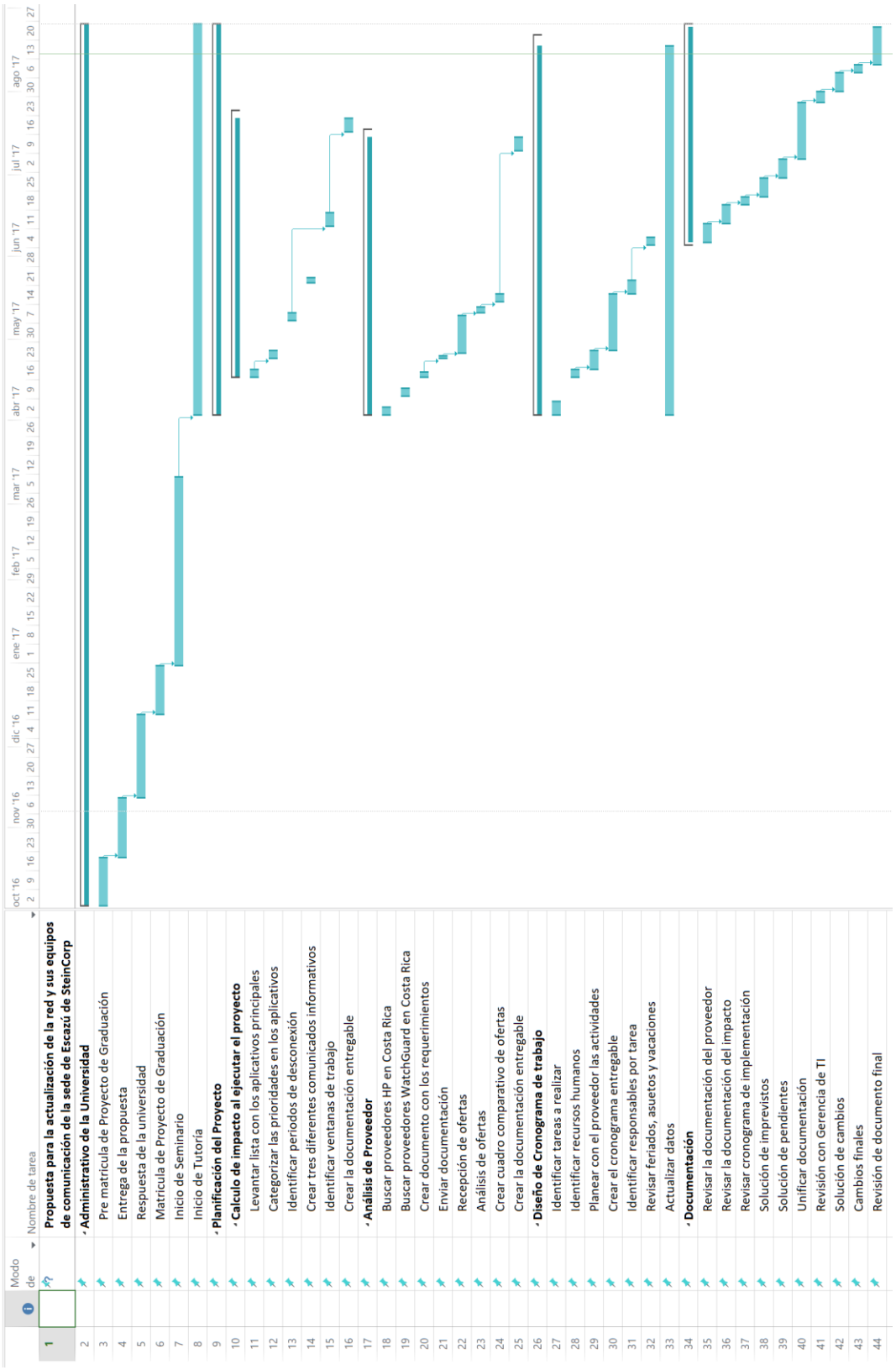
1.5.2 LIMITACIONES

- La primera limitación será que los equipos de hardware que se instalarán deberán ser completamente compatibles con los ya instalados en Cartago, esto para continuar con los equipos bajo el estándar inicial y complementar la infraestructura total de la organización.

- Otra limitación es la del tope de presupuesto para el proyecto, que será de $20.000 máximo, se podrán evaluar otras alternativas como infraestructura como servicio (IaaS), como adicionales.

- Como limitación adicional se solicitará que los trabajos sean agendados fines de semana o en horario nocturno para no impactar a la organización y dejar tiempo suficiente para pruebas y la puesta en marcha.

1.6 CRONOGRAMA DE ACTIVIDADES



Propuesta para la actualización de la red y sus equipos de comunicación de la sede de Escazú de SteinCorp			
Nombre de tarea	**Duración**	**Comienzo**	**Fin**
Administrativo de la Universidad	**235 días**	**lun 3/10/16**	**vie 25/8/17**
Pre matricula de Proyecto de Graduación	14 días	lun 3/10/16	jue 20/10/16
Entrega de la propuesta	16 días	jue 20/10/16	vie 11/11/16
Respuesta de la universidad	21 días	vie 11/11/16	lun 12/12/16
Matricula de Proyecto de Graduación	14 días	lun 12/12/16	vie 30/12/16
Inicio de Seminario	50 días	vie 30/12/16	vie 10/3/17
Inicio de Tutoría	105 días	lun 3/4/17	vie 25/8/17
Planificación del Proyecto	**105 días**	**lun 3/4/17**	**vie 25/8/17**
Calculo de impacto al ejecutar el proyecto	**71 días**	**lun 17/4/17**	**lun 24/7/17**
Levantar lista con los aplicativos principales	3 días	lun 17/4/17	mié 19/4/17
Categorizar las prioridades en los aplicativos	3 días	lun 24/4/17	mié 26/4/17
Identificar periodos de desconexión	3 días	lun 8/5/17	mié 10/5/17
Crear tres diferentes comunicados informativos	2 días	lun 22/5/17	mar 23/5/17
Identificar ventanas de trabajo	5 días	lun 12/6/17	vie 16/6/17
Crear la documentación entregable	5 días	lun 17/7/17	vie 21/7/17
Análisis de Proveedor	**76 días**	**lun 3/4/17**	**lun 17/7/17**
Buscar proveedores HP en Costa Rica	3 días	lun 3/4/17	mié 5/4/17
Buscar proveedores WatchGuard en Costa Rica	3 días	lun 10/4/17	mié 12/4/17
Crear documento con los requerimientos	2 días	lun 17/4/17	mar 18/4/17
Enviar documentación	1 día	lun 24/4/17	lun 24/4/17
Recepción de ofertas	10 días	mié 26/4/17	mar 9/5/17
Análisis de ofertas	2 días	jue 11/5/17	vie 12/5/17
Crear cuadro comparativo de ofertas	3 días	lun 15/5/17	mié 17/5/17
Crear la documentación entregable	5 días	lun 10/7/17	vie 14/7/17
Diseño de Cronograma de trabajo	**101 días**	**lun 3/4/17**	**lun 21/8/17**
Identificar tareas a realizar	5 días	lun 3/4/17	vie 7/4/17
Identificar recursos humanos	3 días	lun 17/4/17	mié 19/4/17
Planear con el proveedor las actividades	5 días	mié 19/4/17	mié 26/4/17
Crear el cronograma entregable	15 días	jue 27/4/17	mié 17/5/17
Identificar responsables por tarea	3 días	jue 18/5/17	lun 22/5/17
Revisar feriados, asuetos y vacaciones	3 días	lun 5/6/17	mié 7/6/17
Actualizar datos	99 días	lun 3/4/17	jue 17/8/17
Documentación	**60 días**	**lun 5/6/17**	**vie 25/8/17**
Revisar la documentación del proveedor	5 días	mar 6/6/17	lun 12/6/17
Revisar la documentación del impacto	5 días	lun 12/6/17	lun 19/6/17
Revisar cronograma de implementación	3 días	lun 19/6/17	jue 22/6/17
Solución de imprevistos	5 días	jue 22/6/17	jue 29/6/17
Solución de pendientes	5 días	jue 29/6/17	jue 6/7/17
Unificar documentación	15 días	jue 6/7/17	jue 27/7/17
Revisión con Gerencia de TI	2 días	jue 27/7/17	lun 31/7/17
Solución de cambios	5 días	lun 31/7/17	lun 7/8/17
Cambios finales	3 días	lun 7/8/17	jue 10/8/17
Revisión de documento final	10 días	jue 10/8/17	jue 24/8/17

CAPÍTULO II

MARCO TEÓRICO

En este capítulo se dará inicio al desarrollo de los conceptos, ideas y tecnologías que van en relación con el proyecto, logrando así poder dar claridad a los términos y llevar al lector para que adquiera o enriquezca su conocimiento para una fácil comprensión del problema que se desea solventar en esta propuesta.

2.1 TELEMÁTICA

Dentro de las ramas de la informática, la que se utilizará en este proyecto será la Telemática.

> “Se puede definir a la Telemática como parte de una Ciencia, buscando brindar el desarrollo de las tecnologías que buscan el constante desarrollo en conjunto tanto de las Telecomunicaciones como de la Informática, brindando metodologías, procesos, técnicas y hasta servicios que pueden resultar útiles para ambas o su aplicación en conjunto” (Revista Electrónica Master magazine, Párrafo 3).

Esta definición ha servido para que grandes profesionales del área en conjunto con grandes corporaciones que inyectan dinero a la investigación y descubrimiento de nuevas tecnologías a llevar conceptos pequeños a grandes trasnacionales y de tecnología de vanguardia y alto costo a las pequeñas empresas y hasta hogares. La ciencia de la computación llevada a las telecomunicaciones ha sido de vanguardia y en

los últimos 40 años ha llevado a un crecimiento exponencial de la tecnología, así como sus riesgos.

El concepto de Telemática data de mediados de los años 70, cuando los desarrollos de las telecomunicaciones debían de estar plenamente relacionados con el desarrollo de los ordenadores y como origen del término está el francés Télématique. La Telemática no solo se centra es desarrollar temas de transmisión de datos entre equipos, va más allá y se mete de lleno en la calidad de la comunicación entre ellos, desarrollando y afianzando planes y estrategias como finalidades de la Telemática en sí. Algunas de esas finalidades son las siguientes:

- La aplicación de las tecnologías informáticas para la creación y desarrollo de diferentes proyectos cuya finalidad es la de producir infraestructuras confiables y eficientes de las telecomunicaciones.

- Creación y desarrollo de nuevas tecnologías que den base para los futuros desarrolladores y que les permitan entregar equipos y comunicaciones confiables.

- Gestionar el desarrollo e implementación de nuevas redes indiferentemente de su cobertura, con la ayuda de acciones planificadas mediante mecanismos y administrar las nuevas tecnologías.

- Un desarrollo eficaz, confiable y de alta seguridad de las telecomunicaciones establecidas gracias al desarrollo de nuevas herramientas para los sistemas y servicios referentes al área de redes.

- Entregar protocolos y certificaciones que definan y clasifiquen la calidad de servicio para los variados medios de telecomunicaciones.

- Entregar normativas necesarias que den acceso a la homologación y dar claridad a los criterios establecidos para las telecomunicaciones, en el desarrollo de nuevas tecnologías, ya sea en hardware o software y las distintas certificaciones que confirmen un método determinado.

La telemática abarca un campo muy amplio, que incluye el estudio, diseño, gestión y la aplicación de las redes de comunicación y sus servicios destinados al transporte, alojamiento y el procesamiento de la información en cualesquiera que sean sus datos, además de que incluye los planos del usuario, control y gestión.

2.2 REDES DE COMUNICACIÓN

Esta tecnología es la base de todas las comunicaciones tecnológicas que conocemos hoy en día, todo dato que se traslada de un lugar a otro viaja por una red. Como ejemplo simple conocemos las redes celulares, cada proveedor en Costa Rica como los son el ICE, Claro y Telefónica poseen su propia red de comunicación por donde

viaja todo dato, e incluso se conoce de costos extra cuando se enlaza a otra red, porque lleva características especiales que se deben enlazar.

La Red de Datos se puede analizar como la unión de dos palabras, una es Red que es “una estructura que cuenta con un patrón característico, puede hacer referencia a la interconexión de computadoras y otros dispositivos que comparten recursos” (Julián Pérez y María Merino, 2014), y la otra palabra es Datos que es “un término que indica una información, un documento o un testimonio que permite alcanzar un conocimiento o deducir las consecuencias legítimas de un hecho” (Julián Pérez y María Merino, 2014, p.36).

Con base en lo anterior, podemos definir que una red de datos es la infraestructura cuya función es la de trasmitir o de llevar de un lado a otro un intercambio de información. Gracias a la evolución de las telecomunicaciones, existen muchas redes que han sido diseñadas para diversos objetivos específicos.

Bajo el concepto simple anterior, así es como se hablan los datos en la red de la empresa, que puede ser tan granular como el administrador de la red desea, incluso de crear pequeñas subredes por departamentos u oficinas, todo depende de la necesidad. Sin embargo, para los temas propios de este proyecto, hablaremos de la red de datos de la organización en su sede de Escazú, por la cual viajará todo dato ya sea de correo electrónico, archivos compartidos, llamadas telefónicas, conversaciones por Skype y

así todo dato que salga de la computadora del usuario y necesite trasladarse ya sea al compañero de al lado o sea a la sede de la India.

Esta red permitirá la comunicación entre el usuario y el resto del mundo, gracias a una serie de dispositivos diseñados para este fin, ya sea para transmitir, almacenar o proteger los datos.

2.2.1 CONCEPTO DE INFORMACIÓN

La información, para el tema en cuestión que es la informática, no es más que un conjunto de datos organizados y procesados que le será útil solamente a quien comprenda de qué trata.

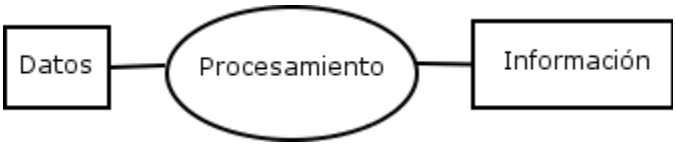


Figura 4: Flujo de la información

Fuente: Web de Datosuno

A través de la historia, el humano ha tenido la necesidad de crear y evolucionar la información para que sea cada vez más eficiente, obviamente una llamada por medio de internet utilizando video va a ser más eficiente que las señales de humo de antaño, este pequeño ejemplo es lo que define en sí uno de los pilares de la informática, que en su evolución ha desarrollado equipos y tecnologías que “permite la comunicación entre

procesos…, un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red" (Lizbeth Martínez, 2013).

2.2.2 MODELOS DE REDES

El concepto de red es algo muy simple de comprender, de forma básica es un grupo de dispositivos, entre ellos computadoras, tabletas, teléfonos, relojes, etc., conectados entre sí para enviar y recibir información por medio de impulsos eléctricos en el caso de que los datos viajen por cable o por ondas electromagnéticas en caso de que sea por señal inalámbrica, o cualquier otro medio con el único fin de trasladar los datos entre ellos. La utilidad en sí misma es la de compartir los recursos e información a distancia, ya sea al escritorio de al lado o a otro continente, pero procurando la seguridad de los datos. Además que siempre esté disponible, y que cada vez su desarrollo sea para aumentar la velocidad disminuyendo su costo.

Para los efectos prácticos de este proyecto analizaremos los modelos de redes clasificados por su alcance, como las redes LAN, MAN y WAM.

2.2.2.1 REDES DE ÁREA LOCAL

Este tipo de redes son las más utilizadas en las empresas, ya que parte de su seguridad es que está limitada a un área física, ya sea una casa, un piso o un edificio, y sirve para conectar los equipos informáticos a los servidores y equipos de

comunicación, ya sea de forma alámbrica o inalámbrica. En la mayoría de los casos se da de forma hibrida, tanto con cable como inalámbricamente.

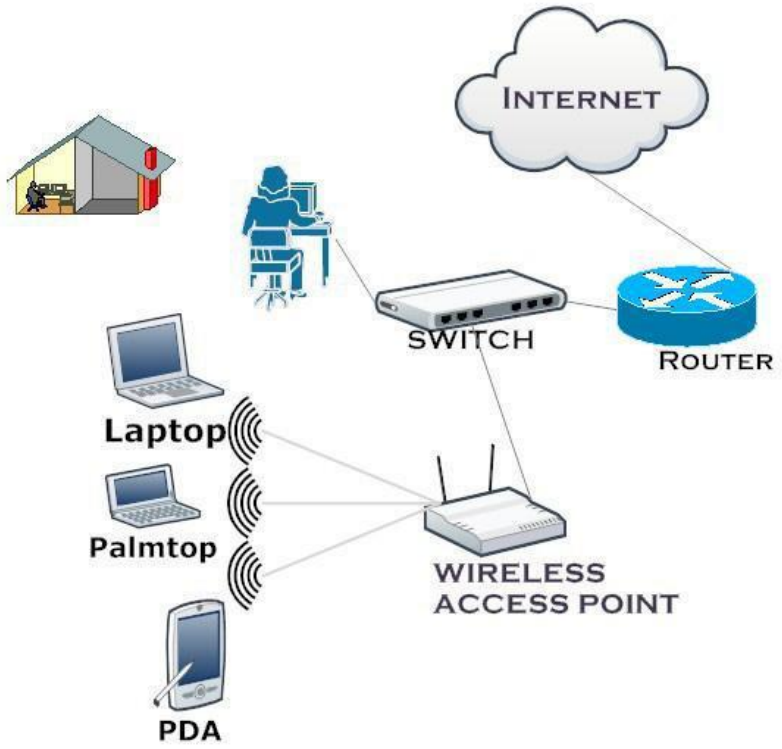


Figura 5: Red LAN en un hogar

Fuente: Computer Networking Demystified

Como se nota en la figura anterior, se trata de un ejemplo práctico que encontramos en los hogares, cuando se conecta un equipo llamado “router” y del cual se hablará más tarde, al proveedor de internet. Este da señal de internet e interconectará a los equipos entre ellos, sea a los dispositivos de la vivienda, incluso hasta a las visitas, esta es una red LAN en uno de sus envergaduras más pequeñas.

La red LAN está formada por su parte física que son los cables / conectores y por su parte inalámbrica que son los dispositivos conectados de forma alámbrica a la red pero que dan de señal inalámbrica donde se conectan los dispositivos. Una de las ventajas de la red alámbrica es la seguridad física, ya que para conectarse a la red hay que estar dentro del edificio y conectado por medio del cable, las redes inalámbricas pierden ese factor y por ello es que se debe introducir seguridad adicional y políticas como cambio de contraseñas, tiempos de conexión y una gran variedad dependiendo de la tecnología utilizada.

2.2.2.2 REDES DE ÁREA METROPOLITANA

Este concepto es casi obsoleto, pero para efectos académicos vale la pena rescatar y analizar su funcionamiento. Este modelo de red lo que hace es conectar dos o más LAN entre sí, y se dan particularmente en zonas geográficamente pequeñas como un barrio o distrito, y por lo general en distancias no mayores a los 7 kilómetros.

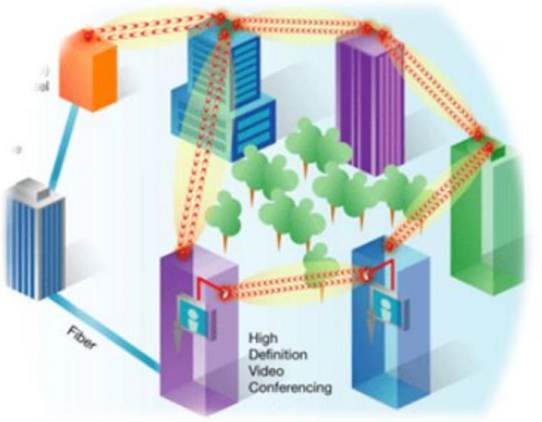


Figura 6*:* Red MAN

Fuente: www.emaze.com

Para nuestros efectos, nuestra sede en Cartago cuenta con una de estas redes, ya que conecta mediante frecuencia inalámbrica dos sectores de la planta, estas separadas por la autopista de un lado y del otro por una calle distrital. Esto nos facilita la gestión de ambos sitios y la integración a la red central.

2.2.2.3 REDES DE ÁREA AMPLIA

Al otro lado de las redes LAN, nos encontramos las redes WAN, que “son redes de comunicaciones que cubren grandes zonas geográficas… sirven para interconectar varias redes LAN, de manera que los dispositivos de una red LAN puedan comunicarse con los de otra red” (Jesus Galindo, 2010). Todo lo anterior aun tomando en cuenta que sus infraestructuras internas sean distintas y no compartan los mismos equipos.

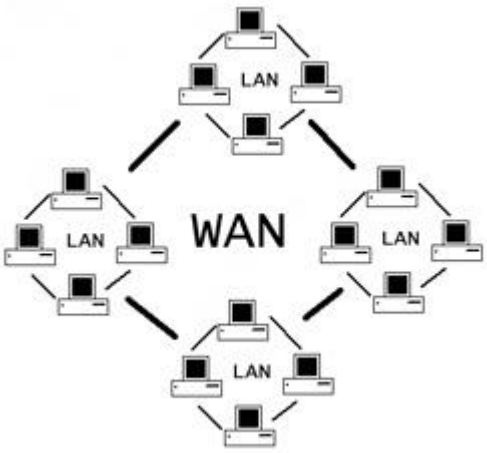


Figura 7*:* Red WAN

Fuente: Web de culturización

Para el efecto práctico de este proyecto, la organización está conectada entre sí gracias a este tipo de redes. En Escazú, Panamá, Salvador, Guatemala, Honduras y República Dominicana existe un equipo que enlaza estas sedes con la sede principal en Cartago, así como un servicio de colocación de servidores en Estados Unidos, permitiendo unir todos estos lugares mediante una gran red con acceso entre sí.

Como ya queda claro, las redes WAN unen las sedes de las organizaciones ubicadas en zonas geográficas distantes, gracias a los avances de la internet. Estas conexiones se pueden hacer mediante su plataforma, aunque existen otras formas de hacerlas, considerando que sus costos se elevan significativamente. Esta es mediante enlaces dedicados, es decir, conectar la sede central ubicada en Cartago, mediante un cable virtual y único directo a la sede de Panamá, se utilizó hace dos años, pero con un costo mensual en esa época de mil doscientos dólares americanos, un pequeño ejemplo de estos costos. Otro ejemplo que cabe recalcar es un servicio que ofrece Microsoft mediante socios mundiales, esto se llama “Express Route” que consiste en un enlace dedicado desde la sede de la organización hasta su Data Center más cercano ubicado al oeste de Estados Unidos. Este servicio tiene un costo cercano a los cinco mil dólares americanos.

2.3 TECNOLOGÍAS DE COMUNICACIÓN

Los avances sociales y tecnológicos en los últimos años han desencadenado un gran impacto en la forma de brindarse la comunicación, sobre todo por la gran cantidad de

información recopilada en los últimos años, logrando un crecimiento exponencial en tendencias tecnológicas hacia todo lo que nos rodea, desde datos para encender luces en el hogar hasta avances a nivel celular en tratamientos clínicos. Las tecnologías de la comunicación están tan presentes en la sociedad actual que en su mayoría pasan inadvertidas antes los usuarios, ya que se encuentran desde el espacio particular hasta en las más grandes multinacionales, inclusive en el espacio.

En la vida cotidiana se cuenta con computadoras, celulares, tabletas; hasta los automóviles ya se están conectado a internet para consumir datos. Esto ha llevado a evolucionar las formas de consumir la información por parte de los usuarios, llevando hasta importantes medios impresos a evolucionar a versiones digitales únicamente, esto es una pequeña muestra de hacia dónde va la tendencia. Pero para poder comprender la forma en que estos datos se trasladan, no tanto a la pantalla del periódico que se ven en la tableta, sino a las formas que esos datos viajaron para poder estar disponibles en la web y ser consumidos, es que a continuación de explicará las tecnologías más usadas en la actualidad.

2.3.1 TECNOLOGÍAS DE ACCESO

Estas son las tecnologías que permiten al usuario poder conectarse a su proveedor de servicio de internet, ya sea por medio cableado o inalámbrico y las cuales se desarrollarán a continuación. Al menos las usadas en la actualidad, que dejan a un lado

las que quedaron rezagadas en el pasado, sobre todo por su poca flexibilidad de trasmitir una gran cantidad de datos en un segundo.

2.3.1.1 ACCESO ALÁMBRICO

Como su nombre lo indica fácilmente, esta es la tecnología que prácticamente ubica al usuario en un sitio fijo, ya que su terminal está cableada hasta su proveedor de internet. Este es el caso de la mayoría de los servicios domésticos de banda ancha, y como tecnologías actuales se pueden describir las siguientes.

2.3.1.1.1 xDSL

Esta tecnología es la que se conoce en Costa Rica como el ADSL que brinda el ICE, ya que conecta al usuario a internet de banda ancha por medio de la línea telefónica tradicional, o mejor dicho por medio de la línea de pares de cobre telefónico. Estas redes, aunque sean muy comunes, están limitadas por un máximo de ancho de banda y distancia de cobertura, por lo que están siendo desplazadas por otras tecnologías que superan esas limitantes.

Esta tecnología es asimétrica, es decir, la velocidad de carga es diferente a la de descarga, siendo esta última por lo general más amplia. Pero a pesar de sus limitantes, es de gran acceso porque utiliza la misma red telefónica instalada desde hace años, sin tener que invertir en una red cableada para tales fines.

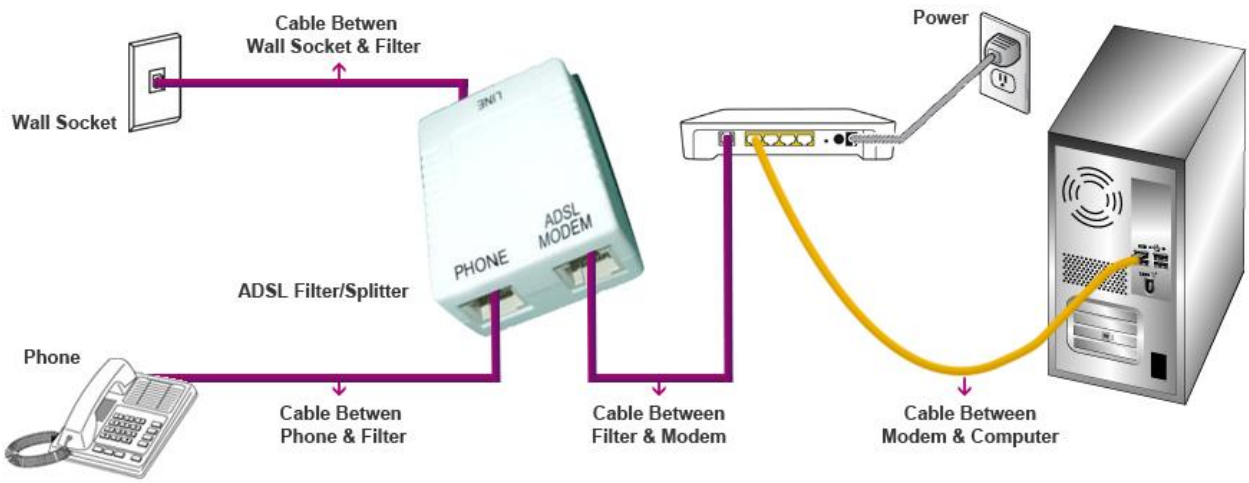


Figura 8*:* Conectividad ADSL

Fuente: Web de test de velocidad

Como se distingue fácilmente en la imagen, la línea del proveedor llega hasta la casa mediante un cable telefónico de 2 pares; de estos un par será utilizado por el teléfono y el otro para la conexión del modem ADSL, de este último conectamos los equipos o un *router wifi* para mejor facilidad de conexión.

2.3.1.1.2 CABLE O HFC

La arquitectura de estas redes de banda ancha es habitualmente Híbrido Fibra Coaxial, esto porque utiliza el cable coaxial en combinación con la fibra óptica dependiendo de sus nodos y distancias. Esta tecnología de redes fue desarrollada en un inicio por los proveedores de televisión por cable, especialmente para su transmisión y proveer a sus abonados, aunque evolucionó hasta la actualidad para entregar banda ancha a sus clientes mediante el dispositivo llamado Cable Módem.

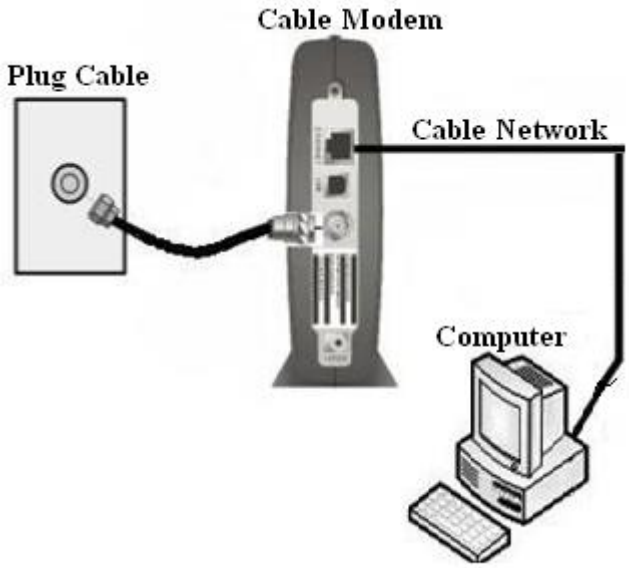


Figura 9*:* Conectividad de Cable Módem

Fuente: Web de oricom

Como bien lo describe la imagen, el servicio entra por cable coaxial al Cable Módem y este entrega internet por una salida de red RJ45, aquí se conecta el equipo o un *Router* para poder entregar a mayor cantidad de dispositivos.

2.3.1.1.3 GPON

Estas siglas significan Red Óptica Pasiva con Capacidad de Gigabit, esta es la tecnología de comunicación más usada en la actualidad cuando se necesita una estabilidad de los datos o existe un alto consumo por parte del usuario. Se ve frecuentemente en las organizaciones, y a nivel de Costa Rica hay grandes empresas

que están llevando fibra óptica a los hogares, a un precio más elevado claro está ya que permite una conexión de Punto a Multipunto, pero sin ser tan exorbitante como unos años atrás.

La tecnología de transmisión por fibra óptica nace como una necesidad al requerir potenciar las redes de cobre, es capaz de brindar una mayor velocidad de transmisión y recepción de datos a través de una sola fibra. Esta gran calidad de servicio permite dar calidad en los servicios de Voz + Video + Datos, ya que tienen una velocidad de 2,4Gbps en una distancia física máxima de 20 km, cifrando su contenido.

Estas redes permiten mayores anchos de banda, menores distancias hasta el abonado, mayor resistencia a interferencias externas, menor degradación en los servicios y un control más proactivo por parte de las empresas, entre otras ventajas, así como la reducción de repetidoras y otros dispositivos, menor consumo eléctrico, menor espacio, menos puntos de fallo, que implican menor inversión por parte del proveedor. Se utiliza una nomenclatura para denotar hacia dónde va la fibra y esta es FTTH cuando va a una casa o negocio. FTTB es la fibra que termina en un punto cercano al abonado y FTTN termina mucho antes, lo que implica que del proveedor sale una fibra al FTTN, de ahí al FTTB y termina en el FTTH, para verlo de una forma más clara la forma de interconexión.

En el caso puntual de la organización, el tema de la redundancia de los enlaces es de vital importancia, por eso en Escazú se cuenta con 2 proveedores distintos que

llegan al edificio con Fibra Óptica por rutas distintas. En el caso de Escazú, que existe una limitante geográfica y de proveedor local, se cuenta con un enlace Inalámbrico, donde el extremo del proveedor se enlaza a su Fibra Óptica y de ahí continúa su trayecto.

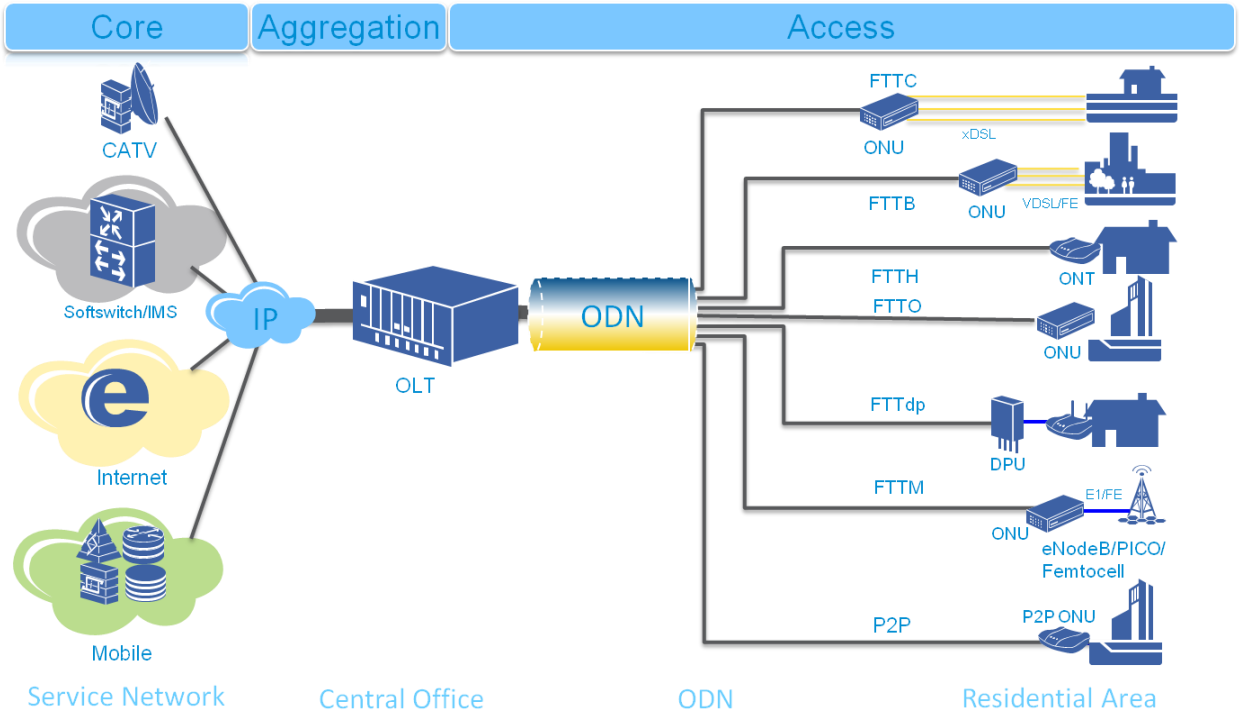


Figura 10: Arquitectura de GPON

Fuente: Web de ZTE Enterprise

Como se nota en la imagen, los servicios se concentran en el OLT y este mediante fibra óptica lo comunica dependiendo del servicio y su fuente.

2.3.1.2 ACCESO INALÁMBRICO

Como acceso inalámbrico describimos a todos aquellos accesos que no necesitan una conexión física por cable hasta el dispositivo del usuario, ya que la comunicación que se enlaza es de manera inalámbrica a través de ondas electromagnéticas, sin embargo, se requiere que el usuario esté dentro del rango de distancia del punto emisor de la señal. Este tipo de tecnología por lo general es una extensión de los enlaces cableados, que logra reemplazar la forma de acceso en el último tramo. Aunque se entregue cierta movilidad, siempre estará sujeto a una cobertura establecida y a un ancho de banda establecido previo contrato con el proveedor.

2.3.1.2.1 Wi-Fi

Esta tecnología permite utilizar ondas electromagnéticas para que los equipos conectados se comuniquen entre ellos. Gracias a su facilidad y flexibilidad de instalación y funcionamiento, ha logrado convertirse en una de las tecnologías inalámbricas más usadas, sobre todo en los hogares y oficinas, sin embargo, no logra superar la estabilidad que la red cableada brinda.

“Estas ofrecen ventajas, tales como una rápida instalación, movilidad, menor coste de mantenimiento y mayor accesibilidad” (Brenda Taveras, 2013). Logra poder entregar una red estable en ámbitos donde se necesite rápidamente o temporal sin incrementar los costos.

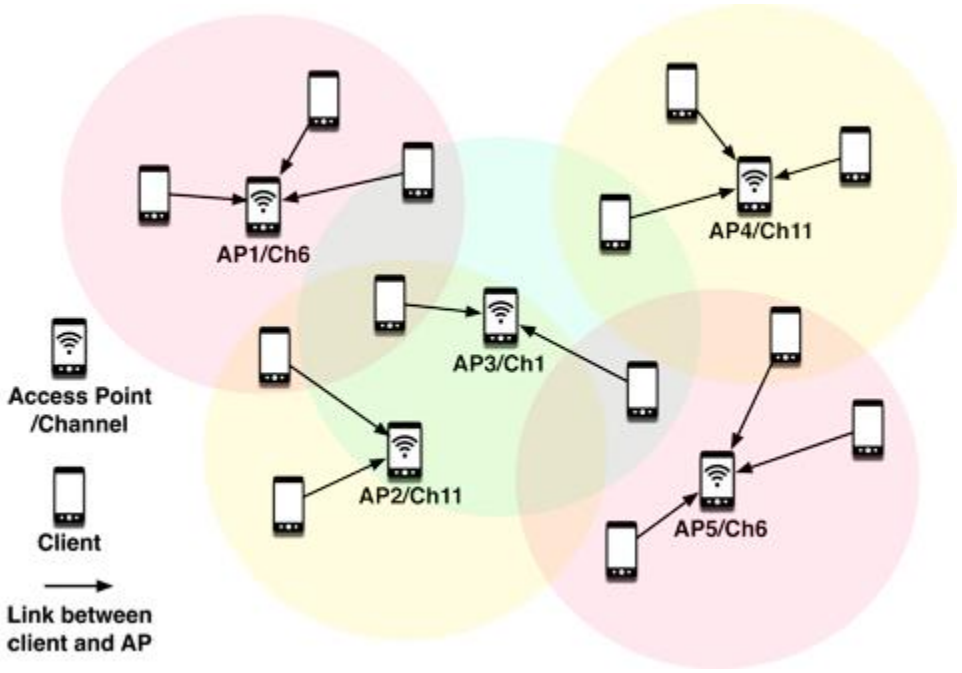


Figura 11*:* Zonas de WiFi

Fuente: Web del MIT

Como se logra observar en la imagen, los diferentes puntos de acceso inalámbricos o Wifi, deben cubrir un área y colocarse de forma que se permita interconectar los dispositivos. Cuando estas redes se dan de esta forma, una buena práctica es la de cambiar los canales de frecuencia o utilizar dispositivos como Wireless Controler que automatizan estos canales para un mejor rendimiento de la red inalámbrica.

2.3.1.2.2 WiMAX

Al igual que la tecnología WiFi anterior, la red WiMAX permite la conectividad inalámbrica entre los dispositivos, con la diferencia de que esta permite una mayor cobertura y una mejora calidad de los servicios alcanzando distancias de hasta 50Km cuando la ubicación es fija y cerca de los 15Km cuando el dispositivo es móvil. Esta tecnología es utilizada por operadores para proveer internet a sus abonados, en Costa Rica el mayor usuario fue Racsa, aunque pequeñas empresas privadas también lo comercializan como lo es MetroWireless o Japi, entre otros.

Figura 12: Como trabaja WiMAX

Fuente: Web de Rubén Javier

Como rangos generales, estas redes funcionan como la red celular, con antenas estratégicamente colocadas que brindan de la señal y al usuario se le coloca una antena receptora, llega a un dispositivo y este entre un conector de red RJ45, de ahí en adelante una red de hogar normal.

Aunque las tarifas sean un poco más costosas, “las redes WiMAX permiten que internet llegue a lugares donde el ADSL o la fibra no alcanzan como, por ejemplo, zonas rurales o de difícil acceso” (José Gallego, 2015). Esta flexibilidad la hace incluso necesaria dependiendo de la zona o como línea de respaldo dependiendo del negocio o requerimiento.

2.3.1.2.3 SATELITAL

Esta tecnología da un paso adelante del WiMAX, funciona prácticamente de la misma manera, pero esta tiene una cobertura casi universal, ambas deben tener una línea de visión directa al emisor, pero en caso de la tecnología Satelital, no está limitado a características geográficas, solo necesita tener visión al cielo. “La experiencia con el servicio de internet satelital ha sido buena, eficiente y muy bien aprovechada” (José Bugueiro, 2009), aunque se tiene conocimiento de que hay factores climáticos que pueden afectar su calidad, sobre todo con tormentas eléctricas, que crea una enorme cantidad de estática entre el satélite y la antena del usuario.

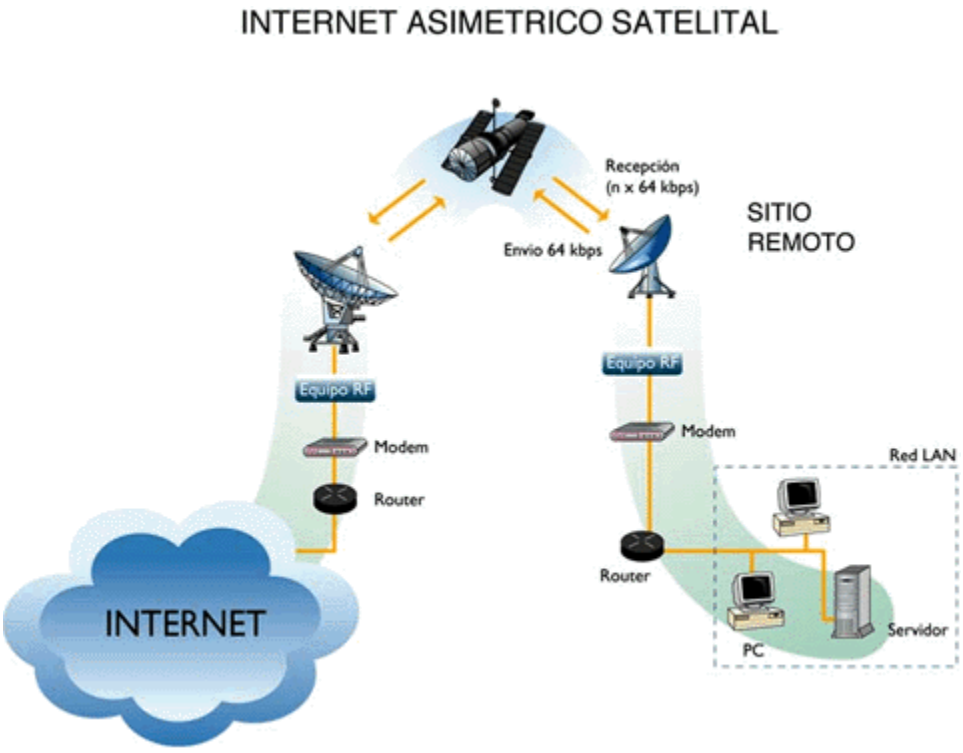


Figura 13*:* Diagrama de Internet Satelital

Fuente: Tuxcom Internet

Como se distingue en la imagen, el satélite cumple la función de conductor de la información entre las dos antenas; como se explicó antes, es por esto que los temas climáticos extremos pueden afectar la señal y degradar el servicio. Obviando esto, es una red de gran flexibilidad, aunque son costos si son elevados.

2.3.2 TECNOLOGÍAS DE TRANSPORTE (DWDM, SDH, PDH)

2.3.2.1 PDH

Jerarquía Digital Plesiócrona: Esta tecnología le da definición a varios sistemas de transmisión que utilizan dos pares de cables y un método de multicanalización por división de tiempo, para crear múltiples canales de datos y voz digital. La palabra Plesiócrona da a entender dos relojes muy cercanos, pero no exactamente el mismo.

Los estándares del PHD son los siguientes:

- T1: Es el estándar norteamericano y consiste en 24 canales de 64 Kbps para un total de capacidad de 1.544Mbps.
- E1: Es el estándar europeo y consiste en 30 canales de 64Kbps y 2 canales reservados para sincronía y señalización para un total de capacidad de 2.048Mbps.
- J1: Es el estándar japonés, es similar al norteamericano en canales y velocidad, su diferencia radica en la forma de obtenerla, ya que esta incluye longitudes de la señal para voz y datos.

Estos estándares tienen la dificultad que no son compatibles entre sí, y con la limitante de no existir un estándar mundial, las interconexiones entre ellas son imposibles, aunque todas las tecnologías utilicen los 64 Kbps en sus canales.

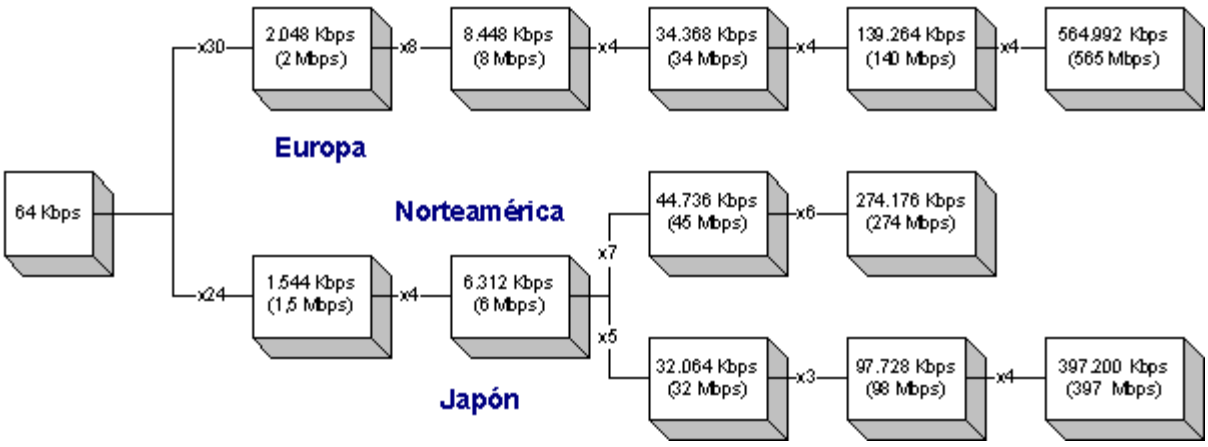


Figura 14*:* Trasmisión PDH

Fuente: Web de Ramón Millan

Como se observa en la imagen, se deben invertir en varios nodos para alcanzar una velocidad idónea según su estándar, “La red de PDH es plesiócrona (casi síncrona), es decir, no todas las señales multiplexadas proceden de equipos que transmiten a la misma velocidad debido a variaciones en los tiempos de propagación” (Ramón Millán, 2001). Este problema elevaba el costo de implementación por que se debían incluir costos equipos que solventaran en parte esos problemas, adicional a la entrada de la fibra óptica que llegó a sustituir el cable coaxial.

2.3.2.2 SDH

Jerarquía Digital Sincrónica: Esta tecnología es un estándar internacional de comunicaciones en redes en alta capacidad de transmisión, nació como un esfuerzo inicial para estandarizar las comunicaciones de voz y minimizar el impacto negativo de las incompatibilidades de PHD.

Estas redes permiten transportar muchos tipos de datos como voz, video, multimedia y paquetes como los que genera IP, además de que gestiona eficientemente el ancho de banda al mismo tiempo que transmite. Adicionalmente detecta fallas y se recupera trasparentemente de fallas en la transmisión hacia las capas superiores.

Figura 15*:* SDH

Fuente: Web de Geovanni Castro Osorio, 2013

Como se observa en la imagen, existe un flujo de todos los diferentes datos en forma sincrónica por medio de la fibra óptica gracias a su reloj, utilizando el modelo OSI. Esta tecnología es vista como un protocolo de nivel 1, que actúa como portador físico de las aplicaciones del nivel 2 al 4, “como la revolución de los sistemas de transmisión, como consecuencia de la utilización de la fibra óptica como medio de transmisión, así como de la necesidad de sistemas más flexibles y que soporten anchos de banda elevados” (Geovanni Castro, 2013, p.34).

En forma de resumen, las comunicaciones por medio de SDH se pueden entender como tuberías que transportan los datos, y esta la gestiona eficientemente a su vez de contar con sistemas de protección.

2.3.2.3 DWDM

Esta es la más reciente tecnología en aparecer y tiene como característica una alta capacidad de transmisión, ya que utiliza varias fuentes de luz que viajan a diferente frecuencia de onda por una misma fibra óptica. Estas señales son separadas entre sí hacia varios detectores al otro extremo, así logra poder obtener, actualmente, una máxima capacidad de transmisión de 1,6 Tb, que corresponden a 160 diferentes señales de 10Gbps cada una, como bien se observa en la siguiente figura.

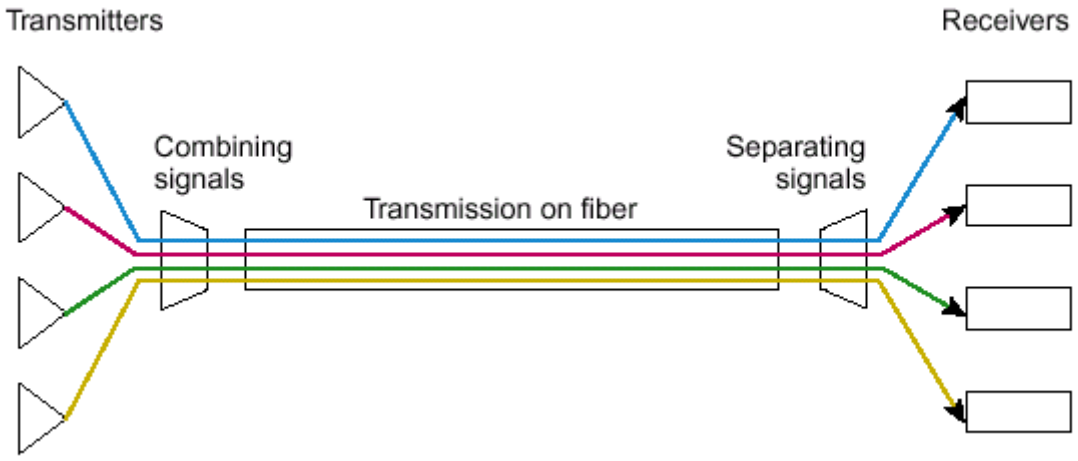


Figura 16*:* Trasmisión DWDM

Fuente: Web de Cable and Wireless

> A finales de los 90, los sistemas densos (DWDM) llegaron a ser una realidad cuando gran número de servicios y multitud de longitudes de onda comenzaron a coexistir en la misma fibra, llegando a enviar 32/40/64/80/96 longitudes de onda a 2,5 Gbps y 10Gb/s. Aun así, pronto veremos los sistemas ultra-densos (UDWDM) con transmisión de 128 y 256 longitudes de onda a 10Gbps y 40 Gbps por canal, ya que la infraestructura actual de fibra óptica no será suficiente para cubrir la demanda. (Jardon, párrafo 5).

2.4 REDES DE TRABAJO

2.4.1 MODELO OSI

Este modelo fue desarrollado en 1984 por la Organización Internacional de Estandarización y el cual fue definido para describir el uso de los datos entre el primer nivel que es la parte física de los datos en la red y el último nivel que es el aplicativo del usuario. Este modelo OSI es un modelo de referencia y no se puede ver como una arquitectura de red, es la forma de acomodar los diferentes componentes del sistema computacional en nivel para un mejor entendimiento, como se demuestra en la siguiente figura.

Figura 17*:* Modelo OSI

Fuente: Web de Microsoft Support

Ya definido el modelo OSI, se puede clarificar para los efectos de este proyecto que un enrutador trabaja en la Capa 2 y el Conmutador en la capa 3 del modelo, y así poder ejemplificar su correcta posición en el esquema de red. Pero para lograr la conexión de los equipos, están los dispositivos que entran en la cuarta capa del modelo, la Capa de Transporte.

Para poder entender más fácilmente, a continuación de menciona el uso de cada capa:

- Capa 7, Aplicación: Encargada de traducir los datos que recibe de la aplicación del usuario.
- Capa 6, Presentación: Realiza tareas e Comprensión, Descomprensión y encriptación de los datos.
- Capa 5, Sesión: Gestiona la comunicación entre los equipos, sincronizándolos.
- Capa 4, Transporte: Vigila, controla y gestiona la transmisión de los datos.
- Capa 3, Red: Gestionan el direccionamiento y ruta de los datos.
- Capa 2, Enlace: Gestionan la fiabilidad, disponibilidad y calidad de la transmisión y líneas.
- Capa 1, Física: Traduce la información a señales para la transmisión o recepción, dependiendo del medio físico por el cual se va a realizar.

2.4.2 ETHERNET

Es el estándar por excelencia de las redes LAN, usa el método de transmisión CSMA/CD, acceso múltiple con detección de portadora y detección de colisiones. Esto significa que antes de que se envíe un dato a través de una red, primero escucha y se da cuenta si algún otro nodo está enviando datos, de no escuchar nada, se envía los datos, caso contrario los retienen hasta que la otra comunicación concluya.

Cada paquete de datos contiene la dirección del destino, la de envío y una secuencia que represente el mensaje transmitido. Cada estación recibe el paquete,

pero ignora los que son dirigidos a otros dispositivos y únicamente procede con los que son dirigidos a ella misma. La velocidad de la comunicación varía dependiendo de la tecnología estándar, en la redes viejas son de 10 Mbps, en las actuales estándar de 100 Mbps y las más modernas de 1Gbps, todas compatibles entre sí, con el detalle de que la comunicación será a la velocidad del nodo más bajo.

Las redes Ethernet cuentan con un direccionamiento de 48 bits, lo que implica que, a cada dispositivo conectado a la red, se le asignará un único número de 48 bits conocido como Dirección IP. En forma de resumen, “es un estándar de redes de computadoras para conectar dos o más computadoras locales, en una proximidad física con el que se podrá intercambiar información entre computadoras y manejar completamente una computadora desde la otra” (Laura de la Cruz, 2012, p. 82).

2.4.3 PROTOCOLO TCP/IP

Este protocolo establece el formato que deben tener los paquetes y el modo de utilizarlos durante el envío y la recepción, este formato se le define como Datagrama IP y están formados por un encabezado que incluye las direcciones IP del receptor y emisor y una sección de datos. Estos protocolos como características principales tiene que son Abiertos y gratuitos, están pensados para interconectar diferentes dispositivos y proporcionan un esquema de direccionamiento común que permite localizar cualquier dispositivo dentro de la red.

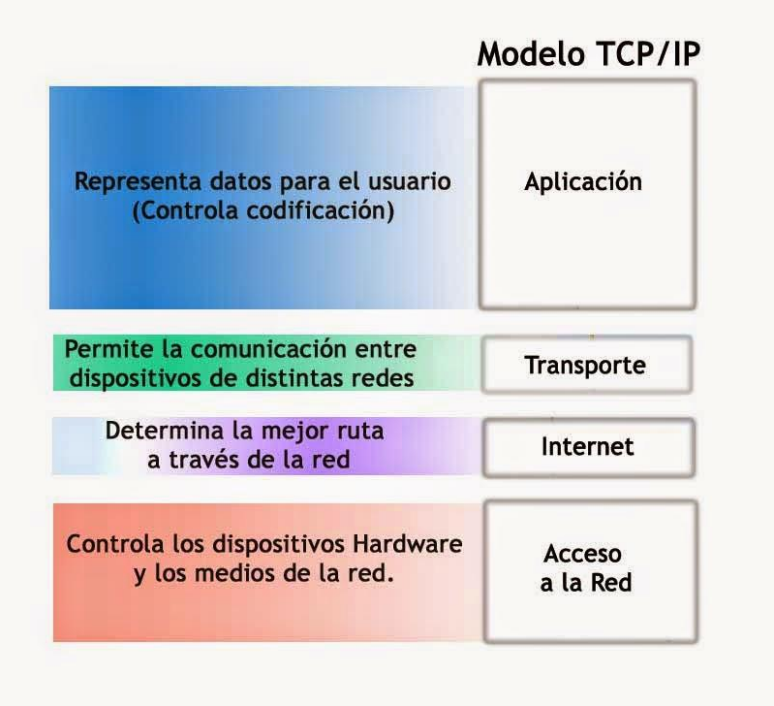


Figura 18: Capas de la arquitectura TCP / IP

Fuente: Redes Locales

Como se detalla en la figura anterior, se logra identificar las cuatro capas de este modelo y sus funciones para una comunicación efectiva, pero para lograr esta comunicación, los dispositivos deben estar dentro de una misma red, por lo cual, la Dirección IP identifica tanto a la red a la que pertenece el dispositivo como a este mismo dentro de la misma red. Una forma práctica de identificar estas redes es separándolas por tipos:

- Clase A: 1.0.0.0 a la 127.0.0.0
- Clase B: 128.0.0.0 a la 191.255.0.0
- Clase C: 192.0.0.0 a la 223.255.255.0

2.4.4 PROTOCOLOS DE ENRUTAMIENTO

“Los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router cuando se comunica con otros routers con el fin de compartir información de enrutamiento. Dicha información se usa para construir y mantener las tablas de enrutamiento” (John Bonilla, 2011, p. 113). Estos protocolos permiten a las redes adaptarse fácilmente a los cambios, de forma que, si un router falla o se incluye uno nuevo a la red, se crean nuevas rutas hacia las redes de destino; dicho de una forma más sencilla, es buscar el camino más rápido para establecer el flujo de datos entre A y B. Para esto existen tres categorías de algoritmos de enrutamiento que continuación se detallan:

Vector distancia: Se comparten las tablas de enrutamiento cada cierto tiempo entre los diferentes routers, informando los cambios realizados en la topología interna de la red, dentro de esta categoría encontramos los protocolos: RIP (Protocolo de Información de Enrutamiento) y IGRP (Protocolo de Enrutamiento de Gateway Interior).

Estado del Enlace: Cada router diseña un árbol con todas las posibilidades de rutas al resto de los diferentes destinos y de ahí calcula sus tablas de enrutamiento, por ello, se necesitan routers con mayor capacidad de memoria y procesamiento. El paquete que envían aquí los routers, contiene la información acerca de la modificación de la topología. Aquí se encuentra el protocolo OSPF (Primero la Ruta Libre más Cerca).

Híbrido: Aquí se combinan los dos algoritmos anteriores, calcula la ruta según la distancia, pero solo envía notificaciones en caso de existir modificaciones en la topología, logrando utilizar menos ancho de banda y recursos. Aquí se encuentra el protocolo EIGRP (Protocolo de Enrutamiento de Gateway interior mejorado).

2.4.5 VPN

Un VPN es una Red Privada Virtual, y con ella se logra crear un túnel privado entre un dispositivo fuera de la red hacia el interno de la misma utilizando el internet como vía de comunicación y un Firewall o dispositivos para VPNs para poder establecer la comunicación, como así se detalla en la siguiente figura:

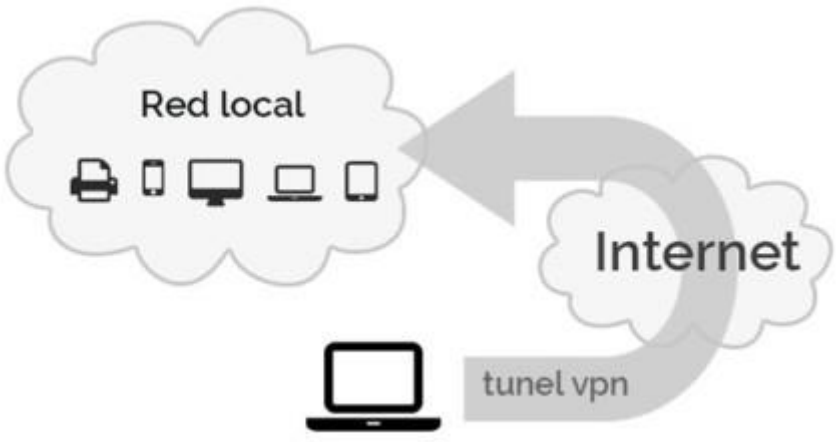


Figura 19*:* VPN

Fuente: Iván Ramirez, Xataca.

Estas redes tienen una gran importancia para las organizaciones corporativas, ya que permiten por ejemplo gestionar el teletrabajo, logrando que un colaborador desde su casa se logre conectar mediante VPN a la red del trabajo, dato de mucha importancia para este proyecto.

2.4.6 VLAN

Para crear estas redes se necesitan conmutadores que lo permitan, y lo que se logra es crear redes virtuales dentro de una misma red física o dominio, para agrupar por departamento, zona o funciones diferentes grupos de equipos y así lograr un mayor control y distribución de la red, así como la segmentación de las IP.

En sí, una VLAN es una red de área local, pero virtual, esto mejora el control y distribución de los colaboradores, a su vez que brinda seguridad, ya que cada VLAN puede ser configurada para diversas funcionalidades y el acceso de una a otra puede ser restringido, para los efectos de este proyecto. Actualmente se cuenta en la sede de Escazú con una VLAN para toda la sede, la idea preliminar es asignar una VLAN a cada piso, esto para controlar quién se traslada entre pisos y temas de seguridad, aprovechando que la red de telefonía se reemplazó por una tecnología que comparte la red de datos.

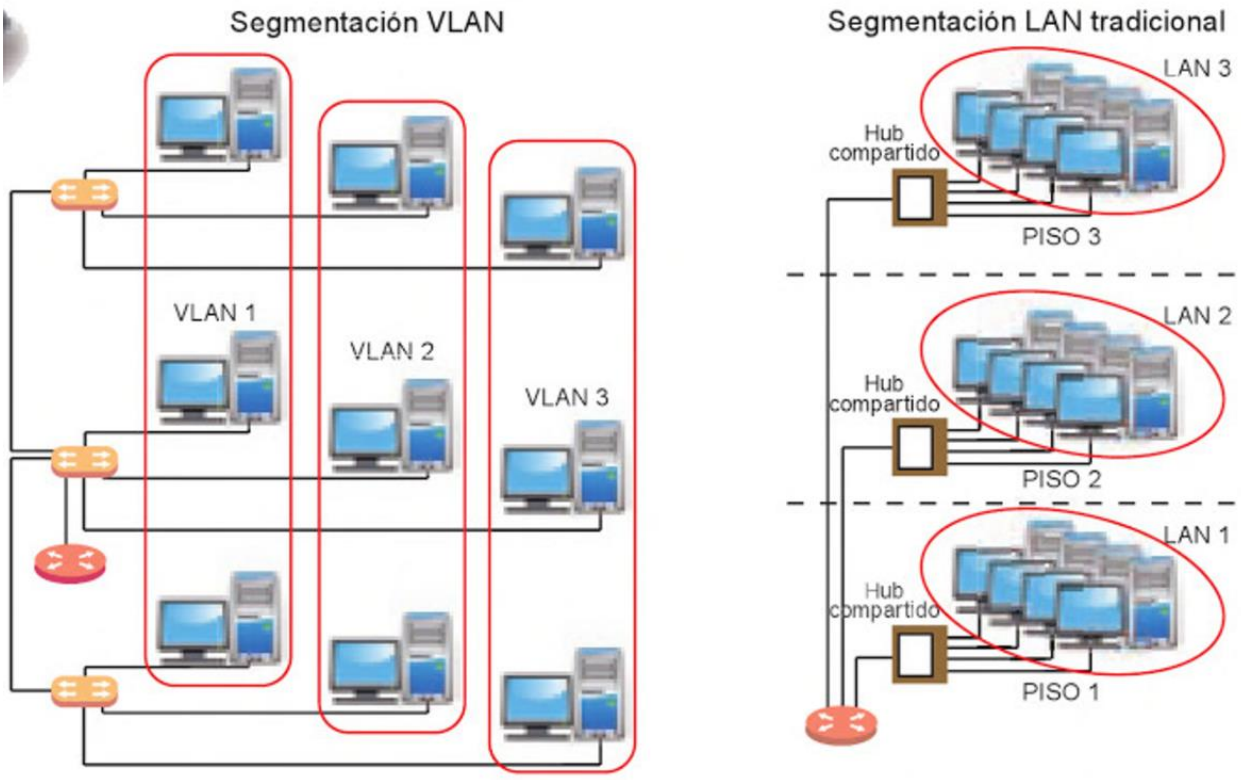


Figura 20*:* VLAN vs LAN Tradicional

Fuente: Redes Locales, Paraninfo.

En la imagen se logra evidenciar claramente el orden que da la implementación de las VLAN en la red de una organización de un tamaño considerable, a su vez de lograr optimizar los recursos y lograr mayor estabilidad.

2.4.7 DHCP

El Protocolo de Configuración Dinámica de Hosts es un servicio que para los efectos del proyecto se encuentra configurado como Rol en un servidor de Windows y es el que se encarga de brindar una Dirección IP (tema antes desarrollado) a cada dispositivo

que se conecte a la red, ya sea de manera alámbrica, inalámbrica o por VPN, de forma dinámica. Lo anterior implica que cada vez que se conecte, recibirá un IP diferente, al menos frecuentemente.

Dentro de este servicio de DHCP, se deben configurar las VLAN que fueron creadas en el equipo conmutador, con el fin de indicarle al servicio que solo debe trabajar con esas subredes y a su vez, en este servicio es donde se configura temas como cantidad de direcciones por repartir y cuáles son direcciones reservadas.

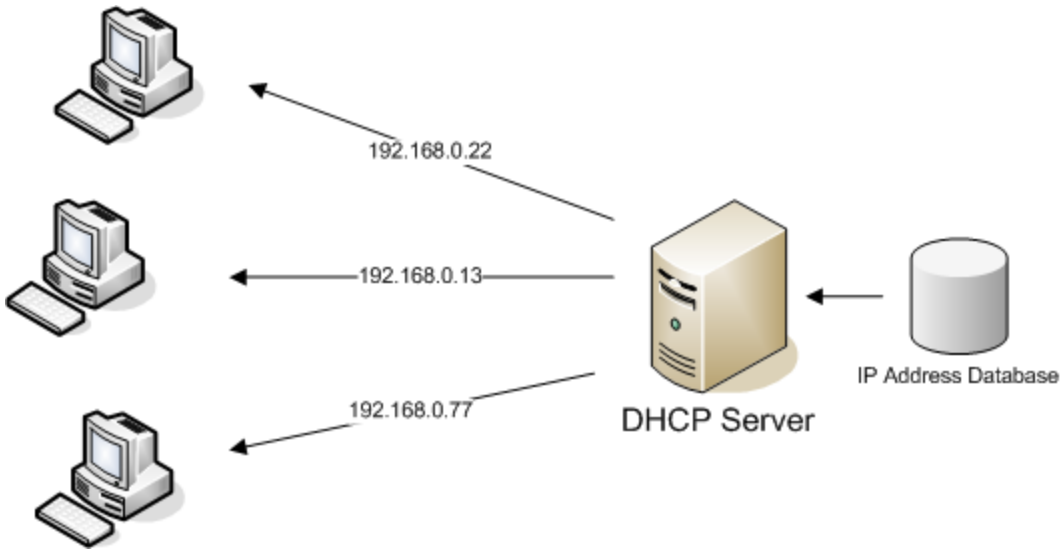


Figura 21*:* DHCP Server

Fuente: Microsoft Support

Como se detalla en la imagen, las IP se crean en el conmutador por medio de VLAN, están direcciones se configuran en el Rol del servidor y este es el que se encarga de repartirlas dependiendo de VLAN y equipos. “El funcionamiento del protocolo DHCP se basa en el envío e diferentes tipos de mensajes. En el caso que el

cliente no disponga de una dirección IP y quiera conseguirla, debe ejecutarse el denominado ciclo básico DHCP” (Maria del Carmen Romero, 2010).

2.5 EQUIPOS DE REDES

2.5.1 SWITCHES y ROUTERS

Como punto medular de una red de datos, se cuenta con los dispositivos que se colocan en la cabeza de la comunicación y sin estos no se puede llevar a cabo las conexiones necesarias y configuraciones para el correcto flujos de datos. Estos equipos se llaman “switch o conmutador y está presente en el conjunto de las redes actuales, principalmente lo encontramos en una topología tipo estrella” (Carlos Vialfa, 2013). Son como la que se presentan en la red de SteinCorp y en todas sus filiales, donde existe un enrutador principal en la sede principal de Cartago y en cada filial existe un conmutador secundario que comunica ambos sitios.

Estos equipos primarios son similares pero su función varía, y es a los que llamamos enrutadores; “son dispositivos para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos” (Oscar Hernández, 2012). Estos equipos trabajan en la capa 3 del modelo OSI.

En la actualidad los conmutadores pueden trabajar en la capa 2 y 3 del modelo OSI, logrando tener la funcionalidad de un Switch y de un Router, con esto se logra poder usarlos en cualquier parte de la red.

La función de un Switch es segmentar la red y así poder seccionar el tráfico entre los diferentes segmentos. Para efectos de este proyecto se trabajará con estos dispositivos, ya que los Routers se encuentran instalados en la sede de Cartago.

Figura 22*:* Switch HP 1920, 48 puertos, PoE

Fuente: Web de HP

Esta imagen representa los modelos utilizados en Cartago para la conexión de las diferentes áreas. Equipos iguales a este o superiores serán los utilizados en este proyecto.

2.5.2 FIREWALL

“Una aplicación adicional a los routers es actuar como pasarela de seguridad (Firewall o cortafuegos) entre la red del cliente y otra red exterior, como podría ser internet, creando una frontera entre ambas” (Antonia Salsosa, 2006). Esta definición a la fecha se encuentra intacta y determina en sí la esencia de un Firewall.

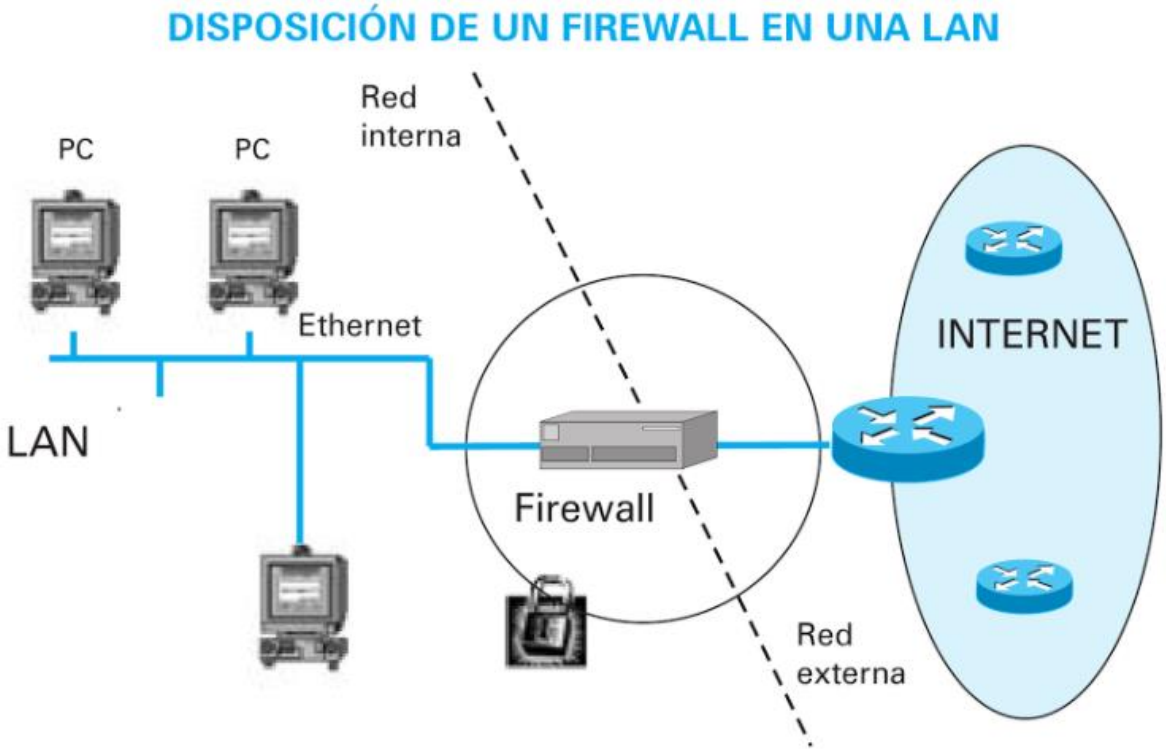


Figura 23*:* Ubicación del Firewall

Fuente: Web de Cisco

Como se determina en la imagen anterior, este dispositivo es el que va en medio de la red interna y todo lo externo a la organización, logrando dar mayor control y

gestionar la seguridad del mismo. Para nuestros efectos, la organización cuenta con un UTM (Gestión Unificada de Amenazas) de WatchGuard, el cual cuenta con las siguientes características:

- Intrusion Prevention Service (IPS)
- Reputation Enabled Defense service (RED)
- Webblocker url filtering
- Spamblocker
- Gateway Antivirus (GAV)
- Application Control
- APT Blocker – Advanced Malware Protection
- Data Loss Prevention (DLP)
- Network Discovery
- Dimension Command

2.5.3 ACCESS POINT

Para efectos académicos se detalla que el método de trasporte puede ser por cable o de forma inalámbrica; esta última es parte medular de este proyecto y llevada a cabo por medio de un Punto de Acceso Inalámbrico.

Un punto de acceso es un dispositivo que crea una red de área local inalámbrica (WLAN), normalmente en una oficina o un edificio de grandes dimensiones. Un

punto de acceso se conecta a un router, switch o hub por un cable Ethernet y proyecta una señal Wi-Fi en un área designada. Por ejemplo, si desea habilitar el acceso Wi-Fi en la zona del vestíbulo de su empresa, pero no tiene un router que pueda cubrirla puede instalar un punto de acceso cerca de la recepción y conectarlo con un cable por el techo a la sala del servidor. (Linksys, sitio web, s.f., 2017, párrafo 4).

De esta forma, el usuario se instala en su espacio de trabajo, enciende su computador y accede a la red por medio del punto de acceso inalámbrico, este está conectado al enrutador que lo va a comunicar con el conmutador, este último es que el redirige la información a donde sea necesario. Es así como de una forma muy simple se menciona el funcionamiento de la red.

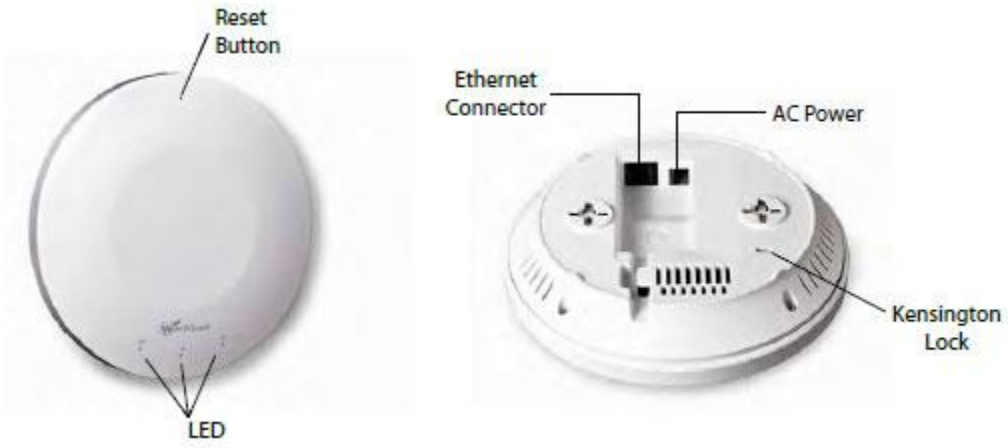


Figura 24*:* WatchGuard AP200

Fuente: Web de WatchGuard

En la red instalada en Cartago se está implementando con estos AP, siendo la referencia mínima de este proyecto para la sede de Escazú.

2.5.4 CABLE UTP

Para lograr la conexión de los equipos dentro de la red es primordial la parte cableada, que para nuestros efectos será con los cables UTP. Estos cables permiten que los datos fluyan de un punto a otro de manera segura y eficaz, están compuestos por ocho cables internos de cobre acomodados en 4 pares, cado uno identificado con un color que ayuda a la hora de instalar el conector en sus extremos. Este conector tiene la identificación de RJ45 y es el estándar mundial, “los hilos están trenzados para reducir las interferencias electromagnéticas con respecto a los pares cercanos que se encuentran a su alrededor” (Andrés Garcia, 2007).

Para que su funcionalidad sea la óptima, el cable no puede tener curvas de menos de 10cm y no puede superar los 100m de extensión. Estas redes por lo general son más confiables a nivel de seguridad que las inalámbricas, ya que para tener acceso a la red hay que conectarse físicamente a ella.

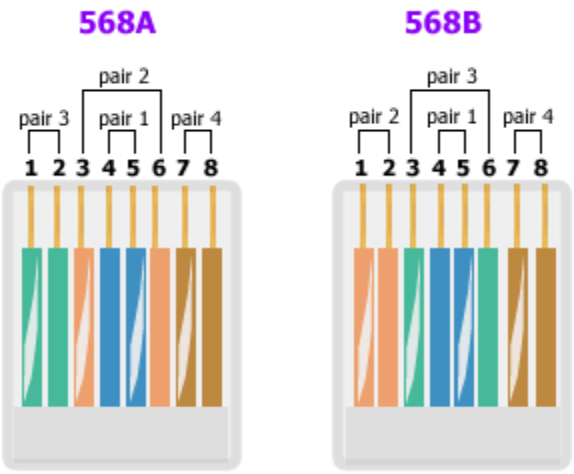


Figura 25*:* Tipos de conexiones UTP

Fuente: Web de Conniq

El estándar utilizado en la organización es el Tipo 568B, este será el del presente proyecto.

2.5.5 FIBRA ÓPTICA

Este documento desarrolló el tema de GPON con anterioridad, este enunciado solo hablará de la fibra óptica como material y sus características. La Fibra Óptica es un medio de transmisión de datos que consiste en un hilo muy fino de material trasparente, vidrio o plástico, o a dónde nos lleve la tecnología. Lo importante es que este material sea capaz de conducir pulsos de luz que representan los datos a transportar mediante tecnología digital binaria de 1 y 0.

La señal se mide por decibeles en kilómetros (dB/Km), con el detalle de que estos cableados son muy susceptibles a las conexiones y empalmes, por lo cual se hacen con equipos especiales para no perder la calidad de la transmisión, ya que esta tecnología se basa en la reflexión interna de la luz.

Elementos que forman la transmisión por fibra óptica:

Transmisor: Debido a que la información debe ser transmitida por luz, el trasmisor será el responsable de convertir la energía electromagnética en luz gracias a un LED o un diodo láser.

Fibra óptica: Es el medio de transmisión, la luz recorrerá el cable, generalmente en zigzag, hasta llegar a un regenerador o receptor.

Regenerador óptico: Para evitar degradación en la señal se utilizará un regenerador óptico que no es más que un láser que aumentará la intensidad de la luz si afectar nada adicional.

Receptor óptico: Este invierte el proceso del transmisor, devolviendo a energía electromagnética la energía luminosa.

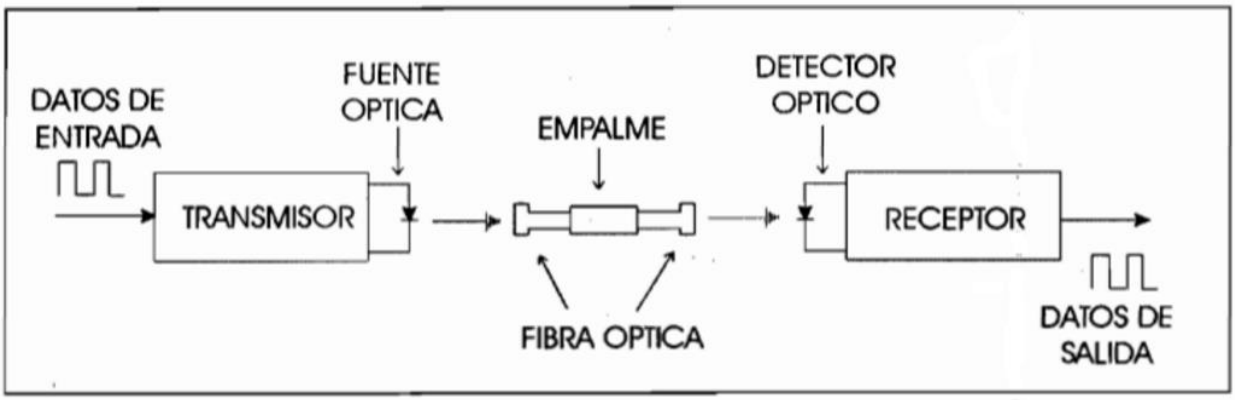


Figura 26*:* Trasmisión de Datos con Fibra Óptica

Fuente: Web de Panda Ancha México

Tipos de fibra Óptica:

Monomodo: Se utilizan cuando la transmisión de datos sea de gran distancia, ya que su núcleo óptico es pequeño, por lo que la luz recorre el cable en un solo un haz, lo que ayuda a que viaje más rápido, más lejos y con menos debilitamiento.

Multimodo: Esta tiene la capacidad de trasmitir múltiples haces de luz gracias a su núcleo de mayor tamaño que ayuda a que la luz se refleje en distintos ángulos.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 TIPO Y ENFOQUE DE LA INVESTIGACIÓN

3.1.1 TIPO DE INVESTIGACIÓN

El tipo de investigación del presente proyecto es la Aplicada, ya se utilizarán los conocimientos en la práctica del proyecto para con ello beneficiar a los miembros de la organización que se ubican en la sede de la organización a efectuar el proyecto.

La finalidad de la presente investigación, al ser Aplicada, es que su objetivo sea la solución al problema de redes que está sufriendo la sede de Escazú de SteinCorp, entregando una propuesta realizable para satisfacer la necesidad con los requerimientos reales y alcanzables.

La dimensión temporal de la propuesta es Transversal, ya que la investigación está centrada en analizar las variables para alcanzar el éxito. Su ventaja es entregar información general entre distintas tecnologías y tomando como referencia la ya implementa en la sede central y homologarla en la sede de Escazú, esto sin dejar nunca de lado el mejorar lo ya implementado y tomando en cuenta, si el presupuesto lo permite, tecnologías más avanzadas o equipos más robustos de los ya implementados y exponerlos como puntos de mejora en relación con lo ya implementado.

En cuanto a la extensión del tema nos referimos a un marco Macro, ya que la necesidad es de una sede completa de la organización e involucra a varios segmentos

de la misma, pero no a toda la organización, pero sin dejar de lado que, desde un punto de vista comparativo, la cantidad de usuarios informáticos de los sistemas en ambas sedes es similar, ya que en Cartago la media es de 130 usuarios recurrentes y en Escazú de 100 usuarios recurrentes.

3.1.2 ENFOQUE DE LA INVESTIGACIÓN

El enfoque de la investigación es Cuantitativo, ya que se puede medir y expresar en valores numéricos, debido a que por su naturaleza se recolectan datos e información sobre los dispositivos y el comportamiento de la red de datos, quejas, computadores, servicios y demás insumos que consumen la infraestructura.

Lo anterior se ve reforzado por la mediación del consumo de los enlaces de internet y el consumo de los datos a nivel telefónico, para mencionar un ejemplo de relevancia al proyecto, ya que, aunque cuente con una minoría de usuarios recurrentes, el consumo de datos de la sede se ve equiparada a la sede central, lo que nos entrega datos tangibles y medibles que solucionar y tomar como base para las mejoras de la presente solución.

Por último, y no menos importante, el carácter de la investigación es el de un Proyecto, ya que tomará el tipo y enfoque de la investigación y lo transformará en un entregable tangible y real según las métricas, para poder avanzar en una sede tan importante y a la vez abandonada tecnológicamente.

3.2 TÉCNICAS Y HERRAMIENTAS

La técnica principal es la homologación de la tecnología de la sede central, será tomar la documentación de cotizaciones y de proyectos de implementación de las fases iniciales gracias al proyecto de construcción de la Planta de Laboratorios Stein y homologar dicha tecnología en la sede de Escazú. Ello se acompaña de la comparación de los enlaces de internet y el consumo de las aplicaciones primarias de la organización.

Adicionalmente se realiza una lista de los equipos y su actualidad por número de serie o modelo, ya que no se tiene información precisa de su adquisición, esto como consecuencia de que el miembro más antiguo del equipo a nivel de infraestructura aun no llega a los cuatro años de trabajar en la organización. De este modo, la comparación de los consumos de ambas sedes, así como la comparación de una tecnología nueva con una obsoleta, será la técnica primordial para establecer el alcance y entregable del presente proyecto.

Las herramientas para la implementación serán tomadas de las mejores prácticas del PMBOK. El proyecto será segregado en etapas, cada una de ellas llevará un control de los tiempos, recursos, proveedores y costos, así como sus informes y entregables semanales con planes de controles.

En la empresa es utilizado el Microsoft Project como mecanismo de seguimiento y control de los proyectos, así como apartados de seguimiento ubicados en el SharePoint de la institución, donde los involucrados reciben notificaciones y dan actualizaciones de las novedades del proyecto. Esto a su vez funciona como norma organizacional.

Dentro de los alcances del proyecto será entregar un demo para su evaluación tangible y su veracidad, todo regido por el modelo de implementación de redes de datos de la organización y que sirve como guía para estas propuestas.

El responsable de brindar la propuesta será en su totalidad Jonathan Cruz, en dado caso quien avalará consultas o situaciones que se produzcan será la Gerente de TI de SteinCorp, la señora Rosana Acuña. Adicionalmente está el Gerente Financiero el señor Mario Gómez, quien recibirá la información final para su evaluación a la espera de su aprobación para la implementación del proyecto al corto o mediano plazo.

Se estima que la propuesta se dé en tres etapas: una de recolección de información, otra de cotizaciones y revisiones de las ofertas, tanto desde un punto de vista técnico como económico y así como revisión de proveedores, y una tercera etapa donde se diseñe la propuesta con los equipos y proveedores que entregó la segunda etapa. Una vez finalizada, la propuesta será entregada al Director Financiero y este tomará una decisión, en ese momento se dará por entregada y será el punto final de

los alcances, la implementación en sí será llevada a cabo en una segunda fase. La limitación de este proyecto queda en ese entregable.

3.3 FUENTES Y SUJETOS DE INFORMACIÓN

3.3.1 FUENTES DE INFORMACIÓN

Antes de entrar en el tema, se debe aclarar que una fuente de información es donde obtenemos la bases y sustento teórico / práctico con el cual se fundamenta una propuesta. Para este proyecto se evalúa todo aquello distinto a personas que valide los resultados del entregable y logramos encontrar las fuentes Primarias y Secundarias.

Esta propuesta de proyecto surge con base en las herramientas para el diseño que se utilizó en la metodología de la fase uno del proyecto de construcción en Cartago, esta evaluó a 3 fabricantes distintos y el departamento escogió la que más le convenía, de allí la fuente primaria. Esta propuesta se anexa a ese estudio y lleva esos requerimientos a la actualización de la red de datos de la sede, esto excluye al ciclo de Deming de la metodología, ya que es darle continuidad y mejora a una implementación ya realizada y que es marcada como punto de partida.

Adicional, la parte de la implementación deberá regirse por las normas propuestas para la homologación de Carbono Neutral del Gobierno de Costa Rica y

será revisado por el departamento responsable para SteinCorp, sobre todo si se deberá de analizar el reciclaje de equipo electrónico.

En busca de propuestas de mejora, es que este proyecto partirá de un inicio ya establecido y con el afán de homologación dará valor de investigación acerca de equipos con mayor rendimiento y opciones de financiamiento, se parte de la metodología de análisis del área de Tecnologías de Información. Esto aplica como caso práctico para definir estas metodologías sobre otras.

Como fuentes secundarias, se tendrá la observación de las principales quejas de los usuarios de la red, a su vez de identificar las necesidades reales de la infraestructura y de cómo los servicios que se trasiegan por la red han crecido exponencialmente. Por ello es que se busca equiparar la necesidad junto a la realidad, dejando un espectro para el crecimiento de la red de datos, esto gracias a la medición del consumo del ancho de banda de los enlaces de internet, el consumo de las aplicaciones de Office 365 y el trasiego de los datos de Voz en las llamadas telefónicas. Lo anterior en comparación a los consumos de las mismas tecnologías en la sede de Cartago y gracias a los informes que se detallan en el Firewall y que entregan los proveedores de internet.

3.3.2 SUJETOS DE INFORMACIÓN

Los sujetos de información son aquellas personas, tanto internas como externas, a quienes se contacta para recolectar información importante para la obtención de datos relevantes del proyecto.

Para una mejor estructura, se utilizará la siguiente tabla:

Tabla 1: Información de los sujetos de la Investigación

Nombre	Organización	Departamento	Puesto	Relación con el proyecto
Rosana Acuña	SteinCorp	TI	Gerente	Apoyo
Ricardo Pacheco	SteinCorp	TI	Soporte Senior	Apoyo
Jerry Meléndez	SteinCorp	TI	Soporte Semi Senior	Apoyo
Jean Carlo Corrales	SteinCorp	TI	Soporte Junior	Apoyo
Randall Martínez	Tecnova	Post Venta	Líder de cuenta	Apoyo
Corwin Ott	Tecnova	Post Venta	Ingeniero	Apoyo
Mario Gómez	SteinCorp	TI	Director de Finanzas	Toma de decisión

3.4 VARIABLES DE LA INVESTIGACIÓN

El propósito del proyecto es la entrega de una propuesta para reemplazar la red de SteinCorp en su sede de Escazú, así lograr una homologación y actualización de la red con referencia a su sede central de Cartago. Este cambio implicaría un mayor procesamiento de los equipos de conmutación de la red y una mejor capacidad de los dispositivos inalámbricos de la red, y da así holgura y mejor experiencia final al usuario.

Debido a lo anterior, el proyecto puede presentar variantes a la hora de avanzar en la propuesta, como variantes en los equipos y por ende en el presupuesto, esta es una limitante ya establecida. Para poder dar una mayor claridad a estas variantes, en la siguiente tabla se detalla lo que puede causar desviaciones en la ejecución:

Tabla 2: Variables del proyecto

Objetivos	Variables	Descripción
Diagnóstico de la red actual	Calidad de los equipos	Este diagnóstico puede darle carácter de urgencia al proyecto o puede aplazar su puesta en marcha
Requerimientos iniciales	Costo de los equipos	Se cuenta con un presupuesto inicial, una variable es que los equipos requeridos excedan el presupuesto establecido
Diseño de la propuesta	Cantidad de equipos	La cantidad de equipos existentes versus los requeridos puede variar de forma positiva o negativa
Plan Piloto	Tecnologías	Puede variar la capacidad de los equipos por temas arquitectónicos o de consumo.

Otros	Capacidad de la red actual	Debido al poco conocimiento del cableado actual de la sede, una variable es invertir en algún trabajo adicional para la implementación

3.5 DISEÑO DE LA INVESTIGACIÓN

Las siguientes fases ayudarán a entender el diseño de la propuesta y a dar un orden más claro a la ejecución del proyecto, así lograr sistematizar los pasos y herramientas a utilizar para lograr el éxito y aprobación en el mediano plazo.

3.5.1 FASE 1: PREPARATORIA

Se documentan todas las tareas necesarias para lograr la implementación antes de ejecutarla. Está formada por tareas críticas como la comunicación a los usuarios de la afectación de los servicios, respaldos, gestiones con los proveedores, preparar los equipos que se implementarán, pruebas de funcionamiento, y comunicar las tareas que se realizarán fuera del horario habitual de oficina.

En esta fase es primordial listar todos los miembros del equipo, sus roles y su información de contacto relevante, así como contacto de escalamiento de cada miembro incluyendo a proveedores.

3.5.2 FASE 2: ANALÍTICA

Se documentarán los equipos existentes para tomar la información y compararla con la propuesta de los proveedores. Así se detallarán los equipos, características físicas y lógicas, y se asignará un proveedor recomendado para la posible implementación, acompañado de una síntesis de su selección, en esta fase se detallará el corazón de la propuesta.

3.5.3 FASE 3: TRABAJO DE CAMPO

El resultado que se espera obtener es un plan de trabajo realizable con sus costos, en un *GANTT* donde se detallen las etapas y las fases, así como todo el plan de implementación en caso de aprobarse, acompañado de toda la documentación recopilada para el proceso de compra y tiempos de importación de los equipos.

Como documentación adicional se entregarán los siguientes planes debidamente definidos:

Plan de Posimplementación: Tiene como finalidad el documentar todas las actividades que minimizarán cualquier impacto negativo que resalte de la implementación y tener la forma de abordar y solucionar este, así como los miembros del equipo dispuestos a trabajar en ello.

Plan de Pruebas: Debe listar y detallar todas las tareas exactas que se deben realizar y los resultados esperados, así como sus dueños ejecutores. Para esto es vital listar los aplicativos en niveles de prioridad para darle importancia a quien la necesita y no basar las pruebas en aplicativos de poco uso o de poco valor operativo, así como tomar usuarios e involucrarlos en esta fase, darles empoderamiento y que ayuden a recopilar información necesaria.

Análisis de Riegos: El equipo debe prevenir errores o situaciones que pueden ocurrir y afectar la ejecución del proyecto y crear tareas para responder ante estas eventualidades, y se incluye dentro del Plan de Implantación. La idea final será listar los riesgos en probabilidades de que ocurran y cuáles serán las acciones para minimizar o anular su impacto.

Plan de Vuelta Atrás: Siempre hay un riesgo que se debe evaluar y documentar en las acciones. El objetivo de este plan es que en caso de que una tarea no fuera exitosa, se regresa a su estado inicial, se valoran las fallas y se retoma en otro momento. Por lo general estas implementaciones se realizan de noche y ante una eventualidad es mejor tener una lista de tareas que realizar y no dejar a la suerte que un miembro del equipo, cansado, tome una mala decisión.

3.5.4 FASE 4: INFORMATIVA

Aquí se desarrollará el **Plan de Comunicación**, dando lugar a la documentación y donde se detallarán los medios de comunicación y la forma de hacerlo de cada tarea, cuando sea necesario. Sirve de mecanismo para darle forma a los comunicados internos y a las reuniones de los equipos involucrados.

CAPÍTULO IV

DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

4.1 DIAGNÓSTICO NORMATIVA Y ESTÁNDARES

4.1.1 NORMATIVA INTERNA SOBRE LA RED DE COMUNICACIONES

Una normativa interna de red u otros elementos a nivel de infraestructura en la organización no existe como tal, ya que el departamento de TI ha trabajado en estabilizar la red con las mejores prácticas y con los mejores equipos costo-beneficio, dejando el tema de documentación para el año 2018. Se considera que la organización está en ejecución para obtener las certificaciones ISO/IEC 17025:2005 e ISO/IEC 27001 para el tercer trimestre del 2017, así TI obtendrá el apalancamiento para fundamentar las inversiones del caso y buscar la documentación y mejores prácticas del mercado, como planes para continuidad de negocios (BCP) y recuperación de desastres (DRP).

Como consecuencia de la falta de una normativa interna como lo anterior mencionado, es que este proyecto toma como base toda la infraestructura implementada en los últimos 2 años y su documentación, la cual se detalla a continuación como base documental de este proyecto y futuros. Se divide la infraestructura en sus tres etapas de renovación de elementos para una mejor comprensión de los trabajos realizados hasta ahora y del porqué las tecnologías a homologar.

Etapa 1, Firewall: En esta oportunidad se evaluaron tecnologías similares a nivel de Cisco, WatchGuard, Fortinet y CheckPoint; quedó Fortinet desestimado desde un inicio por la falta de compromiso por parte del proveedor involucrado.

Cant.	Descripción
	Segmento WAN
4	NGFW ASA 5515-X w/ SW 6GE Data 1GE Mgmt AC 3DES/AES SSD 120G
4	SMBS 8X5XNBD ASA 5515-X with SW
4	ASA 9.1 Software image for ASA 5500-X Series5585-
4	ASA 5500 Series CX Software v9.1
4	AC Power Cord (North America) C13 NEMA 5-15P 2.1m
4	Cisco VPN Client Software (Windows Solaris Linux
4	ASA 5500 Strong Encryption License (3DES/AES)
4	ASA 5500 AnyConnect Client + Cisco Security
4	ASA 5512-X through 5555-X 120GB MLC SED SSD
4	ASA 5515 IPS Part Number with which PCB Serial is
4	ASA 5515-X CX AVC and Web Security Essentials
4	AnyConnect Essentials VPN License - ASA 5515-X
4	AnyConnect Mobile - ASA 5515-X (req. Essentials

Figura 27: Elementos de la oferta Cisco para Firewall

Fuente: Documentación Interna Stein.

Como se nota en la imagen anterior, esta opción de cotización a nivel de Cisco fue con el proveedor más competitivo, y lo que se buscaba era una solución de dicha marca que brindara la seguridad del Firewall más IPS y Antivirus, gestionara VPN, filtrara contenido Web, y demás atributos para darle la oportunidad a la marca y al proveedor de competir con las otras tecnologías y comparar las inversiones finales, ya que era la tecnología presente en la organización hasta ese momento.

CANTIDAD	No. Parte	DESCRIPCIÓN
2	CPAP-SG4600-NGT	Firewall 4600 Next Generation Threat Prevention Appliance
2		Mantenimiento por el período de 1 año
1		Implementación de los equipos

CANTIDAD	No. Parte	DESCRIPCIÓN
2	PAP-SG4400-NGFW	Firewall 4600 4400 Next Generation Firewall Appliance
2	CPSB-URLF-S-1Y	URL Filtering Blade for 1 year - for low-end gateways
2		Mantenimiento por el período de 1 año
1		Implementación de los equipos

Figura 28: Elementos de las ofertas CheckPoint para Firewall

Fuente: Documentación Interna Stein.

Para esta marca CheckPoint en específico, como se nota en la figura anterior, se evaluaron dos modelos en específico, estos Firewall son líderes en el mercado ya que cuentan con un desarrollo propio del ejército israelí, que apreciando el alto nivel al cual habían llegado, empezaron a comercializar modelos específicos para el mercado internacional.

En este caso, el costo fue realmente superior, pero parte de eso es que el proveedor que nos brindó la oferta no es uno oficial de la marca, como consecuencia los costos de intermediación se elevaron y esta oferta quedó excluida por temas de costos.

Cantidad	Descripción
1	**XTM535 licenciamiento de seguridad por 1 año** • Rendimiento de Firewall*: 3 Gbps, Rendimiento de VPN* 550 Mbps, Rendimiento de AV* 1,8 Gbps, Rendimiento de IPS* 2.4 Gbps, Rendimiento agregado UTM* 1.4 Gbps, Interfaces 10/100 1 cobre, Interfaces 10/100/1000 6 cobre, Interfaces I/O 1 Serial/2 USB, Nodos soportados (IPs LAN) Ilimitado, Conexiones concurrentes(bidireccional): • 100.000, Nuevas conexiones / segundo 28.000, VLAN puenteo, etiquetado y modo enrutado 300, Base de datos de usuarios locales 500, VPN Para Sucursales 200, Mobile VPN IPSec (incl./máx.) 300, Mobile VPN SSL/L2TP (incl./máx.) 300
1	**XTM535 para Alta disponibilidad incluye solo licenciamiento live security por 1 año.**
1	**XTM330 licenciamiento de seguridad por 1 año** • Rendimiento de Firewall*: 1,4 Gbps, Rendimiento de VPN* 240 Mbps, Rendimiento de AV* 340 Mbps, Rendimiento de IPS* 640 Mbp, Rendimiento agregado UTM* 298 Mbps, Interfaces 10/100/1000 7 cobre, Interfaces I/O 1 Serial/2 USB, Nodos soportados (IPs LAN) Ilimitado, Conexiones concurrentes(bidireccional): 40.000, Nuevas conexiones / segundo 5.500, VLAN puenteo, etiquetado y modo enrutado 75, Base de datos de usuarios locales 500, VPN Para Sucursales 50, Mobile VPN IPSec (incl./máx.) 5/55, Mobile VPN SSL/L2TP (incl./máx.) 55
1	**XTM330 para Alta disponibilidad incluye solo licenciamiento live security por 1 año.**
1	**Implementación de configuración e instalación XTM535 y XTM330**
1	**Soporte para 4 equipos durante 1 año 24x7 con tiempo de respuesta máximo en 4 horas**

Figura 29: Elementos de la oferta WatchGuard para Firewall

Fuente: Documentación Interna Stein.

Esta fue la tecnología que cumplió con los requerimientos iniciales y que presentó el precio más competitivo. Desde un punto de vista de análisis, la mejor tecnología con el precio más bajo, cumplía con todo lo necesario para poder estabilizar

el tema de los VPNs entre las sedes y un nivel de seguridad perimetral más avanzado. Como adicional, esta opción presenta equipos de bajo costo, lo que abrió la posibilidad de poder incluir para una segunda fase, un proyecto para poder conectar a todas las sedes regionales vía VPN *Site-to-Side* y poder gestionar desde Costa Rica la seguridad de las sedes.

Tabla 3: Comparativa de Firewall, VPN y Filtrado / Control Web

Dispositivito		**Precio x 1 año**	**Precio x 3 años**	**A 5 años**
Cisco ASA		$28 654,68	N/A	$74 913,68
WatchGuard		$19 318,70	$31 374,63	$49 065,81
CheckPoint	4400	$69 380,00	N/A	N/A
	4600	$103 593,50	N/A	N/A

Esta tabla ejemplifica claramente el tema de los costos por cada tecnología evaluada, con la premisa de que deben ser 2 dispositivos para cada sede (Cartago y Escazú), uno activo y el otro para redundancia, donde cada tecnología gestiona esas actividades de manera diferente, siendo ambos equipos Activo/Pasivo o Activo/Activo; adicionalmente del costo a 3 y 5 años para evaluar la inversión a partir de los meses y poder considerar las anualidades, garantías y licenciamientos. Claramente se nota la diferencia del dispositivo WatchGuard, es esta la tecnología que se aprobó para su implementación.

Es importante aclarar que el presupuesto para este proyecto surge del ahorro en el enlace privado que existía entre las sedes de Costa Rica, con una inversión mensual

de $1.200, para una inversión a 36 meses de $43.200, lo que da como resultado de este proyecto un ahorro de más de $10.000 en el enlace, además de todos los avances en tecnología y modernización de la organización en los temas a que un UTM compete.

Etapa 2, Switch Core y distribución: Para esta etapa y aprovechando la necesidad de actualización de los equipos por motivos de la construcción de la nueva Planta de Producción de SteinCorp en su sede de Cartago, el foco principal fue evaluar un nuevo Switch Core para la administración de la red de la organización, y como consecuencia los switch de distribución (o de acceso) tomando en cuenta que la red ya está segregada a nivel regional y conectadas vía VPN a la sede de Cartago. El requerimiento principal es una tecnología eficiente y que mejore los actuales equipos Cisco Catalyst 2960-XR, buscando un costo competitivo comparando las tecnologías de avanzada como valor agregado.

Tomando en cuenta lo anterior es que se busca una competencia efectiva y se incluyen en la evaluación las tecnologías de HP y Alcatel-Lucent, para así no solo buscar valor agregado a nivel competitivo de *partners*, sino de tecnologías. El proceso se hace muy enriquecedor y da aún más claridad al mejorar los requerimientos iniciales al conocer nuevas tendencias y hacia dónde va el mercado. Con esto se resalta que Aruba no se toma en cuenta, ya que se preveía su compra por parte de HP.

Tabla 4: Comparativa de Switch Core

Marca	Stackeable	802.11 AC	Puerto Giga	BYoD Admin	Administración de Invitados	Wireless Controler	Interfaz	Garantía	RED Completa	Monitoreo
WG - HP	SI (IRF)	SI	SI	SI	SI	SI	GUI y HP IMC	5 años	SI	SI
Alcatel - Lucent	SI a 512Gbps	SI	SI	SI	SI	SI	GUI y Comandos	5 años	SI	SI
Cisco	SI a 480Gbps	SI	SI	NO	NO	NO	Comandos	1 año	Licenciada	Licenciada

Como se nota en la tabla anterior, la competencia entregó un valor que no se esperaba, con productos más competitivos que el instalado y tecnologías adicionales incluidas en el precio, como la garantía extendida, administración Web (en la actualidad Cisco ya cuenta con esto), controlador de red inalámbrica, invitados, BYOD (Dispositivos de los empleados) y otras.

Tabla 5: Comparativa de ofertas finales

Dispositivivo	Inversion: 1 año	Inversion: 5 años
HP-WG	$19 396,26	$20 238,66
Alcatel-Lucent	$27 860,09	$27 860,09
Cisco	$28 057,03	$32 584,11

Después de ser comparadas las tecnologías y evaluadas según los requisitos iniciales y necesidad de SteinCORP, y como se nota en la tabla anterior, las tecnologías nuevas, además de ser económicas entregan valor agregado. Tomando en cuenta la compatibilidad nativa del Firewall Instalado, se toma la decisión entre TI y la Dirección Financiera para adquirir las tecnologías de HP, por ser la más económica, además de que entrega igual o más valor que las otras opciones y que presenta

compatibilidad con el Firewall. Esta oferta incluye el switch de acceso y los puntos de acceso inalámbricos.

Etapa 3, acceso alámbrico e inalámbrico: Como consecuencia de la toma de decisión del Switch Core en la etapa 2, implícitamente se toma la decisión por los switch de acceso y access point, ya que debe existir la mayor compatibilidad para un trasiego de datos óptimo y un monitoreo de red sin puntos muertos por temas de incompatibilidad.

Tabla 6: Comparativa entre puntos de acceso inalámbrico

Marca	Control de BYoD	Red de Invitados	Perfiles de Acceso	Integracion con UTM	Wireless Controler	Radios	Antenas	Potencia TX	SSID	Costo (ii)
WatchGuard	SI	SI	SI	Nativa	Integrado	2	4	21 dBi	16	$ 772,17
Alcatel - Lucente	SI	SI	SI	NO	NO	2	4	21 dBi	16	$1 015,00
Cisco	NO	NO	NO	NO	NO	2	4	22 dBi	16	$ 786,67

Como se nota en la tabla anterior, hay un cambio en las posiciones 2 y 3 de los puntos de acceso inalámbrico, aunque la diferencia del costo de la tecnología de Alcatel-Lucent está relacionada con su avances, sí es un costo elevado, sobre todo al tomar en cuenta que la proyección al finalizar la obra será mayor a los 45 dispositivos, lo que generaría una diferencia superior a las $11.000. Al analizar la oferta de Cisco, aunque es un equipo relativamente del mismo precio, se evidencia una inferioridad con los temas de prestaciones de valor agregado.

Lo analizado en las anteriores etapas es un reflejo claro de la investigación de campo realizada para poder entregarle valor a la organización, siempre buscando alta

calidad y a bajo costo de inversión, revisando los detalles de las tecnologías y ajustando las necesidades. Todo esto asienta la base tecnológica de la red de telecomunicaciones informáticas actual de SteinCorp, a lo que este proyecto pretende acoplar y homologar en la sede de Escazú, que ha quedado excluida de esta modernización.

4.1.2 ESTÁNDARES INTERNACIONALES SOBRE LA RED DE COMUNICACIONES

La red cableada de SteinCORP está realizada con cable UTP categoría 5e, esto incluye la sede en cuestión de Escazú. Esta categoría está normada por los estándar EIA/TIA 568B y está diseñada para trasmitir datos hasta a 100 Mbps de velocidad y hasta 100 MHz de frecuencia.

Los estándar EIA/TIA 568B mencionados anteriormente son un conjunto de tres estándares que tratan de normar el cableado comercial para servicios y productos de telecomunicaciones, este sustituye al anterior 568A. Su característica primordial es la de normar la asignación de los pares de cables de 8 hilos, lo que se conoce como Par Trenzado en los cables de red con la nomenclatura T568A y T568B, este segundo es la norma utilizada en la organización para la terminación de los conectores de RJ45. La imagen siguiente muestra su asignación de colores.

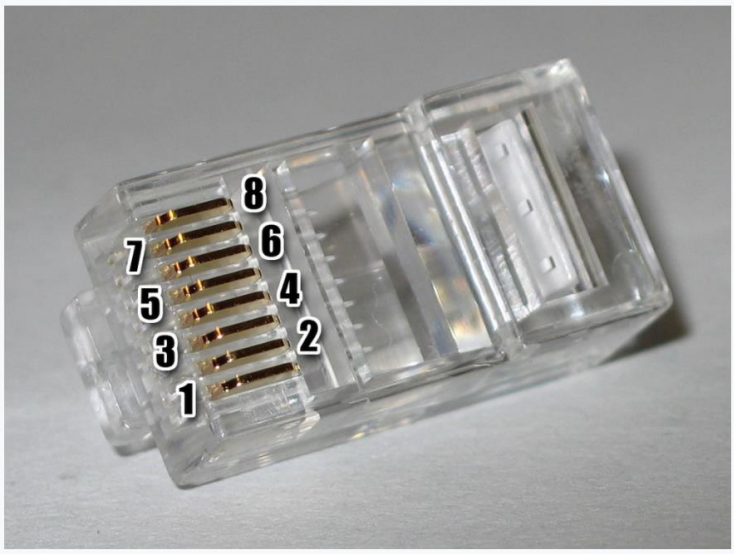
Pin	Color T568A	Color T568B	Pines en conector macho (en conector hembra se invierten)
1	Blanco/Verde (W-G)	Blanco/Naranja (W-O)	
2	Verde (G)	Naranja (O)	
3	Blanco/Naranja (W-O)	Blanco/Verde (W-G)	
4	Azul (BL)	Azul (BL)	
5	Blanco/Azul (W-BL)	Blanco/Azul (W-BL)	
6	Naranja (O)	Verde (G)	
7	Blanco/Marrón (W-BR)	Blanco/Marrón (W-BR)	
8	Marrón (BR)	Marrón (BR)	

Figura 30: Estándar del Par Trenzado A y B en el conector RJ45

Fuente: Web de Cabling Installation & Maintenance.

El objetivo principal de esta norma es definir los estándares que permiten el diseño e implementación de los sistemas de cableado estructural a nivel comercial, logrando así definir los tipos de cables, las distancias, sus conectores, arquitecturas de diseño, terminaciones de cables y las características de rendimiento, así como los requisitos de instalación con sus métodos de pruebas. Lo anterior gracias a las tres siguientes segmentaciones:

- TIA/EIA-568-B.1: Es el estándar principal y define los requisitos generales.

- TIA/EIA-568-B.2: Se centra en componentes de sistemas de cable de pares balanceados.
- TIA/EIA-568-B.3: Aborda componentes de sistemas de cable de fibra óptica.

La finalidad de estos estándares es la de proporcionar una serie de prácticas y guías recomendadas para el diseño e instalación de los sistemas de cableado y cubrir un rango de vida de 10 años.

A nivel lógico de las telecomunicaciones, los equipos a utilizar están normados por la IEEE y su comité 802, ya que los estándares desarrollados por este comité están enfocados en la capa 1 y 2 del modelo OSI. Este comité se divide en Subcomités, los cuales son los siguientes:

- 802.1: Panorámica y Arquitectura, Puentes, redes locales virtuales (VLan)
- 802.2: LLC, Logical Link Control (actualmente en hibernación e inactivo)
- 802.7: Grupos técnicos asesores en redes de banda ancha
- 802.8: Grupos técnicos asesores en fibras ópticas
- 802.10: Niveles de seguridad en estándares 802

Y los Subcomités especializados en los métodos de acceso:

- 802.3: CSMA/CD (Ethernet)
- 802.4: Token Bus (actualmente en hibernación e inactivo)

- 802.5 Token Ring
- 802.6: Distributed Queue Dual Bus (actualmente en hibernación e inactivo)
- 802.9: Servicios Integrados (ISO-Ethernet)
- 802.11: Redes inalámbricas
- 802.12: Demand Priority (100VG-AnyLAN)
- 802.14: Redes de televisión por Cable

Para este caso de estudio, se analizará la especificación IEE 802.11 (ISO/IEC 8802-11), en la cual se regula las redes inalámbricas, y que garantiza la compatibilidad entre los dispositivos inalámbricos y más específicamente a lo que compete a las conexiones de los equipos como lo son la norma 802.11a/b/g/n/ac. Las demás son normas implícitas en los equipos de comunicación actuales.

- 802.11a: Admite un ancho de banda superior de 54 Mbps, aunque en la práctica es de 30 Mbps.
- 802.11b: Ofrece un rendimiento total máximo de 11 Mbps (6 Mbps en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto.
- 802.11g: Igual que el 802.11a, pero en la frecuencia de los 2.4Ghz, lo que amplía el alcance.
- 802.11n: Mejora a sus predecesores alcanzando velocidades hasta los 600mbps, aunque en la práctica es de 300Mbps, y el usuario percibe unos 100Mbps, logrando comparación con el cable UTP.

- 802.11ac: Mejora la 802.11n, trabaja en la banda de los 5Ghz y alcanza teóricamente la velocidad de 1.3Gbps, logrando mejorar la taza de transferencia hasta 433 Mbps por cada flujo de datos.

4.2 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

Hace más de cinco años, las nuevas oficinas administrativas de SteinCorp en su sede de Escazú presentaban equipos de gran tecnología, al menos eso fue propuesto por el proveedor de redes en aquel entonces. Al buscar un poco de documentación del proyecto en los archivos de aquel entonces, no se encuentra información de dicho proceso, lo que imposibilita saber qué se tomó en cuenta, como resultado se instaló una infraestructura sólida y funcional para el dimensionamiento inicial pero con la opción de crecimiento muy reducida. Poco más de un año después, se expande la oficina de Escazú al adquirir un nuevo espacio administrativo en el piso de abajo, donde lo que se busca, a nivel de infraestructura, es acoplarse a lo ya existente, con la gran limitante de TI de no poder mejorar lo que ya estaba instalado, solo unirse a la red.

Aunque en su momento, lo anterior dejó a la sede de Escazú superiormente más actualizada que a la sede de Cartago, la ausencia de un análisis y proyección a futuro deja hoy en día a dicha sede con un colapso tecnológico y redes saturadas. Por esta

razón se enlistarán a continuación los equipos actuales instalados, que son los que el presente proyecto planteará sustituir y homologar con la sede central.

Tabla 7: Equipos actuales de SteinCorp en la sede de Escazú

Descripción	Cantidad	Modelo	Puertos	Antigüedad	Garantía
5to Piso					
Switch	1	Cisco 2960	48	+ 5 años	No
Switch	1	Cisco 2960	48	+ 5 años	No
Switch	1	3Com 4226T	24	+ 5 años	No
Switch PoE	1	Linksys LGS318P	18	- 1 año	Si
Access Point	4	AIR-CAP1602I-A-K9		+ 5 años	No
4to Piso					
Switch	1	Cisco 2960-X	24	+ 3 años	No
Switch	2	Catalyst 2960-C	12	+ 3 años	No
Wireless Controler	1	Cisco 2504		+ 3 años	No
Access Point	3	AIR-CAP1602I-A-K9		+ 5 años	No

Como se nota en la tabla anterior, se tiene el listado de los equipos actuales instalados en la sede de Escazú. El único que cuenta con garantía y que es un modelo reciente, fue adquirido únicamente para la instalación de teléfonos ejecutivos para ser alimentados por PoE, pero el cual no es lo suficientemente robusto para el trasiego de datos de la organización.

El resto de equipos ya se encuentra sin garantía y se dejó de pagar el *smartnet* de Cisco. En caso de falla se reemplaza por equipos en igualdad de condiciones, dichos equipos son los que se han reemplazado en Cartago y que aún se encuentran en calidad funcional, aunque obsoletos y sin valor en libros.

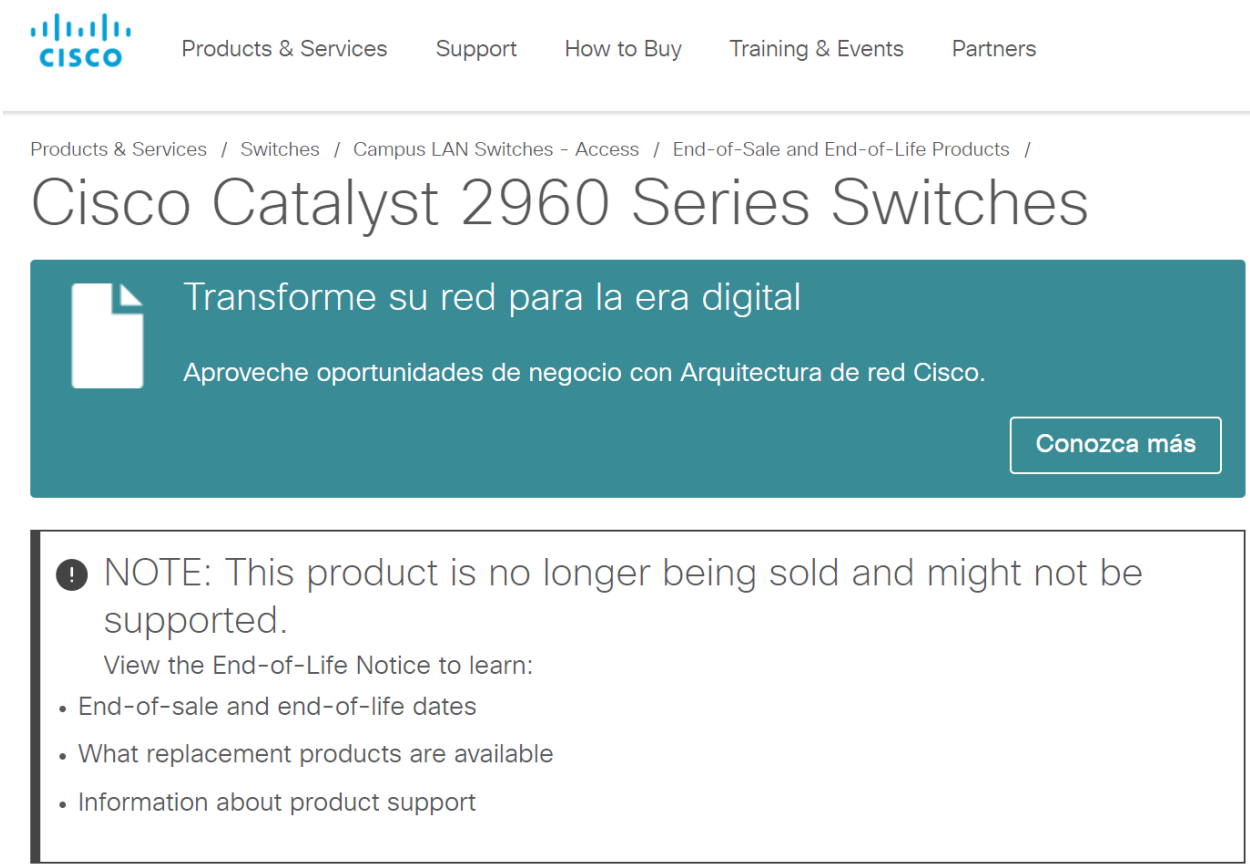


Figura 31: Estado de equipos Cisco 2960

Fuente: Web de Cisco.

Como se nota en la figura anterior, los equipos principales de la sede de Escazú ya no se encuentran cubiertos por el soporte de Cisco, de aquí la urgencia de reemplazarlos; una falla en estos equipos significa desconexión y pérdidas cuantificadas minuto a minuto.

4.2.1 OBJETIVOS DEL PROYECTO DEL NUEVO SITIO

Como proyecto tecnológico el objetivo es simple, es el darle conectividad y valor a los colaboradores de la organización, logrando minimizar el impacto por los errores frecuentes de red y aumentando la efectividad de las transacciones de datos de información. Se logra además ser eficientes y entregar un producto de calidad en la sede de Escazú, aprovechando la experiencia acumulada en la nueva planta de Cartago. Dicha red ha traído gran valor a los distintos departamentos que ya están aprovechando su nueva infraestructura.

En sí, no se trata de comprar, configurar y montar equipos nuevos, se trata de minimizar los errores y entregarle una conexión segura, estable y de calidad al usuario final, donde su satisfacción sea del 100% y se aumente su productividad, todo bajo los estándares correctos y las mejores prácticas de implementación. También se busca el precio más competitivo y el proveedor de mayor experiencia, para lograr así la confianza que genera el saber que se trabaja con el mejor y al costo más justo.

4.2.2 EQUIPOS E INFRAESTRUCTURA ACTUAL

Como ya se ha mencionado anteriormente, la organización ha invertido en todos los equipos de red gracias a las obras de remodelación de la planta de Cartago, a su vez de cada nueva sede de los países cuando se trasladan. Estos equipos se adquieren con 5 años de garantía NBD (próximo día laborable) adicional de la garantía de por

vida de los conmutadores HP y de 3 años en el caso de los *access point* de WatchGuard; el por qué estos equipos tienen menos años de garantía, es para evaluar en su vencimiento si se extiende o se renueva, si la tecnología nueva en su momento genera valor.

Tabla 8: Equipos actuales de SteinCorp en la sede de Cartago (Julio 2017)

Descripción	Cantidad	Modelo	Puertos	Antigüedad	Garantía
DataCenter / TI					
Core Switch HP 01	1	HP 5130	48	- 2 años	Si
Core Switch HP 02	1	HP 5130	48	- 2 años	Si
Switch de Acceso PoE	1	Aruba 2530	48	- 2 meses	Si
Switch de Acceso PoE	1	Aruba 1920	24	- 2 meses	Si
AP WG	1	AP 100		- 1 años	Si
Bodega					
Switch de Acceso PoE	1	HP 2530	48	- 2 años	Si
AP WG	10	AP 100		- 2 años	Si
Anexo A					
Switch de Acceso PoE	1	HP 2530	48	- 2 años	Si
AP WG	4	AP 100		- 2 años	Si
Área 100 / 200					
Switch de Acceso PoE	1	HP 1920	24	- 1 años	Si
AP WG	2	AP 100		- 1 años	Si
Zona Franca					
Switch de Acceso PoE	1	HP 1920	24	- 1 años	Si
AP WG	1	AP 100		- 1 años	Si
Anexo B					
Switch de Acceso PoE	2	Aruba 2530	48	- 1 años	Si
AP WG	5	AP 100		- 1 años	Si
Área 5 / 6 / 7					
Switch de Acceso PoE	2	Aruba 2530	48	- 2 meses	Si
AP WG	4	AP 100		- 2 meses	Si
Panamá					
Switch de Acceso PoE	1	HP 1920	24	- 1 años	Si

AP WG	2	AP 100		- 1 años	Si
República Dominicana					
Switch de Acceso PoE	1	HP 1920	24	- 1 años	Si
AP WG	2	AP 100		- 1 años	Si

Como se nota en la tabla anterior, todos los equipos de conmutación que se adquieren son HP, con ese nombre se identifican las primeras compras y con el nombre de Aruba las siguientes; esto después de que HP formalizara la compra de Aruba a inicios del 2015. La nomenclatura de los equipos permanece.

Figura 32: Cuadrante Gartner, Redes 2014 vs 2016

Fuente: Web de Gartner.

Como se nota en la figura, para el 2014 los competidores de Cisco a nivel de redes eran HP y Aruba, con esta “alianza” se pretendía una competencia más agresiva, y logra a finales del 2016 posicionarse más cerca aún. A nivel de la organización la experiencia del usuario final y la administración de la red por parte del departamento de

TI ha sido realmente satisfactoria, con lo que se logra crear grandes expectativas y afianzar el proyecto de obra constructiva fácilmente. Cada nueva etapa lleva consigo una compra de estos equipos, la cual es firmada con confianza por parte del comité de la obra.

4.3 ESTABLECIMIENTO DE BRECHAS

Lo que se analizará a continuación es la necesidad real del por qué esta propuesta de proyecto es prioritaria para la organización y que generará gran valor y efectividad a los colaboradores. Desde el punto de vista comparativo a lo que se ha implementado recientemente y cómo se ha visto afectada la sede de Escazú al quedar aparte de estos avances a nivel de redes.

4.3.1 COMPARACIÓN DE LA SITUACIÓN IDEAL VERSUS LO ACTUAL

La brecha principal entre la sede de Escazú y la de Cartago son los equipos de conmutación y sus puntos de acceso inalámbrico, como se ha explicado ampliamente con anterioridad, la diferencia radica en los equipos están obsoletos en esta sede. Gracias al cambio de la central telefónica en marzo anterior, de Cisco a Microsoft (CloudPBX), se evidenció las grandes deficiencias al trasferir paquetes de datos, obligando a los usuarios a conectarse por medio de cable a la red, como consecuencia de que al realizar llamadas vía Skype Empresarial, existía interferencia o las llamadas colapsaban, se ocasionaba su corte. Adicionalmente se tiene el tema de la saturación

de los switch de accesos al no contar con puertos disponibles y tener que liberar puntos menos importantes para conectar equipos prioritarios.

Mientras que en Cartago (y otras sedes) se cuenta con una red alámbrica e inalámbrica robusta, donde los usuarios no perciben una diferencia al estar conectados en una o en otra red, en Escazú existe la necesidad de estar conectado por cable para lograr una calidad aceptable. Esto sin considerar las demás aplicaciones involucradas como SAP y toda la plataforma de Office 365 con la cual cuenta la organización, donde el Firewall de cada sede regula mediante calidad de servicio (QoS) los enlaces y aplicativos; en Escazú se pierde esta manipulación al ser trasegados en la red interna. Como consecuencia de esta problemática, se tuvo que crear una red independiente y que saliera directamente del Firewall al área de Alta Gerencia, para minimizar el impacto negativo que estaban generando los altos ejecutivos y que esta propuesta pretende resolver al resto de la organización.

Como punto final de la brecha, se encuentra la alta demanda de las direcciones IP. Actualmente se cuenta con una VLAN para toda la sede de Escazú, en un inicio no había problema al ser poca la cantidad de colaboradores, pero con la inclusión del cuarto piso y el crecimiento de la planilla, es que se debe limitar el ingreso de dispositivos *BYOD* debido al que el segmento del DHCP se satura. A esto se le agrega la política de renovación de cada 4 horas, para ir liberando el segmento de equipos que ya no están conectados. Esta propuesta incluye la creación de una VLAN para cada piso, para solucionar este problema de forma definitiva.

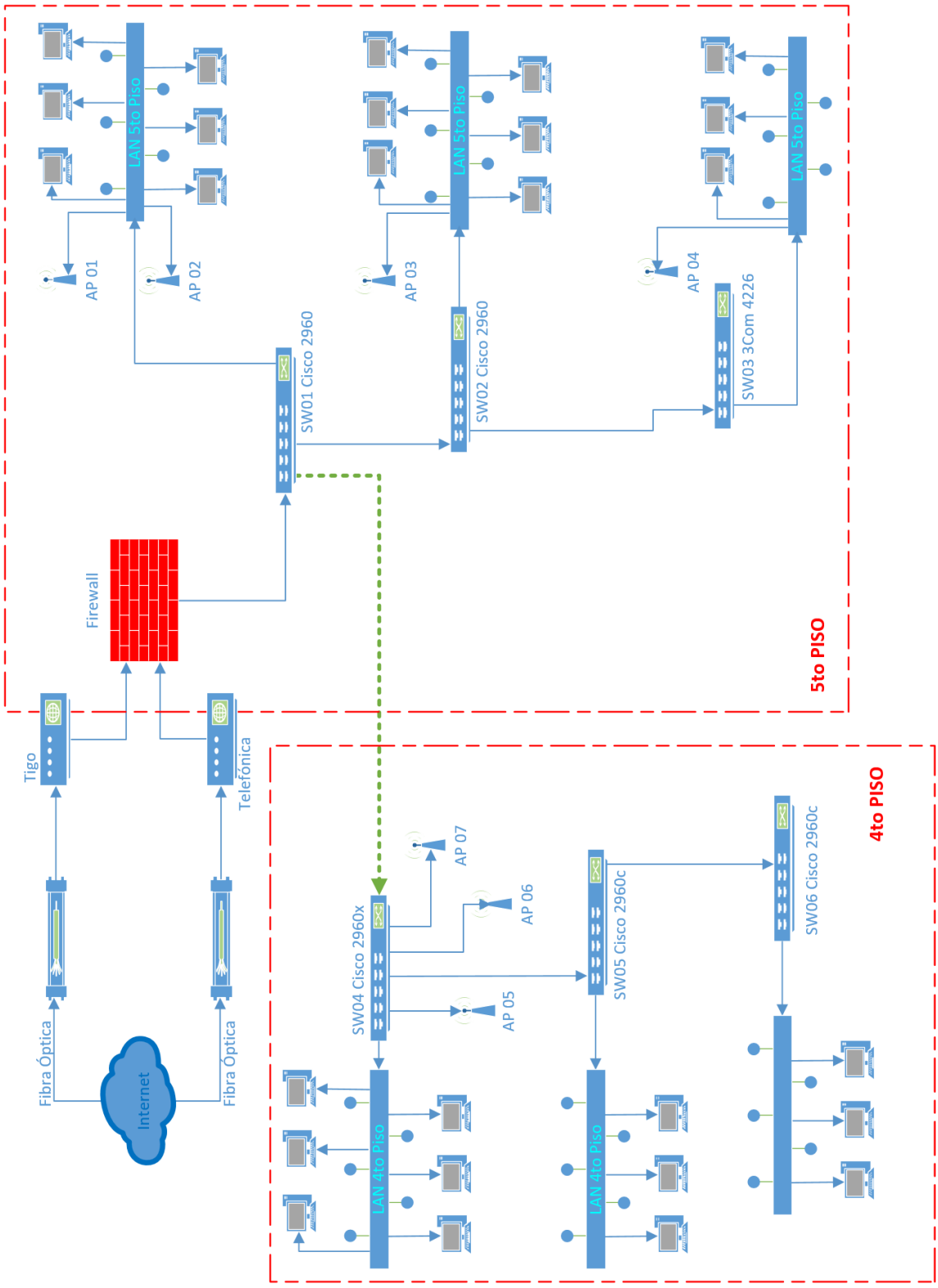


Figura 33: Red Actual de la sede de Escazú

Fuente: Diseño Propio.

La figura anterior detalla los equipos instalados en la sede de Escazú (sus respectivos detalles se encuentran en la tabla 7 de la sección 4.2). Su fin es ayudar a comprender la diferencia entre la red actual y la red propuesta, descrita en el diagrama de la siguiente figura 34 de la sección 5.2.1 del presente documento, y retomando el tema anterior, saturación del segmento de red de Escazú. Esto en comparación con la sede de Cartago, donde cada subred tiene su propia VLAN, con su respectivo direccionamiento independiente, donde se permite lograr una separación en los segmentos y se evita fallas masivas, así como un control más puntual a nivel de la identificación de IPs en caso de amenazas.

4.3.2 CONCLUSIONES DEL DIAGNÓSTICO

Gracias al análisis inicial y a la documentación existe de la renovación del Core Switch y los equipos de acceso, así como de las vanguardias y tecnologías actuales a nivel de redes, es que se logra identificar fácilmente que la tecnología instalada en la sede central de SteinCorp en Cartago y sus filiales más actuales. Es lo que a la organización le ha resultado funcional, al lograr una convivencia ideal entre los equipos de firewall, los de redes y los puntos de acceso inalámbrico, y lo que al usuario le ha sido gratificante, casi que omitiendo los problemas de red.

Lo anterior en comparación a los reportes y a la experiencia acumulada con la implementación de SharePoint en Office 365 a inicio del 2016, es que el consumo de

los recursos de red se vieron degradados de una forma relativamente notoria. Pero con las migración de la central telefonía a Skype Empresarial de Microsoft, colocando el CloudConnect en Cartago y aumentando aún más dicho consumo, es que se volvió evidente la necesidad de esta propuesta, sobre todo al ser previsto este problema en el Diagrama de Ishikawa en la figura uno del presente documento y creado desde el 2016.

Para cubrir la necesidad de consumo de datos de los usuarios, satisfacer a los altos ejecutivos con servicios estables y activos, minimizar las fallas de comunicación y extraer lo máximo de todo el valor agregado con la cual cuenta la plataforma de Office 365, es que esta propuesta debe ser considerada y aprobada, en pro de buscar la homologación de las redes y eliminar la brecha que existe actualmente entre Cartago y Escazú. Más aun con la necesidad de brindar al sector administrativo de la organización, bienes y productos informáticos de calidad y estables, buscando siempre la alianza estratégica entre TI y el resto de la organización.

Para allanar este camino de implementación es que recientemente se renovó los equipos de Firewall de ambas sedes principales, equipos que controlan hasta 800 usuarios recurrentes y bajo modalidad de infraestructura como servicio, dando valor y garantía de funcionalidad. Lo que resta a nivel de Escazú es igualar la red de datos entre ese Firewall y el usuario final, al estar conscientes de que la red cableada se encuentra en perfectas condiciones y cableando desde cero únicamente los equipos de

acceso inalámbrico, para poder contar con la certeza de la funcionalidad correcta de dichos dispositivos.

En modo resumen, es vital para la organización adquirir equipos robustos y nuevos que controlen el trasiego de datos, así como equipos de acceso inalámbrico que le den autonomía y movilidad a los colaboradores de la organización, para facilitar su trabajo y aumentar su rendimiento y satisfacción. En los tiempos que se vive actualmente en SteinCorp, el colaborador necesita estar conectado para cumplir sus funciones, esta propuesta se enfoca en brindar esa conectividad con el mínimo impacto negativo.

CAPÍTULO V

PROPUESTA DE PROYECTO

5.1 REQUERIMIENTOS DEL PROYECTO

En esta sección se aborda los requerimientos técnicos y documentales que la organización necesita para poder ejecutar la propuesta, desde detalles específicos de los equipos hasta temas de comunicados y respaldos. Se da forma así a todo el proyecto, sumando las pequeñas tareas.

5.1.1 REQUERIMIENTOS DE LA ORGANIZACIÓN

Para poder ejecutar las tareas, la organización necesita la documentación inicial de la implementación, así como la elaboración de una guía de tareas específicas antes de poder desconectar el primer cable, por ello es que se elaboran como requerimiento los Planes de Comunicación y de Posimplementación.

Plan de Comunicación: Cada labor a realizar tangible deberá ser comunicada mediante correo electrónico y utilizando la cuenta de recursos humanos en coordinación con la comunicadora de la organización, esto le dará visibilidad del proyecto al personal. En semanas previas a la ejecución se enviará una serie de comunicados organizacionales informando de los cambios y mejoras que el proyecto traerá, esto para elevar la percepción del usuario y limitar la resistencia al cambio que por lo general estos proyectos generan.

Como parte de estos comunicados previos, se hablará de una forma muy simple de las mejoras en los equipos y de cómo estos ayudarán a una mejor ejecución de las tareas diarias, así como de *tips* que sean de utilidad y mensajes de importancia, como los nombres de las redes y la inclusión de una red de invitados. De forma paralela se les comunicará a los altos mandos, por parte de la Gerencia de TI, detalles más específicos y afectaciones más puntuales, esto para minimizar la brecha y acercar a estos personeros al proyecto de una forma en que se sientan parte del proyecto, así como datos de inversiones y consultorías involucradas.

Una semana antes del proyecto, se deberá intensificar los comunicados y cambios más sensibles, para que en la puesta en marcha del proyecto sea trasparente y el cambio de la red inalámbrica no los tome por sorpresa y sea de su entender que mientras los personeros de Soporte Técnico le configuran la nueva red, se puede conectar por cable para que su trabajo no se vea interferido. También se deberá comunicar que los dos primeros días del proyecto un personero externo a la organización atenderá exclusivamente temas de conexión y autentificación, esto para que lo reconozcan cuando el personero los visite y atienda sus consultas.

Plan de Posimplementación: Este requerimiento tiene como finalidad el documentar todas las actividades que minimizarán cualquier impacto negativo que resulte de la implementación y tener la forma de abordar y solucionar, así como los miembros del equipo dispuestos a solucionar y que están descritos en la tabla de responsables y en la Matriz RACI que se detallará más adelante.

Para efectos de esta propuesta, se realizará una tabla de las posibles causas de fallas o de percepción. Esta tabla será de uso de todo el equipo de TI, para estar alineados en la información y en las posibles causales, y así no generar una percepción incorrecta del proyecto ya implementado.

Tabla 9: Check-List del Plan Posimplementación

Queja	Actividad	Monitoreo
Sin conexión a la red	Revisar el punto o la conexión a la WiFi.	Monitorear el Switch y el Wireless Controler del WatchGuard.
Red lenta	Revisar actividad del usuario o de los enlaces de Internet desde el punto del usuario.	Monitorear los enlaces de Internet y sus consumos.
Autentificación de usuario	Reautentificar o reiniciar el equipo.	Monitorear el punto de conexión cercano al usuario y el DHCP de Escazú.
Fallo o caída en la telefonía	Revisar consumo del usuario, actualizaciones de Windows o punto cercano de conexión.	Monitorear el enlace de Internet y el VPN con Cartago.
SAP lento	Revisar actividad de consumo del usuario o conectividad desde el punto del usuario.	Monitorear los enlaces de Internet y sus consumos.
Certificado de Outlook	Reautentificar o reiniciar el equipo.	Monitorear el punto de conexión cercano al usuario.
Skype se cierra solo	Reautentificar o reiniciar el equipo.	Monitorear el Switch y el Wireless Controler del WatchGuard.
Señal de la llamada débil	Revisar consumo del usuario, actualizaciones de Windows o punto cercano de conexión.	Monitorear el enlace de Internet y el VPN con Cartago.
Frecuentes desconexiones de la red	Elevar el caso al proveedor del Firewall y/o proveedor de los equipos de Red	Consumo y funcionamiento de los equipos de red.
Fallas frecuentes con el internet	Elevar el caso al proveedor de internet involucrado, o a ambos.	Consumo y funcionamiento de los enlaces de internet.

Errores frecuentes en los usuarios	Comunicado a toda la organización y capacitación de esos errores frecuentes.	Mediante el HelpDesk controlar las métricas de los problemas reportados con base en el proyecto.

Como los equipos serán reemplazados por equipos nuevos, los anteriores quedarán en acceso para tomar respaldos o utilizarlos en caso del Plan de Marcha Atrás, que se verá más adelante.

Con respecto a la información de configuración de los Switch, estos serán extraídos y documentados como primera parte del proyecto, esto para tener un control total de la configuración, rutas, VLan y demás que este pueda contener. Cabe resaltar que los equipos nuevos tendrán información completamente nueva, nada será igual, para asegurarse de una implementación limpia y funcional desde cero; esto incluye VLan nuevas hasta SSID nuevos con la inclusión de una red de visitas.

Por último, se dará Gestión con el Proveedor de forma directa con el ingeniero implementador y el Ejecutivo Postventa, para asegurar el compromiso y acompañamiento de la empresa implementadora.

5.1.2 REQUERIMIENTOS TÉCNICOS

En esta sección se tratará exclusivamente a la parte técnica de los requerimientos como lo son los equipos y sus características, así como la nomenclatura de las VLan y sus respectivos direccionamientos IP, que por temas de seguridad serán excluidos de toda información en este documento. Será únicamente documentado por parte del proveedor con la entrega del informe final, en caso de su implementación. En el caso de los Switch, los equipos a utilizar son de la marca Aruba (HP) y su modelo base el 2530, uno de 24 y cuatro de 48 puertos, todos PoE y montables en Rack con sus respectivos insumos.

Especificaciones técnicas:

- **Diferenciador:** El Aruba 2530-PoE+ es un conmutador de capa 2 completamente administrado
- **Puertos:** Puertos RJ-45 PoE+ 10/100/1000 con detección automática y cuatro Puertos SFP Gigabit Ethernet fijos
- **Memoria y procesador:** ARM9E a 800 MHz, flash de 128 MB, búfer para paquetes de 3 MB asignados dinámicamente y 256 MB de DIMM DDR3
- **Latencia:** Latencia de 100 Mb: < 7,4 µs, Latencia de 1000 Mb: < 2.3 µs
- **Velocidad:** Hasta 77,3 Mbps
- **Capacidad de Switching**: 104 Gbps
- **Función PoE:** 382 W

- **Capacidad de apilado:** Virtual o 16 conmutadores
- **Funciones de gestión:** Aruba AirWave Network Management, IMC - Intelligent Management Center, Interfaz de línea de comandos, Navegador web, Menú Configuración, Administración fuera de banda (RS-232C serie o micro USB), MIB Ethernet IEEE 802.3, MIB de repetidor, MIB de interfaz Ethernet
- **Garantía:** Garantía limitada de por vida + NBD por 5 años

En el caso de los Access Point serían los WatchGuard AP120, es la versión mejorada y actualizada de los AP200 que se venían utilizando hasta ahora. Su costo unitario se incrementa de los $420 a los $700.

Especificaciones técnicas:

- **Implementación:** Interior
- **Cantidad de radios:** 2
- **Bandas de frecuencias soportadas:** 2,4 GHz y 5 GHz simultáneas
- **Cantidad de Antenas:** 4 internas, omnidireccionales
- **Flujos TX/RX:** Transmisiones espaciales duales de 2x2 MIMO
- **Potencia máxima:** 20 dBm
- **Tasa Máxima de Datos:** Hasta 866 Mbps en 11ac / Hasta 300 Mbps en 11n
- **SSID por Radio:** 8
- **Opciones de seguridad:** WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK (Mixto), WPA-802.1X (Enterprise) WPA2-802.1X (Enterprise) WPA-

802.1X/WPA2-802.1X (Mixto), TKIP, AES, TKIP/AES, Portal Cautivo, Lista blanca/negra de MAC, Etiquetado VLAN

- **Ethernet:** 1 de 1Gb
- **Alimentación Ethernet (PoE):** Sl
- **Estándares del IEEE admitidos:** 802.11a/b/g/n/ac, 802.11i, 802.1q, 802.1X, 802.3af/at, 802.11e
- **Soporte y Mantenimiento:** Standard Support de 3 años para obtener garantía de hardware con reposición avanzada, soporte al cliente y actualizaciones de software, todo incluido con la compra

En el caso del cableado a requerir, serían cables de máximo 1,5 pies de categoría 5e con la norma T568B, esto para sustituir algunos defectuosos y las horas de Implementación por parte del ingeniero de Tecnova, ya que este es quien ha acompañado a TI en las demás configuraciones y es el ingeniero responsable de la topología del Firewall del WatchGuard.

Adicional a las características técnicas de los equipos, otro requerimiento técnico son las pruebas a realizar. Siempre y cuando las VLan y los direccionamientos IP sean declarados correctamente en las rutas del Firewall y del DC, no existe mayor complejidad, aun así, se deben realizar pruebas como las siguientes:

Pruebas de comunicación: Están pruebas se enfocan en la comunicación bidireccional de los dispositivos, sedes y redes externas, permitiendo el correcto flujo

de datos, y para ello se probará que la información entre la sede de Escazú y las siguientes redes externas sean correctas:

- Escazú – Cartago
- Escazú – SAP
- Escazú – Office365
- Escazú – Internet
- Escazú – ICE
- Escazú – Llamadas Internacionales
- Escazú – SharePoint

Pruebas de funcionamiento: Estas pruebas están enfocadas en el funcionamiento de los equipos del usuario final, y se enfoca en el correcto funcionamiento de sus aplicaciones que consumen datos de la red:

- Ofimática y Telefonía
- SAP
- SharePoint
- Aplicativos que conectan a: CCSS, Ministerio de Hacienda, Ministerio de Salud, Agencia de Viajes, Almacenes Fiscales.
- Impresoras
- Escáner

5.1.3 REQUERIMIENTOS DE NORMAS O MEJORES PRÁCTICAS

Parte de este enunciado ya se viene explicando en los dos anteriores, aunque acá se detallan dos prácticas comunes en TI de la organización como el Análisis de Riegos y el Plan de Vuelta Atrás.

Análisis de Riesgos: El equipo deberá prevenir errores o situaciones que pueden ocurrir y afectar la ejecución del proyecto y crear tareas para responder ante estas eventualidades. La idea final será listar los riesgos en probabilidades de que ocurran y cuáles serán las acciones para minimizar o anular su impacto.

Tabla 10: Análisis de Riesgo

Riesgo	Acción
Equipos Dañados	Configurar una semana antes del día 0
VLan no funcional	Configurar una semana antes del día 0
IPs no funcionales	Configurar una semana antes del día 0
Cables dañados	Tener cables adicionales, así como puntas de RJ45, Clipadora y Ponchadora
Enfermedad	Colaborador adicional para cada tarea
SSID sin respuestas	Reconfigurar SSID o contraseña

Claro está que esta tabla se podría alimentar aun con más detalle a la hora de la configuración inicial y extracción de la configuración del equipo a reemplazar, con la información completa de todas las configuraciones mínimas que se escapan de las iniciales.

Plan de Vuelta Atrás: Por supuesto que siempre existe el riesgo que se debe evaluar y documentar las acciones en caso de que lo que se vaya a implementar sufra un colapso y se deba devolver a la configuración y equipos anteriores. El objetivo de este plan es que en caso de que una tarea no fuera exitosa, se regresa a su estado inicial, se valoran las fallas y se retoma en otro momento. Por lo general estas implementaciones se realizan de noche o en fin de semana, y ante una eventualidad es mejor tener una lista de tareas que realizar y no permitir que un miembro del equipo, cansado, tome una mala decisión.

Para lo anterior y de una forma muy sencilla y metodológica, los equipos Aruba y WatchGuard se configurarán con una semana de anticipación como mínimo. Una vez que sea todo funcional, el día 0 se reemplaza y en caso de tener que regresar atrás, se desconectan los equipos nuevos y se vuelve a instalar los equipos viejos. Se retrasa el proyecto dos semanas más mientras se evalúan las causas, se corrige y se busca una fecha para volver a ejecutar.

Adicional a lo anterior, como parte de los protocolos y requisitos por parte de TI se encuentra la Inducción de Equipos y tecnologías usadas en TI, esto para los miembros del equipo de trabajo y poder así agregar una charla técnica de la infraestructura actual y a lo que se va a llegar. Esto para los miembros del equipo que no tengan la experiencia del diseño de la red de la organización, y con este entendimiento se pueda optar por ideas y pasos más acertados, ya que se tendrá el conocimiento real por parte de los involucrados.

5.2 DISEÑO DE LA RED

En este enunciado se detallará la infraestructura a utilizar, según el número de puestos de la organización en la sede de Escazú y proyectando un crecimiento, así como la cantidad de puntos de acceso inalámbricos existentes, que serán reemplazados por la misma cantidad, pero con tecnología más eficiente. Así mismo que se instalarán expuestos en el cielorraso para evitar así pérdida de calidad de la señal por tener que atravesar el material con el cual está construido.

El diseño de la infraestructura es realizado en Visio Pro 2016 de Microsoft y se detallan los equipos y la forma de conectarse entre ellos, a su vez de especificar los puntos de acceso inalámbrico por piso. Este diseño se verá apoyado por los planos arquitectónicos de la organización para la correcta ubicación de los equipos y poder así tener un panorama más amplio y exacto de la ubicación, para una mejor cobertura de los alcances y límite máximo de usuarios recurrentes por dispositivo. De los planos arquitectónicos se limita la información por temas de seguridad en el presente documento, aunque en los planos de la documentación interna será detallado con exactitud.

5.2.1 DISEÑO O ARQUITECTURA GENERAL

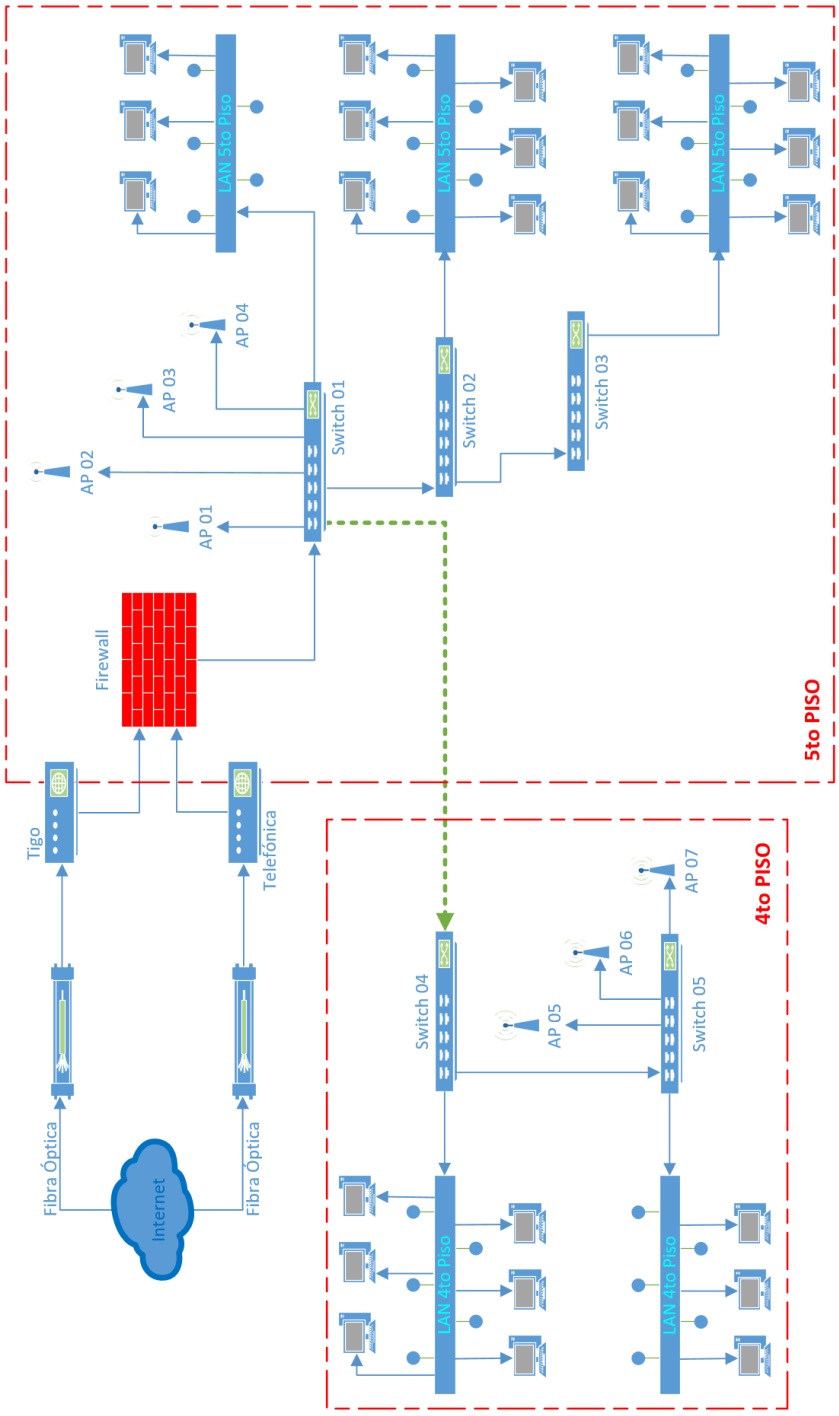


Figura 34: Diseño de Red de SteinCorp Escazú

Fuente: Diseño propio.

Como se detalla en la imagen anterior y en comparación a la figura 33 de la sección 4.3.1, es evidenciada la reingeniería de la red, se logra conectar todos los APs desde los equipos switch gracias a que se incluye la tecnología PoE en la totalidad de la red. A su vez permite conectar los equipos mediante un control de cargas, ya sea por medio de conexión alámbrica, o por medio del monitoreo web que los equipos incluyen de fábrica; se puede así ser proactivos en el servicio y no reactivos ante errores de conexión, esto entrega valor agregado.

También se detalla la reducción de equipos, pero aumento de puertos disponibles, gracias al reemplazo de dos equipos de 24 puertos, por los nuevos de 48 puertos y los dos equipos de 12 puertos por uno de 24 puertos, con esto se genera automáticamente el beneficio de mejorar el rendimiento.

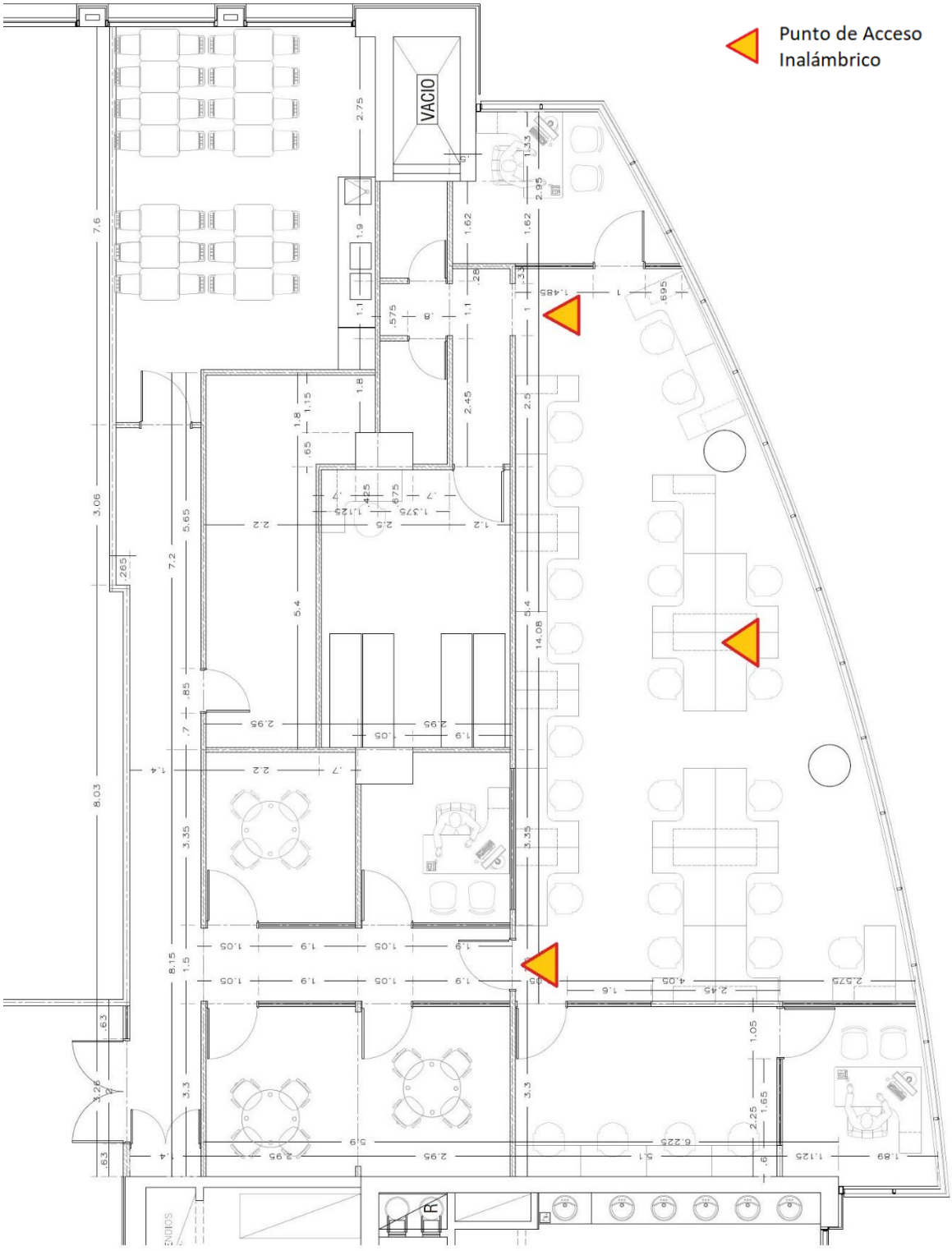


Figura 35: Colocación de los APs del 4to piso, SteinCorp Escazú

Fuente: Constructora Prifer e intervención propia.

La figura anterior identifica la ubicación correcta de los futuros puntos de acceso inalámbricos, estratégicamente colocados tomando en cuenta las cotas arquitectónicas, la cantidad de colaboradores por sectores y el mapa de calor de señal por parte del fabricante. Se logra así la identificación específica de la necesidad de tres dispositivos para este cuarto piso.

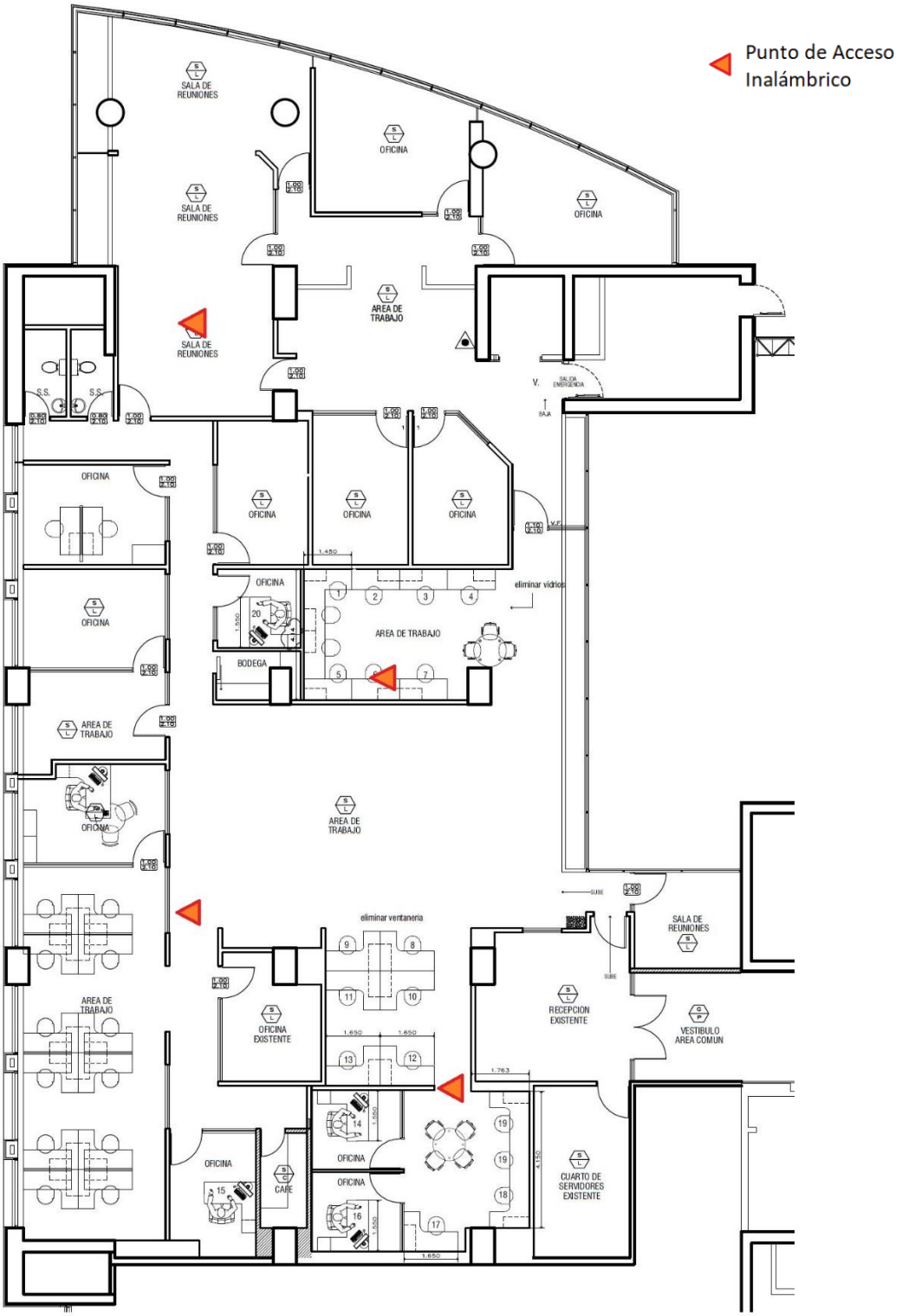


Figura 36: Colocación de los APs del 5to piso, SteinCorp Escazú

Fuente: Constructora Prifer e intervención propia.

La figura anterior, al igual que la del cuarto piso, identifica la ubicación correcta de los futuros puntos de acceso inalámbricos, estratégicamente colocados tomando en cuenta las cotas arquitectónicas, la cantidad de colaboradores por sectores y el mapa de calor de señal por pate del fabricante. Se logra así la identificación específica de la necesidad de cuatro dispositivos para este quinto piso.

Como detalle de esta figura, en la zona superior derecha del plano no se incluye ningún punto de acceso inalámbrico, a consecuencia de que estas oficinas son ocupadas por altos ejecutivos de la organización y cuentan con una red independiente que para efectos de esta propuesta no se verá modificada, ya que actualmente los equipos son funcionales y la inversión no tiene justificación.

Como conclusión, estas tres figuras anteriores detallan de una manera gráfica el resultado que la posible implementación de esta propuesta entregará a la organización, y en relación con lo descrito en la sección 4.3.1, muestra las mejoras en temas de eficiencia y espacio, así como el detalle que se contempló para los diseños y ubicaciones de los equipos en la futura infraestructura.

5.2.2 DIMENSIONAMIENTO DE LA INFRAESTRUCTURA DE TELECOMUNICACIONES

Tomando en cuenta la información suministrada en el Capítulo Cuatro del presente documento, exactamente en la “Tabla 3: Equipos actuales de SteinCorp en la sede de Escazú”, es que se detalla la lista de equipos requeridos para la presente propuesta:

Tabla 11: Dimensionamiento de los equipos a adquirir

Cantidad	Descripción	Marca	Modelo	Garantía
4to Piso				
1	Aruba 2530 24G PoE+ Switch	Aruba	2530	5 Años
1	Aruba 2530 48G PoE+ Switch	Aruba	2530	5 Años
3	Puntos de Acceso Inalámbrico (AP's)	WatchGuard	AP120	3 Años
5to Piso				
3	Aruba 2530 48G PoE+ Switch	Aruba	2530	5 Años
4	Puntos de Acceso Inalámbrico (AP's)	WatchGuard	AP120	3 Años
Adicional				
1	Servicio de Instalación Física de los AP's			
1	Servicio de Soporte de Ingeniero			

Las características técnicas de los equipos anteriores están específicamente descritas en el enunciado del capítulo “5.1.2 Requerimientos Técnicos”. Solamente estos equipos serán los tomados en consideración por cumplir con lo requerido para la organización en el tema de homologación ampliamente descrito en este documento, con la variante en la mejora del Punto de Acceso Inalámbrico, homologando y dando valor agregado con una mejora tecnológica en el tema de frecuencias.

Como referencia y base del dimensionamiento de los equipos y de las cantidades es que se estudia y evalúa cada oficina, sala de reunión y requerimientos especiales.

Tabla 12: Dimensionamiento de la necesidad de puntos disponibles.

Detalle	Cantidad
5to Piso	
Usuarios	62
Impresoras	5
APs	4
Teléfonos IP	12
Oficinas Gerenciales	20
Salas de Reunión	8
Telepresencia	2
Equipos Especiales	7
Puertos totales	120
4to Piso	
Usuarios	31
Impresoras	1
APs	3
Teléfonos IP	2
Oficinas Gerenciales	9
Salas de Reunión	4
Equipos Especiales	2
Puertos totales	52

Como se detalla en la tabla anterior, el requerimiento para el quinto piso es de 120 puntos, los cuales serán cubiertos con los 3 equipos de 48 puertos para un total de 144 puntos disponibles. Para el cuarto piso la necesidad es de 52 puntos que serán cubiertos con un equipo de 48 puertos y otro de 24 puertos, para un total de 72.

De la referencia anterior es que nacen los requisitos de dimensionamiento de los equipos que se necesitan para reemplazar los existentes, a su vez de permitir un crecimiento oportuno con las limitantes de la organización. Esto ayuda a no sobredimensionar una realidad que no tiene razón de considerarse.

Con base en lo anterior y a las tecnologías de Cartago que funcionan de base para esta propuesta, se identifican los requerimientos básicos que los equipos se van a adquirir deben cumplir.

Tabla 13: Dimensionamiento de los equipos inalámbricos.

Punto de Acceso Inalámbrico WatchGuard AP 120	
Compatibilidad con el Firewall	SI
Estándares 802.11a/b/g/n/ac	SI
RJ45 PoE	1
Montable en Cielo Raso	SI
Indoor	SI
Radios	2
Frecuencias	2.4GHz / 5GHz Concurrentes
Antenas	4
SSID mínimos	8
Peso Máximo	0,40 kg

En la tabla anterior se detallan los requerimientos mínimos con los cuales debe contar el punto de acceso inalámbrico para su correcto funcionamiento en la red de la presente propuesta, con más detalle se especifica en el Anexo II.

Tabla 14: Dimensionamiento de los equipos de conmutación.

	Aruba 2530 24G	Aruba 2530 48G
Calidad de Servicio (QoS)	SI	
Administración GUI	SI	
Apilamiento Virtual	SI	
Monitoreo	SI	
Autocorrección de problemas	SI	
Renombrar Puertos	SI	
SFP	4	
VLan	512	
Memoria	128 MB flash Packet buffer size: 3 MB dynamically allocated 256 MB DDR3 DIMM	
Procesador	ARM9E 800 MHz	
PoE	195w	382W
Capacidad	100 Mb Latency < 7.4 µs (LIFO 64-byte packets) 1000 Mb Latency < 2.3 µs (LIFO 64-byte packets) Throughput up to 77.3 Mpps (64-byte packets)	
Capacidad de Switching	104 Gbps	56 Gbps

En la tabla anterior se detallan los requerimientos mínimos con los cuales deben contar los equipos de conmutación para su correcto funcionamiento en la red de la presente propuesta y satisfacer la necesidad de puntos a conectar de forma física, con más detalle se especifica en el Anexo IV.

Las tres tablas anteriores resumen la lista de requerimientos del dimensionamiento de las necesidades de la presente propuesta, desde la necesidad de

los puntos a conectar, como las prestaciones de latencia y rendimiento de los equipos, así como temas básicos a cumplir como lo son VLan y SSID.

5.2.3 CONFIGURACIÓN DE LA RED DE COMUNICACIONES

Las nomenclaturas y descripción detallada de la topología de la red deben ser simplificadas para poder hacer público el presente documento, aunque esta tipología deberá estar debidamente documentada en el informe final del proyecto en caso de realizarse. En sí hay dos configuraciones de prioridad a realizar en esta propuesta, que son la configuración de las VLan y los SSID, para lo cual utilizaremos información ficticia para su documentación y ejemplificación.

En el caso de las VLan, como se ha explicado en la sección 2.4.6, es una red virtual dentro de una red física, los equipos que se requieren administran hasta 512 redes de este tipo, aunque el requerimiento técnico de la presente propuesta especifica la creación de tres redes virtuales para una correcta administración y segmentación, estas serán para cada piso y una administrativa para equipos de red y servidores. Como requerimiento deberán tener reservadas las 30 primeras IP y por DHCP el resto será entregado a la red para la conectividad de los equipos.

VLan Cuarto Piso – ID 404: Esta red entregará direccionamiento de IPs del segmento de red 192.168.40.1, de las cuales las 30 primeras IP (192.168.40.1 -

192.168.40.30) estarán reservadas para las impresoras, APs, Teléfonos IP y equipos especiales.

El total de puntos de red con conectividad de este piso es de 52, los equipos que se necesitan adquirir completan 72 puntos, lo que permite dejar disponibles 20 puntos para crecimiento. Sí es necesario recalcar que por temas arquitectónicos, el crecimiento está muy limitado por espacio insuficiente, un tema que podría afectar en este punto es convertir las 2 salas en oficinas para cuatro colaboradores cada una, lo que implicaría solo 2 puntos adicionales; un movimiento de mayor envergadura implicaría la adquisición de más equipos para evitar una nueva saturación.

Esta VLan entregará por DHCP un total de 224 direcciones IP, asumiendo que cada usuario conectará tres equipos por temas de BYOD, que se tienen en cada sala cinco visitantes y las oficinas de los gerentes en reunión, se estima un uso de 120 direcciones, y quedan disponibles alrededor del 46%.

VLan Quinto Piso – ID 405: Esta red entregará direccionamiento de IPs del segmento de red 192.168.50.1, de las cuales las 30 primeras IP (192.168.50.1 - 192.168.50.30) estarán reservadas para las impresoras, APs, Teléfonos IP, Equipos Polycom de Telepresencia y Salas de Reunión, equipos especiales, Bloomberg y cámaras.

El total de puntos de red con conectividad de este piso es de 120, los equipos que se necesita adquirir completan 144 puntos, lo que permite dejar disponibles 24 puntos para crecimiento. Sí es necesario recalcar, al igual que en el cuarto piso, que por temas arquitectónicos, el crecimiento está muy limitado por espacio insuficiente, una variante sería convertir dos de las salas, las pequeñas, en oficinas para cuatro colaboradores cada una, lo que implicaría solo 2 puntos adicionales, un movimiento de mayor envergadura implicaría la adquisición de más equipos para evitar una nueva saturación.

Esta VLan entregará por DHCP un total de 224 direcciones IP, asumiendo que cada usuario conectará tres equipos por temas de BYOD, que se tiene un total de 15 visitantes y las oficinas de los gerentes en reunión, se estima un uso de 221 direcciones, lo que claramente evidencia casi el 100% del consumo. Esto se le resta las oficinas de Alta Dirección ya que se conectan a una red externa y que el *WhatsApp* está bloqueado a nivel del Firewall, lo que previene la conexión de celulares a la red, con esto se limita el acceso de al menos 100 dispositivos. Con esto para el DHCP, se estima desde el punto de vista técnico un consumo de 121 direcciones IP, lo que pretende entregar un 45% del segmento libre de asignación.

Los cálculos de ambos pisos son considerados cuando están llenos en su totalidad, cuestión que no es del todo cierta, ya que existe un movimiento continuo entre los pisos, inclusive en las sedes. Actualmente se presenta un consumo del 98% con refrescamientos del DHCP cada 4 horas, incluso se ha tenido que intervenir el

DHCP y “desconectar” dispositivos del segmento, ya que solo existe un segmento para toda la sede, esta segmentación de los pisos vendría a equiparar la carga.

VLan de Administración – ID 406: Esta red entregará direccionamiento de IPs del segmento de red 172.16.60.1, y será exclusivamente para uso administrativo de los equipos de TI, no será entregada por DHCP, sino que será asignada manualmente a los equipos de comunicación y servidores, limitando el acceso desde las otras VLan y ayudando a limitar el tema de la seguridad informática.

A modo de ejemplo, se detallan los comandos CLI (Interfase de Líneas de Comando) para la creación de una VLan en los equipos Aruba.

(host) (config) #vlan <406>

(host) (config) #interface fastethernet|gigabitethernet <1>/<4>

(host) (config-if) #switchport access vlan <406>

(host) (config) #vlan-name Administracion

(host) (config) #vlan Administracion 406

La otra variante de la infraestructura que se verá manipulada es el caso de los SSID, este es el nombre que recibe la tecnología que ayuda a identificar las redes inalámbricas. Cabe destacar que para que los equipos se comuniquen entre sí de forma inalámbrica, deben pertenecer a un mismo SSID, lo que implica que una red

inalámbrica no tiene acceso a la otra, y de forma resumen un SSID es a la que se le llama comúnmente como nombre de la red.

Desde un tema de requerimiento técnico, los equipos inalámbricos deben controlar un mínimo de seis SSID, aunque para este efecto solo serán utilizadas cuatro distintas redes para un control mayor de los dispositivos, segmentación de cargas y administración de la seguridad, las cuales se detallan a continuación:

SSID 01 = WLEZ: Esta red será la oficial y utilizada por todos los colaboradores de la organización, tendrá factor de autentificación Web del Firewall y sobre esta red trabajarán los perfiles de acceso según el puesto y funciones del colaborador. Esta red será la incluida en la capacitación que TI entrega a los colaborares en su inducción y será anunciada mediante comunicado oficial y documentado en las políticas de TI. Todo miembro de la organización deberá estar conectado a esta red únicamente.

SSID 02 = Visitas: Esta red será la utilizada por las visitas de la organización, tendrá factor de autentificación Web del Firewall, por el cual el único perfil que dará será el de Visitas, con acceso limitado y seguro. Esta red no tendrá comunicación con ninguna otra red de la organización y su contraseña será cambiada por el equipo de TI mínimo una vez a la semana o cuando este lo considere conveniente, en caso de ser antes de los siete días.

SSID 03 = Presidencia: Esta red será la utilizada únicamente por los dueños de la organización, no tendrá factor de autentificación Web del Firewall y perfil Full Acceso a internet. Este SSID es completamente independiente a toda la infraestructura, ya está creado y sale exclusivamente del Firewall, se menciona para temas documentales.

SSID 04 = TI: Esta red será la utilizada únicamente por los colaboradores de TI, estará oculta, con factor de autentificación Web del Firewall y perfil Full Acceso a internet, su función será la de descargar de actualizaciones, programas y paquetes técnicos. Su contraseña será cambiada frecuentemente y tendrá un alto grado de complejidad para que no se dé fácil acceso para los usuarios. El equipo de soporte técnico será el responsable de la misma y velará por su seguridad.

A continuación, se detallan los pasos para la inclusión de una nueva SSID en el GUI (interfaz gráfica de usuario) del Firewall, este funciona como Controlador Inalámbrico de los puntos de acceso inalámbrico AP120 que se pretenden adquirir.

1. En el Firewall, seleccione Red y Controlador Inalámbrico de Puerta de Enlace.
2. En el cuadro de texto Nombre de red (SSID), ingrese el nombre del SSID.
3. Indicar la VLan a distribuir, ya debe estar creada en el switch y DHCP.
4. Agregar Radios de Dispositivo AP, para agregar los dos diferentes radios que se utilizan en los AP120.
5. En la lista desplegable Modo de seguridad, seleccione WPA/WPA2 Enterprise como protocolo de seguridad para utilizar con este SSID.

6. Configurar contraseña.
7. Listo: SSID creado y configurado.

Cabe mencionar que de los switch que se van a adquirir, el que se dedique a interconectar los otros equipos será el que menos dispositivos tenga conectados, esto para ayudarle a evitar saturación y se dedique a la conmutación de la señal de los Puntos de Acceso Inalámbricos y los otros equipos de conmutación. Al igual en el cuarto piso, el equipo más ocioso será el que tenga los dispositivos inalámbricos conectados a él. Estas pequeñas consideraciones minimizan el factor de riesgo en pérdida de paquetes y velocidad de respuesta.

5.2.4 PRESUPUESTO DE SOLUCIONES

El presupuesto a solicitar se divide en tres requerimientos especiales los cuales integran la puesta en marcha total del proyecto, más una variación del +5% para considerar cambios en los precios o inflaciones. De ser aprobado, esto contempla el presupuesto total y será dividido de la siguiente forma.

Compra de insumos tecnológicos: Esta sección se llevará la gran parte del presupuesto y está destinada a la compra de los equipos de redes e inalámbricos, nace de un estudio de diversas cotizaciones y se ajusta a la mejor opción. La necesidad de inversión en este factor asciende a $17 200.

Apoyo Técnico: Esta sección incluye el presupuesto de $850 para adquirir horas del proveedor de los equipos técnicos en caso de necesitar soporte o ayuda a la hora de la configuración.

Insumos y Mano de Obra: Esta sección incluye un presupuesto de $1000 para los costos en cables, conectores y personal para la colocación de los 7 puntos de acceso inalámbrico que el proyecto incluye.

Variación: Se incluye un 5% de variación para tomar en cuenta los imprevistos, alzas o insumos de más que puedan surgir de proyectos como este, y que sirva de amortización en caso de necesidad y no afecte el flujo de caja del proyecto.

En manera de resumen, se detalla la siguiente tabla:

Tabla 15: Presupuesto del proyecto

Detalle	Presupuesto
Compra de insumos tecnológicos	$17 200,00
Apoyo Técnico de Proveedor Experto	$850,00
Insumos y mano de obra para colocación de APs	$1 000,00
Variación del 5%	$950,00
Total	**$20 000,00**

5.3 PLAN PILOTO DE IMPLEMENTACIÓN

A continuación, se tratará de ejemplificar mediante un Plan Piloto la necesidad del proyecto y las mejoras que la red podría obtener en caso de llevarse a cabo la propuesta. En este caso a ejemplificar, se crea un par de VLan ficticias para realizar las pruebas tanto en Cartago como en Escazú y se omitirán datos reales cuando lo amerite, todo para salvaguardar la integridad y seguridad de la organización.

Los equipos a utilizar son un Switch Aruba 2530 de 24 puertos PoE y un Punto de acceso inalámbrico WatchGuard modelo AP200. Este es el utilizado en Cartago y es inferior al que se pretende implementar en Escazú.

5.3.1 ACTIVIDADES PRINCIPALES

Para un correcto dimensionamiento de los alcances de las pruebas a realizar con el Plan Piloto y de los involucrados, es que a continuación se detallan las actividades a realizar en el demo:

- Realizar encuesta de las fallas comunes de la red en Escazú.
- Aplicar encuesta a los funcionarios de soporte técnico.
- Realizar pruebas PING y documentar.
- Configurar Switch Aruba 2530 en Escazú con VLan de pruebas.
- Configurar AP200 con los SSID de Cartago en Escazú.

- Puesta en marcha del Plan Piloto por 2 días en TI y departamento adjunto.
- Aplicar encuesta a los funcionarios de soporte técnico.
- Realizar pruebas PING y documentar.
- Recopilar y resumir la información recolectada.

5.3.2 MATRIZ RACI DE IMPLEMENTACIONES

La siguiente figura referencia y detalla la Matriz RACI de las tareas e involucrados en el Plan Piloto, en donde se destaca la participación de los funcionarios de soporte técnico, el acompañamiento del proveedor interesado en la adquisición de la propuesta y la Gerente de TI, Rosana Acuña.

	Rosana Acuña	Ricardo Pacheco	Jean Carlo Corrales	Jerry Meléndez	Proveedor	Jonathan Cruz
Realizar encuesta de las fallas comunes de la red en Escazú.						RA
Aplicar encuesta a los funcionarios de soporte técnico.	I	R	R	R		RA
Realizar pruebas PING y documentar.						RA
Configurar Switch Aruba 2530 en Escazú con VLan de pruebas.					A	R
Configurar AP200 con los SSID de Cartago en Escazú.					A	R
Puesta en marcha del Plan Piloto por 2 días en TI y departamento adjunto.	I	C	C	C		RA
Aplicar encuesta a los funcionarios de soporte técnico.	I	R	R	R		RA
Realizar pruebas PING y documentar.						RA
Recopilar y resumir información	I					RA

Figura 37: Matriz RACI

Fuente: Diseño propio.

5.3.3 PRUEBAS DE ACEPTACIÓN E INDICADORES

En coordinación con el proveedor se crea un VLan de pruebas y una SSID para configurar los dispositivos en Escazú, dichos dispositivos corresponden a un Switch Aruba 2530 y un punto de acceso inalámbrico WatchGuard AP200. Los trabajos se realizan antes de la puesta en marcha, y queda todo listo para que, el lunes 7 de agosto, los miembros del equipo de soporte técnico conecten los dispositivos a la nueva red.

El Plan de Pruebas a realizar con el proyecto finalizado deberá listar y detallar todas las tareas exactas que se deben realizar y los resultados esperados, así como sus dueños ejecutores. Para esto es vital listar los aplicativos en niveles de prioridad para darle importancia a quien la necesita y no basar las pruebas en aplicativos de poco uso o de poco valor operativo, así como tomar usuarios e involucrarlos en esta fase, darles empoderamiento y que ayuden a recopilar información necesaria.

En el caso del Plan Piloto, se tiene la limitación con el tiempo y disposición del proveedor al ser un demo, por lo cual las pruebas a realizar están reducidas al personal técnico. Esto da valor agregado de usuario ultra experto y su conocimiento de los errores frecuentes, así como al ser más sensibles al cambio.

La zona a cubrir en las pruebas está formada por el área de TI, recepción y un área de la parte comercial de vital valor para la organización, cuya ubicación es la más

próxima a TI, zona idónea para poder realizar las pruebas del caso y estar presentes en momento de fallas o en caso de tener que anular el demo de forma completa.

La primera prueba, para estar presente en la realidad actual y compararla al Plan Piloto, es una encuesta al personal de TI una semana antes del demo, con base en su conocimiento técnico y atención del usuario, donde deben marcar en cada respuesta según el nivel de incidencia, conforme a la siguiente escala de valores:

1	2	3	4
Sin reportes	Menos de 2 reportes	Entre 3 y 5 reportes	Más de 6 reportes

Las preguntas a evaluar son las siguientes seis:

1. ¿Con qué frecuencia los usuarios se deben reautentificar en el Firewall?
2. ¿Con qué frecuencia los usuarios reportan llamadas caídas?
3. ¿Con qué frecuencia los usuarios reportan Skype Empresarial autodesconectado?
4. ¿Con qué frecuencia los usuarios reportan problemas con la calidad de las llamadas en Skype Empresarial?
5. ¿Con qué frecuencia los usuarios reportan la ventana de certificado de Outlook?
6. ¿Con qué frecuencia los usuarios reportan desconexión con SAP?

La encuesta anterior, realizada entre el 31 de julio y el 4 de agosto, arrojó el siguiente resultado que refleja el problema actual de la organización y que los técnicos han logrado resolver al usuario según su incidencia, aunque esto les recorta el tiempo de ejecución de otras tareas.

Antes							
Pregunta	1	2	3	4	5	6	
Calificación	3	2	3	4	2	1	Ricardo Pacheco
	3	2	2	3	3	2	Jerry Meléndez
	4	2	3	2	3	2	Jean Carlo Corrales
Total	10	6	8	9	8	5	46

Mejor Nota	18
Peor Nota	72

Figura 38: Resultados de la encuesta preliminar al Plan Piloto

Fuente: Diseño propio.

Como se observa en la imagen anterior, la nota de la encuesta arroja un 46 que equivale a un 52% de errores. Visto de otra manera, la mitad de los usuarios tuvo al menos un incidente en donde su plataforma tecnológica se vio degradada o afectada.

Durante la ejecución del Plan Piloto, se prestó principal atención a los mismos problemas para evaluar una disminución de incidentes y el comportamiento de la red provisional, así como la satisfacción del usuario final y del mismo departamento de soporte técnico, ya que una disminución en su tiempo dedicado a la atención de estos casos se traduce en proactividad y beneficios a la organización.

Plan Piloto							
Pregunta	1	2	3	4	5	6	
Calificación	1	1	1	2	1	1	Ricardo Pacheco
	2	1	1	1	1	1	Jerry Meléndez
	1	1	1	1	1	1	Jean Carlo Corrales
Total	4	3	3	4	3	3	20

Mejor Nota	18
Peor Nota	72

Figura 39: Resultados de la encuesta preliminar al Plan Piloto

Fuente: Diseño propio.

Como se observa a detalle en la imagen anterior, solo se presentaron mínimos errores en la autentificación del Firewall y en la calidad de las llamadas, que pueden ser causados por otros factores que no se trató de desarrollar ya que solo representan una incidencia de errores del 4% durante los dos días que duró el demo. Esto no significa que no sean importantes, solo que aún con esos errores, no tiene representación en los indicadores de soporte técnico.

La evaluación de las encuestas a nivel de soporte técnico arroja como resultado una mejora realmente significativa en la estabilidad de la red, y logra disminuir los incidentes de un 52% a un 4%. Al tener a los técnicos dedicados en esta labor, filtra significativamente errores que no tienen relevancia con la red y que pueden ser causados por temas de equipo, traslado, reinicio y demás factores que pueden generar una percepción de problemas de red, aunque no sea el caso.

Una segunda ronda de pruebas, aunque en paralelo, se realizan mediante el comando PING, normalmente este término corresponde al acrónimo de *Packet Internet Groper* y hace referencia a “Buscador o rastreador de paquetes en redes”. Este comando corresponde a MS-DOS y es utilizado para diagnosticar el estado de la comunicación que existe entre el *host* (equipo desde donde se realiza la prueba) y el equipo remoto, es este caso el Firewall que es el último punto de la red antes de salir a Internet.

En el caso en particular de las pruebas realizadas, al ejecutar un Ping de solicitud, el equipo local envía al Firewall un mensaje ICMP (Protocolo de mensajes de control de Internet) que se le llama comúnmente paquete. Estos mensajes funcionan a modo de eco, nacen de la funcionalidad de un sonar de submarino, y determinan si el equipo remoto está activo o no, y a su vez, y lo que nos compete en esta prueba, el tiempo que tarda el mensaje en llagar hasta el Firewall. Este tiempo nos indica la estabilidad de la red, ya que entre menor sea el tiempo de la respuesta, significa que el paquete fluyó de forma más rápida por la red, y una red rápida es una red estable.

Antes de presentar los resultados de las pruebas, se detalla el equipo utilizado en la ejecución de las mismas, para evidenciar la capacidad de ejecución:

Marca: Dell, Modelo: Mobile Precision 5510, Procesador: Intel Core i7-6820HQ, Memoria: 16Gb, Disco Duro: 256Gb SSD, Red: Intel WiFi Link 8260 2x2 802.11ac, Video: Nvidia Quadro M1000M 2GB GDDR5, Win 10 Pro 64 Bits.

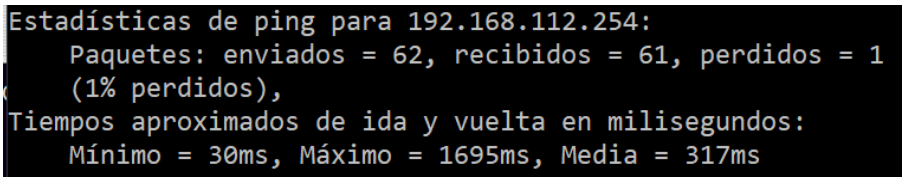
A continuación, se detallan las pruebas Ping realizadas. Todas las pruebas se ejecutan desde el mismo equipo, anteriormente descrito, y conectado a la red dependiendo del objetivo a analizar. En cada imagen se detalla las características de las conexiones y a cuál equipo se realizó la prueba, ya que es necesario probar tanto al equipo interno, como el externo al otro lado del VPN, esto debido a que virtualmente existe una conexión entre Cartago y Escazú. Ambos sitios comparten una misma red por la cantidad de servicios alojados en la DataCenter de Cartago y que son compartidos, por ejemplo la telefonía.

Este primer segmento de pruebas realizadas es desde la red normal de SteinCorp en su sede de Escazú, se hizo el martes 8 de agosto del 2017. De una forma simple, consiste en conectar el equipo en diferentes áreas del quinto y cuarto piso, tanto en la red inalámbrica como en la alámbrica. De esta forma se logra evaluar el funcionamiento en un momento dado en diferentes zonas que están conectas al DataCenter de Escazú de diferente forma.

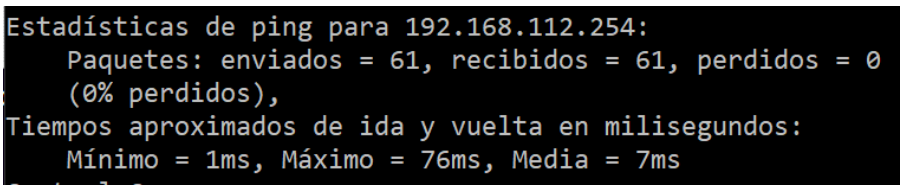
Tanto de forma inalámbrica o alámbrica, y desde varias oficinas, se ejecutan comandos Ping al Firewall de Escazú (Local) y Cartago (conectado vía VPN entre Firewalls) con un promedio de 58 paquetes por prueba. Esto nos dará un promedio que se llama Media, este número indica el promedio en milisegundos que dura el paquete en llegar al equipo al cual se está enviando el paquete. Entre más cerca está la Media a cero, más rápida y eficiente es la red.

Otros indicadores son los valores de Mínimo, que es el tiempo, en milisegundos, en que el paquete recibió la respuesta más rápida y el otro indicador es el Máximo, que a diferencia es la duración más extensa en que se recibió respuesta, igual en milisegundos. También es importante apreciar cuando se pierden paquetes, ya sean enviados o recibidos, esto es por tiempo de espera excedido o paquete perdido en la comunicación, por lo general son síntomas de errores en la comunicación.

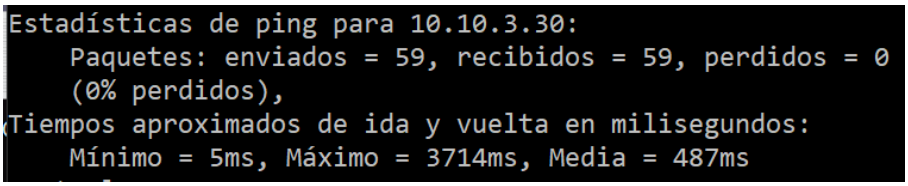
Desde: Departamento Legal, 5to piso



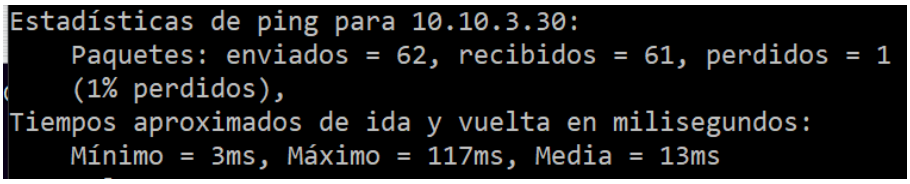
WiFi - Escazú



LAN - Escazú



Wi Fi - Hasta Cartago



LAN - Hasta Cartago

Se evidencia una alta latencia en los tiempos de comunicación, el máximo fue de 3714 milisegundos entre Escazú y Cartago conectado por Wi Fi.

Desde: Departamento de RRHH, 5to piso

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 52, recibidos = 52, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 3ms, Máximo = 120ms, Media = 27ms
```

Wi Fi - Escazú

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 60, recibidos = 60, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 113ms, Media = 3ms
```

LAN - Escazú

```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 59, recibidos = 59, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 3ms, Máximo = 539ms, Media = 87ms
```

Wi Fi - Hasta Cartago

```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 58, recibidos = 58, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 77ms, Media = 7ms
```

LAN - Hasta Cartago

Se evidencia una alta latencia en los tiempos de comunicación, el máximo fue de 539 milisegundos entre Escazú y Cartago conectado por Wi Fi.

Desde: Departamento de Tesorería, 4to piso

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 60, recibidos = 60, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 640ms, Media = 80ms
```

Wi Fi - Escazú

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 57, recibidos = 57, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 12ms, Media = 3ms
```

LAN - Escazú

```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 59, recibidos = 59, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 3ms, Máximo = 539ms, Media = 87ms
```

Wi Fi - Hasta Cartago

```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 59, recibidos = 59, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 3ms, Máximo = 20ms, Media = 5ms
```

LAN - Hasta Cartago

Se evidencia una alta latencia en los tiempos de comunicación, el máximo fue de 640 milisegundos dentro de la red interna conectado por Wi Fi.

Desde: Departamento de Procurement, 4to piso

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 60, recibidos = 58, perdidos = 2
    (3% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1884ms, Media = 99ms
```

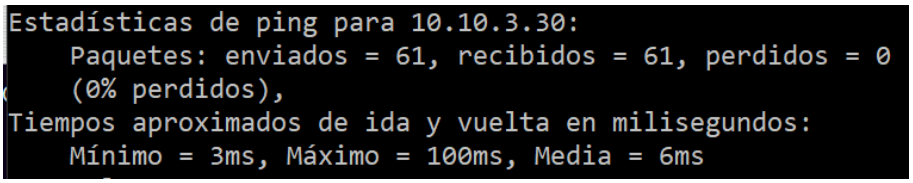
Wi Fi - Escazú

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 60, recibidos = 60, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 113ms, Media = 3ms
```

LAN - Escazú

```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 61, recibidos = 61, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 3ms, Máximo = 2810ms, Media = 186ms
```

Wi Fi - Hasta Cartago



LAN - Hasta Cartago

Se evidencia una alta latencia en los tiempos de comunicación, el máximo fue de 2810 milisegundos dentro de la red interna conectado por Wi Fi.

Las pruebas anteriores cierran las que se efectúan en la red de la organización. Las pruebas que se ejecutan a continuación son realizadas dentro de la red DEMO del Plan Piloto, ejecutado en SteinCorp en su sede de Escazú, el martes 8 de agosto del 2017.

Como se detalló al inicio de estas pruebas, el objetivo es medir la Media en milisegundos de la transmisión de datos. La prueba a continuación, conectada a un punto de acceso inalámbrico y este a un switch conectado al Firewall de Escazú, o directamente conectada al switch por medio de cable, es la emulación de la configuración de los equipos si la presente propuesta se lleva a cabo y se ejecuta. Esta emulación implicó la creación de VLan y SSID nuevos para una verificación más realista ante una posible implementación real.

Estas pruebas se realizarán de la misma forma que las anteriores, la única variante son las oficinas involucradas que, por temas de equipos y cercanía, varían de las otras. Por temas estratégicos, una de las dos zonas a probar el demo es el área de

TI, ya que en este departamento hay un alto consumo de datos y de comunicación con la sede de Cartago.

Desde: Departamento de TI, 5to piso

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 53, recibidos = 53, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 10ms, Media = 3ms
```

Wi Fi - Escazú

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 58, recibidos = 58, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms
```

LAN - Escazú

```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 52, recibidos = 52, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 85ms, Media = 5ms
```

Wi Fi - Hasta Cartago

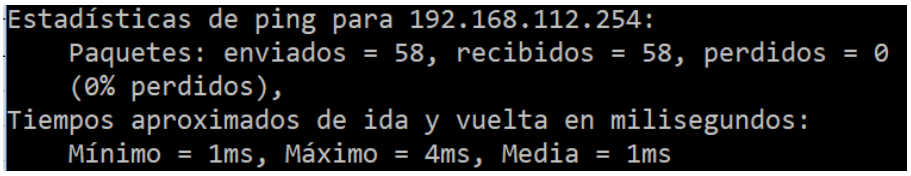
```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 53, recibidos = 53, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 6ms, Media = 2ms
```

LAN - Hasta Cartago

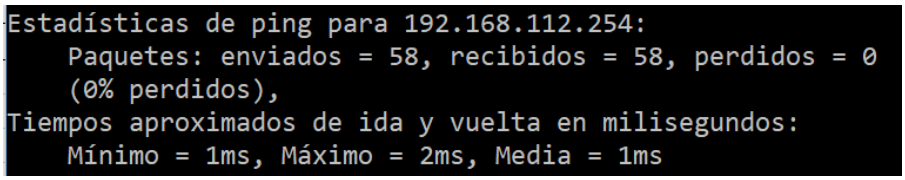
Se evidencia que la latencia disminuyó, no hay pérdida de paquetes y la Máxima fue de 85 milisegundos conectados por Wi Fi y comunicándose hasta Cartago, aunque la media indicó solo 5 milisegundos. Es notable la diferencia con estos equipos de Demo en comparación a los ya descritos e instalados en Cartago.

La segunda zona a probar el demo es el área de Comercial, este departamento tiene un alto consumo de la red por el uso de la telefonía y tener la mayor parte de sus documentos y procesos en SharePoint.

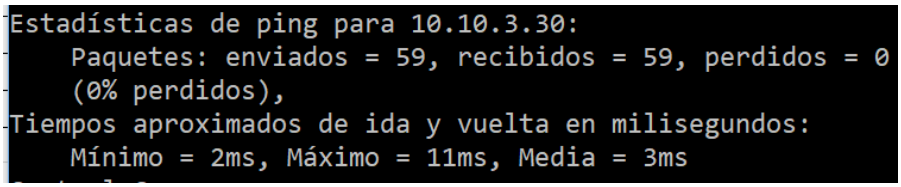
Desde: Departamento Comercial, 5to piso



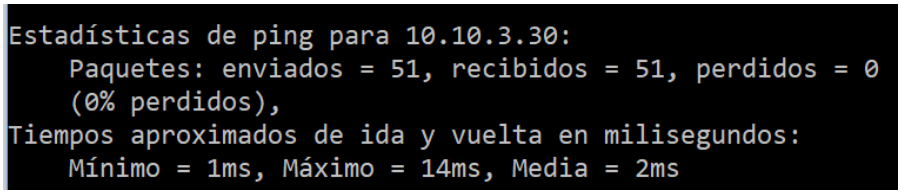
Wi Fi - Escazú



LAN - Escazú



Wi Fi - Hasta Cartago



LAN - Hasta Cartago

Al igual que las pruebas en la zona de TI, en esta se evidencia que la latencia disminuyó, no hay pérdida de paquetes y la Máxima fue de 14 milisegundos conectados por LAN y comunicándose hasta Cartago. La media indicó solo 2 milisegundos, lo que consolida esta propuesta como un proyecto viable.

A modo conclusión, desde un punto de vista de factor humano, la encuesta reflejó que el personal técnico notó una evidente mejoría en la red y disminución de reportes en temas de redes, y desde el punto técnico, las pruebas con Ping evidencian una mejoría radical en los tiempos de respuesta de los paquetes. Ambas pruebas resultaron satisfactorias y evidencian el éxito en caso de que esta propuesta sea llevada a cabo.

El martes 8 de agosto, después de las 5pm se apagan y retiran los equipos del Plan Piloto.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES DEL PROYECTO

6.1 CONCLUSIONES

Para las conclusiones de la presenta propuesta de proyecto, se inicia por el objetivo general y se continúa según cada uno de los objetivos específicos anteriormente desarrollados según la fase de acción o ejecución.

- Proponer la arquitectura de red de comunicaciones de la empresa SteinCorp en Escazú para su homologación con la red de la sede central en Cartago.

Se concluye de forma general la realidad de una urgente homologación de las redes de comunicaciones de ambos sitios, y que dará a la organización estabilidad interna a nivel de comunicaciones y competitividad en el mundo tecnológico actual, sobre todo al comparar a sus grandes competidoras como Pfizer, Glaxo-SmithKline y Gutis, entre otras. Esta necesidad se desarrolla desde dos aristas de suma importancia.

El primer factor es por temas completamente técnicos, donde se evidencia la brecha tecnológica de la sede de Escazú, no solo con su red principal, sino con los estándares internaciones y funcionalidad básica. La confianza del departamento de TI sobre esta red de Escazú está degradada y son conscientes de la urgencia de una remodelación tecnológica, ya que sus esfuerzos para estabilizar los temas de proveedores de Internet y seguridad perimetral, así como ir a la vanguardia a nivel

nacional con la reciente implementación del CloudPBX de Office 365, no están siendo explotados en su máximo potencial por las deficientes comunicaciones de esta sede.

Igual de importante es el segundo factor, el nivel de competitividad nacional e internacional. La ejecución de este proyecto presenta una comunicación, tanto en datos como en voz, así mismo con el exterior de la sede, lo que traerá como resultado efectividad de los colaboradores y comunicaciones sólidas con los proveedores, sedes regionales y nuevos mercados que se están tratando de abrir a nivel mundial. A su vez provee de comunicaciones fluidas con los proveedores internacionales que le dan valor a la organización a nivel de investigación y tecnología a nivel farmacéutico.

Como conclusiones de los objetivos específicos se desarrollan los siguientes puntos, que juntos, le dan la razón a la conclusión general ya descrita.

- Diagnosticar la situación actual de la red de comunicaciones de la empresa en su sede de Escazú evaluando los equipos existentes para la definición de las brechas a nivel técnico y operativo.

Se concluye como consecuencia del diagnóstico que la actual red de comunicaciones de la organización en su sede de Escazú se encuentra obsoleta y con grandes deficiencias técnicas, que su mal dimensionamiento inicial trae en la actualidad grandes problemas de latencia, que sumados al día a día y las prestaciones que la sede administrativa consume, esta red no da la calidad requerida para cumplir con las funciones y necesidades de la sede.

Las grandes deficiencias técnicas de esta sede elevan el consumo de presupuesto por temas de mantenimiento, y el personal técnico debe consumir tiempo valioso en estar dando soporte por temas recurrentes a consecuencia de esta infraestructura obsoleta y sin soporte por parte de la marca implementadora, a consecuencia de que los dispositivos se encuentran fuera de garantía. Adicionalmente se tiene la problemática de que, en un lapso de 2 años, dos proveedores fueron destituidos por su mal servicio proactivo.

- Establecer los requerimientos que la empresa necesita evaluando proveedores y alcances para la identificación de los equipos de su nueva red de comunicaciones en la sede de Escazú.

A nivel de switchs o conmutadores, se concluye que la mejor opción es seguir trabajando con los equipos Aruba 2530 ya implementados en la sede de Cartago y en países como Panamá y República Dominicana, al ser de la misma gama a nivel de red facilita la administración; además de que el personal técnico ya se encuentra capacitado, por ende la curva de aprendizaje es nula. Esa misma experiencia da la confianza al departamento de adquirir equipos funcionales, inversión justa por los equipos adquiridos. Por último, su administración web facilita el acceso remoto en caso de que el dispositivo necesite soporte, lo que facilita en gran medida la función del personal técnico.

Con respecto a los puntos de acceso inalámbrico, se concluye que la mejor opción en calidad, confianza y costos es seguir trabajando con los equipos que la marca WatchGuard ofrece, solamente que en lugar de seguir trabajando con los modelos AP200 que se han utilizado los últimos dos años, se da un avance en tecnología y esta propuesta determina que los modelos AP120 son los que la organización necesita para poder brindar un red inalámbrica de calidad, robusta y que satisfaga los requerimientos de comunicación que se necesita. Esta facilita la administración, no incluye curva de aprendizaje y limita de carga de procesos a equipos de seguridad perimetral.

Un factor determinante para la toma de decisión es el acompañamiento de un proveedor experto, por lo que esta propuesta es contundente en seleccionar a Tecnova S.A. como la empresa responsable en brindar el acompañamiento en la futura implementación de red. Esto como consecuencia de la evaluación de cotizaciones, donde esta empresa fue la mejor oferta presentada, y por su gran experiencia en la organización, pues es la que ha acompañado al departamento de TI en la puesta en marcha de todos los cambios a nivel de redes. Lo anterior ha generado amplio conocimiento en cómo funciona las conexiones internas, VLan, telefonía, sedes, hosting y demás participantes de las comunicaciones, esto le da valor a la implementación, reduce los riesgos que podrían ocurrir por la inexperiencia y le entrega confianza a los miembros del equipo de TI.

En resumen, este punto concluye que los equipos de la sede deben ser reemplazados en su totalidad y entrega los modelos de los equipos, así como el proveedor idóneo para la implementación, con un presupuesto específico y alcanzable.

- Diseñar la arquitectura necesaria estimando los requerimientos con el diagnóstico para un dimensionamiento real de la nueva red de comunicaciones de le empresa en su sede de Escazú.

Se define la infraestructura requerida para llevar con éxito el proyecto, la cual especifica las conexiones de los 4 equipos de conmutación y su respectivo control de carga de los dispositivos, y se logra así no saturar a los equipos de procesos. Adicionalmente se indica la ubicación de los puntos de acceso inalámbrico en ambos pisos de la sede de Escazú, esto concluye la infraestructura idónea en la cual se podrá llevar a cabo una implementación exitosa, que es el resultado del análisis de factores como cantidad de usuarios, funciones de los departamentos, áreas de alto y bajo trasiego de datos informáticos. Se logra entregar un diseño definitivo de la red, producido a la medida para la organización, donde hasta los detalles mínimos han sido tomados en cuenta para entregar un resultado claro e inobjetable.

Como conclusión, se entrega un diseño de red lógico basándose en la cantidad de conexiones actuales más un crecimiento del 15% ajustado a la infraestructura arquitectónica, que no permite una expansión mayor, y gracias a los diseños que la

constructora de la organización facilita, se entrega la ubicación de los dispositivos inalámbricos en puntos reales gracias a las cotas del plano, para ofrecer un “mapa de calor” real, eficiente y sin sobredimensionar, que evite gastos innecesarios.

- Establecer un plan piloto comparando la situación actual de la red con la diseñada en esta propuesta para demostrar la necesidad del proyecto en SteinCorp de su sede de Escazú.

Todos los objetivos son importantes, pero este es contundente, ya que traduce la prosa de este documento en una realidad cuantificable, al evidenciar con datos la definitiva necesidad de la ejecución de la propuesta.

En conclusión, la organización necesita cuanto antes la aprobación y puesta en marcha de este proyecto, los resultados de las encuestas al personal técnico son contundentes, en el hecho de la cantidad de tiempo invertido por ellos en la solución de problemas, causados por temas de red. Se logra identificar una diferencia superior en comparación, inclusive, a otros trabajos, a esto se le incluye las pruebas técnicas que evidencian problemas reales de latencia y pérdida de paquetes, que se traducen en una ineficiente experiencia del usuario. Esto genera esto inconformidad, produce quejas a las gerencias y de forma directa afecta la imagen y función del departamento de TI.

Es rotunda la necesidad de este proyecto, se tiene claro cuáles son los procesos, los equipos necesarios, el proveedor participante y la forma de ejecutarlo. El diseño de la red es definitivo y sin duda resolutivo a toda la problemática descrita y cotidiana en la organización, así como es determinante obtener el presupuesto para la ejecución cuanto antes de la implementación, que al final será traducida en efectividad.

6.2 RECOMENDACIONES

Como recomendaciones a la organización, se enumeran las siguientes, para su análisis y consideración:

1. Se recomienda la exigencia a todo departamento de la organización, en caso de presentar algún proyecto que incluye tecnología, a sus respectivas direcciones, contar con la debida autorización o aval del Departamento de TI.

2. Se recomienda la capacitación a todos los usuarios de equipo informático, capacitaciones en temas de seguridad informática.

3. Se recomienda una comunicación efectiva con las jefaturas y gerencias en los temas de informática, así como nuevos proyectos a ejecutar, el fin es lograr una unificación de fuerzas.

4. Se recomienda, a nivel de gestión del software, la elaboración de un documento para la realización de pruebas con los alcances definidos por los usuarios

solicitantes, así tener claro los requisitos y que el usuario firme su respectivo recibido.

5. Se recomienda la creación de un DRP y BCP para la plataforma informática de TI.

6. Se recomienda una capacitación técnica avanzada a los miembros de soporte técnico en equipos Aruba.

7. Se recomienda la donación de los equipos obsoletos a Colegios Técnicos.

CAPÍTULO VII

BIBLIOGRAFÍA

REFERENCIAS BIBLIOGRÁFICAS

Aguilera López, Purificación (2011). Seguridad Informática. Madrid: Editex.

Alonso, L. y Arévalo, D. (2013). Diseño Técnico de laboratorio de Redes y Seguridad para Universidad Minuto de Dios Centro Regional Soacha. (Proyecto de Graduación). Universidad Minuto de Dios, Bogotá, Colombia.

Amaya, J. (2010). Sistemas de Información. 2ª ed. Bogotá: Ecoe Ediciones

Andreu, J. (2010). Servicios de Red. Madrid: Editex.

Aparicio Colis, A. (2015). Conceptualización, diseño e implementación de infraestructura de red. (Tesis inédita de Ingeniería Informática). Universidad de la Rioja, La Rioja, España.

Barbancho, J. y Benjumea, J. (2014) Redes Locales. España: Ed. Paraninfo.

Barragán, J. (2012). ¿Qué es ethernet? Disponible en: http://uhu.es/antonio.barragan/content/ethernet

Caccuri, V. (2012). Computación para docentes. 1ª ed. Buenos Aires: Fox Andina; Dálaga.

Cardona Benítez, J. (2014). Fortalecimiento y actualización de la Infraestructura Tecnológica del Ministerio de Hacienda (Proyecto). Ministerio de Hacienda, Gobierno de Costa Rica.

Castro, A. (2013). Comunicaciones - una introducción a las redes digitales de transmisión de datos y señales isócronas. Buenos Aires: Alfaomega.

Cnet ®. (2015). WatchGuard AP200 - wireless access point Overview. Disponible en: https://www.cnet.com/es/analisis/watchguard-ap200-wireless-access-point-wg002503

Cnet ®. (2015). WatchGuard AP200. Disponible en: https://www.cnet.com/es/analisis/watchguard-ap200-wireless-access-point-wg002503

Dans, E. (2009). Todo va a cambiar. Barcelona: Deusto Ediciones.

Díaz, G. (2015). Introducción a las Redes de Computadoras. Disponible en: http://webdelprofesor.ula.ve/ingenieria/gilberto/redes/02_introduccion.pdf

Dordoigne, J. (2015). Redes informáticas - Nociones fundamentales. 5ª ed. Barcelona: Ed. ENI.

Flickernger, R. (2008). Redes inalámbricas en los países en desarrollo: una guía práctica para planificar y construir infraestructuras de telecomunicaciones de bajo costo. 3ª ed. Gran Bretaña: Hacker Friendly LLC.

Forouzan, A. (2007). Transmisión de datos y redes de comunicaciones. 4ª ed. Madrid: McGraw-Hill.

Galindo, J. (2010), Escaneando la informática, Reimpresa, España: Editorial UOC.

Gallego, J. (2015). FPB - Instalación y mantenimiento de redes para transmisión de datos. España: Editex.

García León, C. y Toro Barrientos, C. (2013). Diseño e implementación de la red de voz y datos del proyecto call center torre central piso 8. (Tesis inédita de Tecnólogo en Electricidad). Universidad Tecnológica de Pereira, Pereira, Colombia.

García, A. (2007). CIM: El computador en la automatización de la producción, España, Universidad de Castilla – La Mancha.

Gestión. (2015). El 87% de empresas considera que la falta de compromiso laboral es su principal problema. Disponible en: http://gestion.pe/empleo-management/87-empresas-considera-que-falta-compromiso-laboral-su-principal-problema-2149055

Gido, J. y Clements, J. (2012). Administración exitosa de proyectos. 5ª ed. México D.F.: Cengage Learning.

GmbH, T. (2016). Actualización de redes para satisfacer las necesidades empresariales y de seguridad de hoy en día. Obtenido de: https://www.t-systems.com/es/es/soluciones/telecomunicaciones/redes-de-area-local-lan-y-redes-de-area-amplia-wan--203786

Godínez Benavides, Johel. (2013). Diseño e Implementación de una red de Comunicaciones Unificada utilizando VDI y Presencia. (Proyecto de Graduación para grado académico de Licenciatura como Ingeniero en Electrónica). Instituto Tecnológico de Costa Rica, Cartago, Costa Rica.

González Vallejo, L. (2012). Competencias Universales y su impacto en el curso de Técnicas de Comunicación, alumnos de primer ingreso UH. (Tesis inédita de Doctorado). Universidad Hispanoamericana, San José, Costa Rica.

Hallberg, B. (2007). Fundamentos de redes. 4ª ed. México, DF: McGraw-Hill.

HPE ®. (2013). Save up to 50% with the HP. Disponible en: http://usnew.ingrammicro.com/Documents/vendors/h/hp/switch_flyer2530_85x11_Hires.pdf

HPE ®. (2016). Serie de conmutadores 2530. Disponible en: https://www.hpe.com/mx/es/product-catalog/networking/networking-switches/pip.5333803.html

Kurose, J. (2010). Redes de Computadoras: un enfoque descendente. 5ª ed. Madrid: Pearson.

Microsoft ®. (2013). Definición de las siete capas del modelo OSI y explicación de las funciones. Disponible en: https://support.microsoft.com/es-es/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained

Microsoft ®. (2016). Procedimientos para usar Office-365. Disponible en: https://support.office.com/es-es/article/Procedimientos-recomendados-para-usar-Office-365-en-una-red-lenta-fd16c8d2-4799-4c39-8fd7-045f0664016

Microsoft ®. (2016). Solucionar problemas de conexión. Disponible en: https://support.microsoft.com/es-do/help/10741/windows-10-fix-network-connection-issues

Moro, V. (2013). Infraestructuras de redes de datos y sistemas de telefonía. Madrid: Paraninfo.

Muñoz, C. (2002). Auditoria en sistemas computacionales. México: Pearson.

NIETO, M., Galliani, R. (2017). Cómo citar y referenciar páginas web con normas APA. Disponible en: http://normasapa.com/como-citar-referenciar-paginas-web-con-normas-apa

Núñez, G. y Mesa, J. (2014). Diseño de la infraestructura de telecomunicaciones para la operación de un IP Contact Center para la Universidad de San Buenaventura (Proyecto de Grado presentado para optar para el título de Ingeniería de Telecomunicaciones). Universidad de San Buenaventura, Bogotá, Colombia

Oricom Internet Inc. (2017). Connection Diagram for DSL Módem, Cable Módem and VoIP Gateway. Disponible en: https://www.oricom.ca/en/support/connection-diagram-for-dsl-modem,-cable-modem-and-voip-gateway/

Oz, E. (2008). Administración de los sistemas de información. 5ª ed. México D.F.: Thomson

Palmer, M. (2000). Redes informáticas: Guía práctica. España: Ed. Paraninfo.

Porras, A. (2015). Acerca de Nosotros. Disponible en: http://10.10.3.60/intranet/?p=539

Porras, A. (2015). Misión, Visión y valores. Disponible en: http://10.10.3.60/intranet/?p=527

Román Acuña, A. (2001). Diseño de un modelo lógico y su plan de migración para la reestructuración de la red de la SUGEF. (Informe de Proyecto de Graduación). Instituto Tecnológico de Costa Rica, Cartago, Costa Rica.

Rujavi. (2009). Wi-Max. Disponible en: https://rubenja.wordpress.com

Stallings, W. (2004). Comunicaciones y redes de computadores. 7ª ed. Madrid: Pearson Educación.

Stallings, W. (2004). Fundamentos de seguridad en redes. Aplicaciones y estándares. 2ª ed. Madrid: Pearson.

Tanenbaum, A. (2003). Redes de computadoras. 4ª ed. México: Prentice-Hall.

Taveras, B. (2013). Propuesta de Diseño e Implementación de la Red Wi-Fi del Campus

Universitario UCNE. República Dominicana: GRIN Verlag.

Toro, F. (2013). Administración de proyectos de informática. Bogotá: Ecoe Ediciones.

Torres. G (2014). Redes de computadoras. 2ª ed. Rio de Janeiro: Novaterra.

Vieira, C. (2016). WatchGuard reinventa la gestión de las amenazas persistentes avanzadas con el lanzamiento de WatchGuard APT Blocker. Disponible en: http://www.watchguard.com/es/wgrd-international/news-events/press-releases/watchguard-technologies-reinventa-la-gestion-de-las

WatchGuard ® (2016). Porqué comprar WatchGuard. Disponible en: http://www.watchguard.com/wgrd-about/why-buy-red

WatchGuard ®. (2013). WatchGuard XTM, hoja de datos. Disponible en: https://www.watchguard.com/docs/datasheet/wg_xtm5_ds_es.pdf

WatchGuard ®. (2016). Puntos de Acceso Inalámbrico. Disponible en: https://www.watchguard.com/docs/datasheet/wg_access-point_ds_es.pdf

Web Master. (2016). La Organización. Disponible en: http://www.labstein.com/laorganizacion/

Web Master. (2016). Sobre Nosotros. Disponible en: http://www.labstein.com/sobre-nosotros/

Web Master. (2016). Visión de futuro. Disponible en: http://www.labstein.com/vision-de-futuro/

CAPÍTULO VIII

APÉNDICES

8.1 Apéndice I. Carta de Aprobación

STEINCORP

7 de noviembre, 2016
San José, Costa Rica

Facultad de Ingeniería
Dirección Escuela de Ingeniería Informatica.
Universidad Hispanoamericana.
A quien interese:

Por medio de la presente, hago constar en mi potestad de Gerente de Tecnologías de Información de SteinCorp, que Jonathan Cruz Hidalgo posee completa autorización para realizar el proyecto de graduación "*Propuesta de la arquitectura de la red de comunicaciones de la empresa SteinCorp en Escazú para su homologación con la red de la sede central en Cartago, aplicando métodos de diseño de redes*" en nuestras oficinas, dicho proyecto es de suma importancia, ya que presenta grandes retos y la finalidad del mismo es entregarle valor a la organización.

Debo de recalcar que el rol de participación de Jonathan en la propuesta será el de líder y dueño, siendo este proyecto total responsabilidad de su persona y se espera como resultado una propuesta realizable y de agrado a Gerencia Financiera para una futura implementación.

Sin más por el momento, agradezco la atención brindada a la misma.

STEIN

Rosana Acuña Ostos
Ced.: 186200202207
Gerente de TI
SteinCorp

Laboratorios Stein, una compañía de Stein Corp. - Cartago - Costa Rica
Teléfonos: 2550 6500 - 2550 6565 Fax: (506) 2550-6552
Correo Postal: 930-1007 Centro Colón, San José Costa Rica.
Correo electrónico: cliente@labstein.com

Encuesta sobre servicio y errores comunes

Del 31de julio al 4 de agosto

Técnico: Jean Carlo Corrales

Basados en su conocimiento técnico y atención del usuario, por favor marque cada respuesta según su nivel de incidencia, con forme a la siguiente escala de valores, donde:

1	2	3	4
sin reportes	menos de 2 reportes	Entre 3 y 5 reportes	Mas de 6 reportes

1. ¿Con que frecuencia los usuarios se deben de re-autentificar en el Firewall?

1	2	3	4
			X

2. ¿Con que frecuencia los usuarios reportan llamadas caídas?

1	2	3	4
	X		

Propuesta de Proyecto
Nueva red de Telecomunicaciones de SteinCorp Escazú
Plan Piloto

3. ¿Con que frecuencia los usuarios reportan Skype Empresarial auto-desconectado?

1	2	3	4
		X	

4. ¿Con que frecuencia los usuarios reportan problemas con la calidad de las llamadas en Skype Empresarial?

1	2	3	4
	X		

5. ¿Con que frecuencia los usuarios reportan la ventana de certificado de Outlook?

1	2	3	4
		X	

6. ¿Con que frecuencia los usuarios reportan desconexión con SAP?

1	2	3	4
	X		

8.2 Apéndice II. Encuestas

Encuesta sobre servicio y errores comunes

7 y 8 de agosto

Técnico: Jean Carlo Corrales

Basados en su conocimiento técnico y atención del usuario, por favor marque cada respuesta según su nivel de incidencia, con forme a la siguiente escala de valores, donde:

1	2	3	4
sin reportes	menos de 2 reportes	Entre 3 y 5 reportes	Mas de 6 reportes

1. ¿Con que frecuencia los usuarios se deben de re-autentificar en el Firewall?

1	2	3	4
X			

2. ¿Con que frecuencia los usuarios reportan llamadas caídas?

1	2	3	4
X			

Propuesta de Proyecto
Nueva red de Telecomunicaciones de SteinCorp Escazú
Plan Piloto

3. ¿Con que frecuencia los usuarios reportan Skype Empresarial auto-desconectado?

1	2	3	4
X			

4. ¿Con que frecuencia los usuarios reportan problemas con la calidad de las llamadas en Skype Empresarial?

1	2	3	4
X			

5. ¿Con que frecuencia los usuarios reportan la ventana de certificado de Outlook?

1	2	3	4
X			

6. ¿Con que frecuencia los usuarios reportan desconexión con SAP?

1	2	3	4
X			

Encuesta sobre servicio y errores comunes

Del 31de julio al 4 de agosto

Técnico: Jerry Meléndez

Basados en su conocimiento técnico y atención del usuario, por favor marque cada respuesta según su nivel de incidencia, con forme a la siguiente escala de valores, donde:

1	2	3	4
sin reportes	menos de 2 reportes	Entre 3 y 5 reportes	Mas de 6 reportes

1. ¿Con que frecuencia los usuarios se deben de re-autentificar en el Firewall?

1	2	3	4
		X	

2. ¿Con que frecuencia los usuarios reportan llamadas caídas?

1	2	3	4
	X		

Propuesta de Proyecto
Nueva red de Telecomunicaciones de SteinCorp Escazú
Plan Piloto

3. ¿Con que frecuencia los usuarios reportan Skype Empresarial auto-desconectado?

1	2	3	4
	X		

4. ¿Con que frecuencia los usuarios reportan problemas con la calidad de las llamadas en Skype Empresarial?

1	2	3	4
		X	

5. ¿Con que frecuencia los usuarios reportan la ventana de certificado de Outlook?

1	2	3	4
		X	

6. ¿Con que frecuencia los usuarios reportan desconexión con SAP?

1	2	3	4
	X		

Encuesta sobre servicio y errores comunes

7 y 8 de agosto

Técnico: Jerry Meléndez

Basados en su conocimiento técnico y atención del usuario, por favor marque cada respuesta según su nivel de incidencia, con forme a la siguiente escala de valores, donde:

1	2	3	4
sin reportes	menos de 2 reportes	Entre 3 y 5 reportes	Mas de 6 reportes

1. ¿Con que frecuencia los usuarios se deben de re-autentificar en el Firewall?

1	2	3	4
	X		

2. ¿Con que frecuencia los usuarios reportan llamadas caídas?

1	2	3	4
X			

Propuesta de Proyecto
Nueva red de Telecomunicaciones de SteinCorp Escazú
Plan Piloto

3. ¿Con que frecuencia los usuarios reportan Skype Empresarial auto-desconectado?

1	2	3	4
X			

4. ¿Con que frecuencia los usuarios reportan problemas con la calidad de las llamadas en Skype Empresarial?

1	2	3	4
X			

5. ¿Con que frecuencia los usuarios reportan la ventana de certificado de Outlook?

1	2	3	4
X			

6. ¿Con que frecuencia los usuarios reportan desconexión con SAP?

1	2	3	4
X			

Encuesta sobre servicio y errores comunes

Del 31de julio al 4 de agosto

Técnico: Ricardo Pacheco

Basados en su conocimiento técnico y atención del usuario, por favor marque cada respuesta según su nivel de incidencia, con forme a la siguiente escala de valores, donde:

1	2	3	4
sin reportes	menos de 2 reportes	Entre 3 y 5 reportes	Mas de 6 reportes

1. ¿Con que frecuencia los usuarios se deben de re-autentificar en el Firewall?

1	2	3	4
		X	

2. ¿Con que frecuencia los usuarios reportan llamadas caídas?

1	2	3	4
	X		

Propuesta de Proyecto
Nueva red de Telecomunicaciones de SteinCorp Escazú
Plan Piloto

3. ¿Con que frecuencia los usuarios reportan Skype Empresarial auto-desconectado?

1	2	3	4
		X	

4. ¿Con que frecuencia los usuarios reportan problemas con la calidad de las llamadas en Skype Empresarial?

1	2	3	4
			X

5. ¿Con que frecuencia los usuarios reportan la ventana de certificado de Outlook?

1	2	3	4
	X		

6. ¿Con que frecuencia los usuarios reportan desconexión con SAP?

1	2	3	4
X			

Encuesta sobre servicio y errores comunes

Del 31de julio al 4 de agosto

Técnico: Ricardo Pacheco

Basados en su conocimiento técnico y atención del usuario, por favor marque cada respuesta según su nivel de incidencia, con forme a la siguiente escala de valores, donde:

1	2	3	4
sin reportes	menos de 2 reportes	Entre 3 y 5 reportes	Mas de 6 reportes

1. ¿Con que frecuencia los usuarios se deben de re-autentificar en el Firewall?

1	2	3	4
X			

2. ¿Con que frecuencia los usuarios reportan llamadas caídas?

1	2	3	4
X			

Propuesta de Proyecto
Nueva red de Telecomunicaciones de SteinCorp Escazú
Plan Piloto

3. ¿Con que frecuencia los usuarios reportan Skype Empresarial auto-desconectado?

1	2	3	4
X			

4. ¿Con que frecuencia los usuarios reportan problemas con la calidad de las llamadas en Skype Empresarial?

1	2	3	4
	X		

5. ¿Con que frecuencia los usuarios reportan la ventana de certificado de Outlook?

1	2	3	4
X			

6. ¿Con que frecuencia los usuarios reportan desconexión con SAP?

1	2	3	4
X			

8.3 Apéndice III. Cotizaciones para elaboración del presupuesto

	Cantidad	Articulo	Precio	IV	SubTotal
Tecnova	1	Aruba 2530 24G Poe	$ 1 058,00	$ 137,54	$ 1 195,54
		Garantía NBD - 5 años	Incluida		
	4	Aruba 2530 48G Poe	$ 2 200,00	$ 286,00	$ 9 944,00
		Garantía NBD - 5 años	Incluida		$ -
				ARUBA	$ 11 139,54
	7	WatchGuard AP120 + Kit de montaje	$ 765,00	$ 99,45	$ 6 051,15
		Garantía NBD - 3 años	Incluida		
				TOTAL	**$ 17 190,69**

El Orbe	1	Aruba 2530 24G Poe	$ 989,37	$ 128,62	$ 1 117,99
	1	Garantía NBD - 5 años	$ 561,15	$ 72,95	$ 634,10
	4	Aruba 2530 48G Poe	$ 1 888,39	$ 245,49	$ 8 535,52
	4	Garantía NBD - 5 años	$ 710,12	$ 92,32	$ 3 209,74
				ARUBA	$ 13 497,35
	7	WatchGuard AP120 + Kit de montaje	$ 775,36	$ 100,80	$ 6 133,10
	1	Garantía NBD - 3 años	Incluida		
				TOTAL	**$ 19 630,45**

Alfatec	1	Aruba 2530 24G Poe	$ 962,00	$ 125,06	$ 1 087,06
	1	Garantía NBD - 5 años	$ 370,00	$ 48,10	$ 418,10
	4	Aruba 2530 48G Poe	$ 1 835,00	$ 238,55	$ 8 294,20
	4	Garantía NBD - 5 años	$ 695,00	$ 90,35	$ 3 141,40
				ARUBA	$ 12 940,76
	7	WatchGuard AP120 + Kit de montaje	$ 786,00	$ 102,18	$ 6 217,26
	1	Garantía NBD - 3 años			
				TOTAL	**$ 19 158,02**

Grupo Sega	1	Aruba 2530 24G Poe	$ 994,32	$ 129,26	$ 1 123,58
	1	Garantía NBD - 5 años	$ 390,91	$ 50,82	$ 441,73
	4	Aruba 2530 48G Poe	$ 1 897,73	$ 246,70	$ 8 577,74
	4	Garantía NBD - 5 años	$ 390,91	$ 50,82	$ 1 766,91
				ARUBA	$ 11 909,96
		No vende WatchGuard			
				TOTAL	**$ 11 909,96**

8.4 Apéndice IV. Compra de Equipos en Cartago

Modelo	Cantidad
HP 2530	6
HP 5130	2
HP 1920	2
AP 200	29

8.5 Apéndice V. Inversión - Primera Fase Cartago 2015

Dispositivivo	Inversion: 1 año	Inversion: 5 años
HP-WG	$19 396,26	$20 238,66
Alcatel-Lucent	$27 860,09	$27 860,09
Cisco	$28 057,03	$32 584,11

8.6 Apéndice VI. Switch - Primera Fase Cartago 2015

Marca	Stackeable	802.11 AC	Puerto Giga	BYoD Admin	Administración de Invitados	Wireless Controler	Interfaz	Garantía	RED Completa	Monitoreo
WG - HP	SI (IRF)	SI	SI	SI	SI	SI	GUI y HP IMC	5 años	SI	SI
Alcatel - Lucent	SI a 512Gbps	SI	SI	SI	SI	SI	GUI y Comandos	5 años	SI	SI
Cisco	SI a 480Gbps	SI	SI	NO	NO	NO	Comandos	1 año	Licenciada	Licenciada

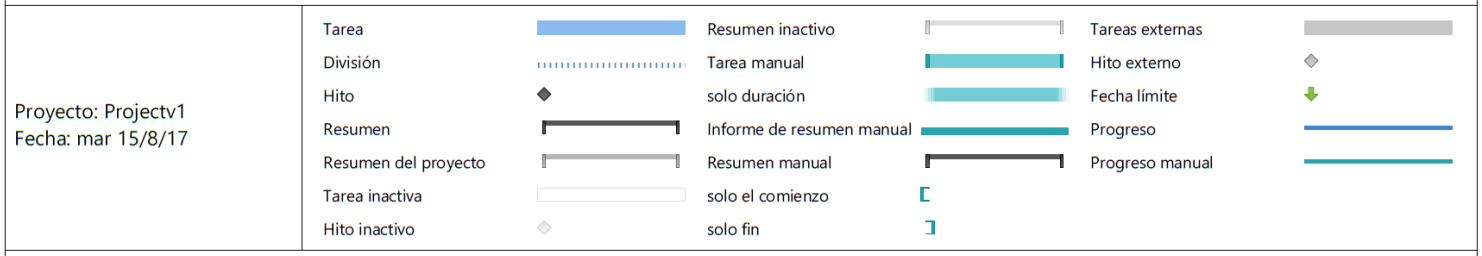
8.7 Apéndice VII. APs - Primera Fase Cartago 2015

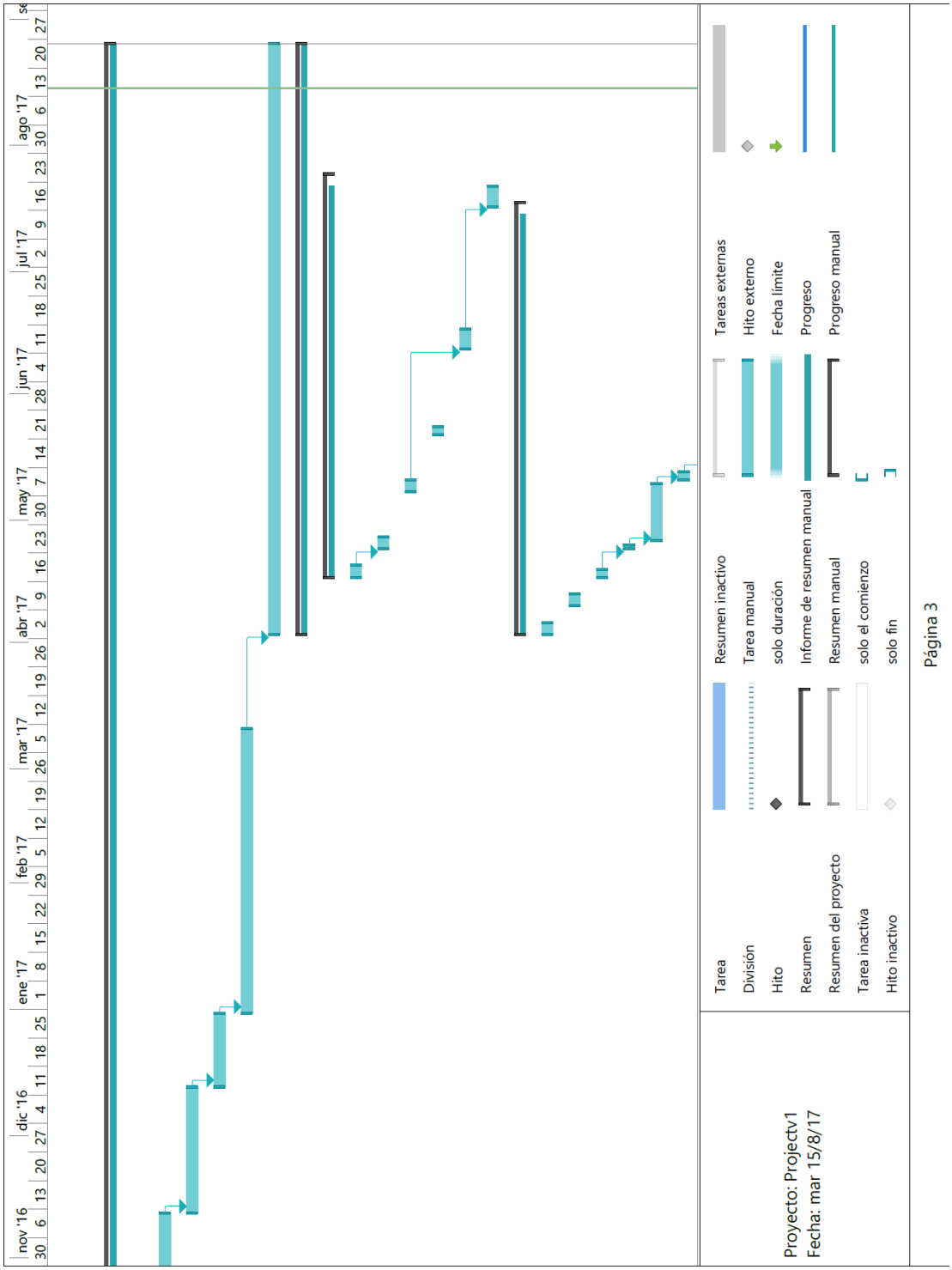
Marca	Control de BYoD	Red de Invitados	Perfiles de Acceso	Integracion con UTM	Wireless Controler	Radios	Antenas	Potencia TX	SSID	Costo (ii)
WatchGuard	SI	SI	SI	Nativa	Integrado	2	4	21 dBi	16	$ 772,17
Alcatel - Lucente	SI	SI	SI	NO	NO	2	4	21 dBi	16	$1 015,00
Cisco	NO	NO	NO	NO	NO	2	4	22 dBi	16	$ 786,67

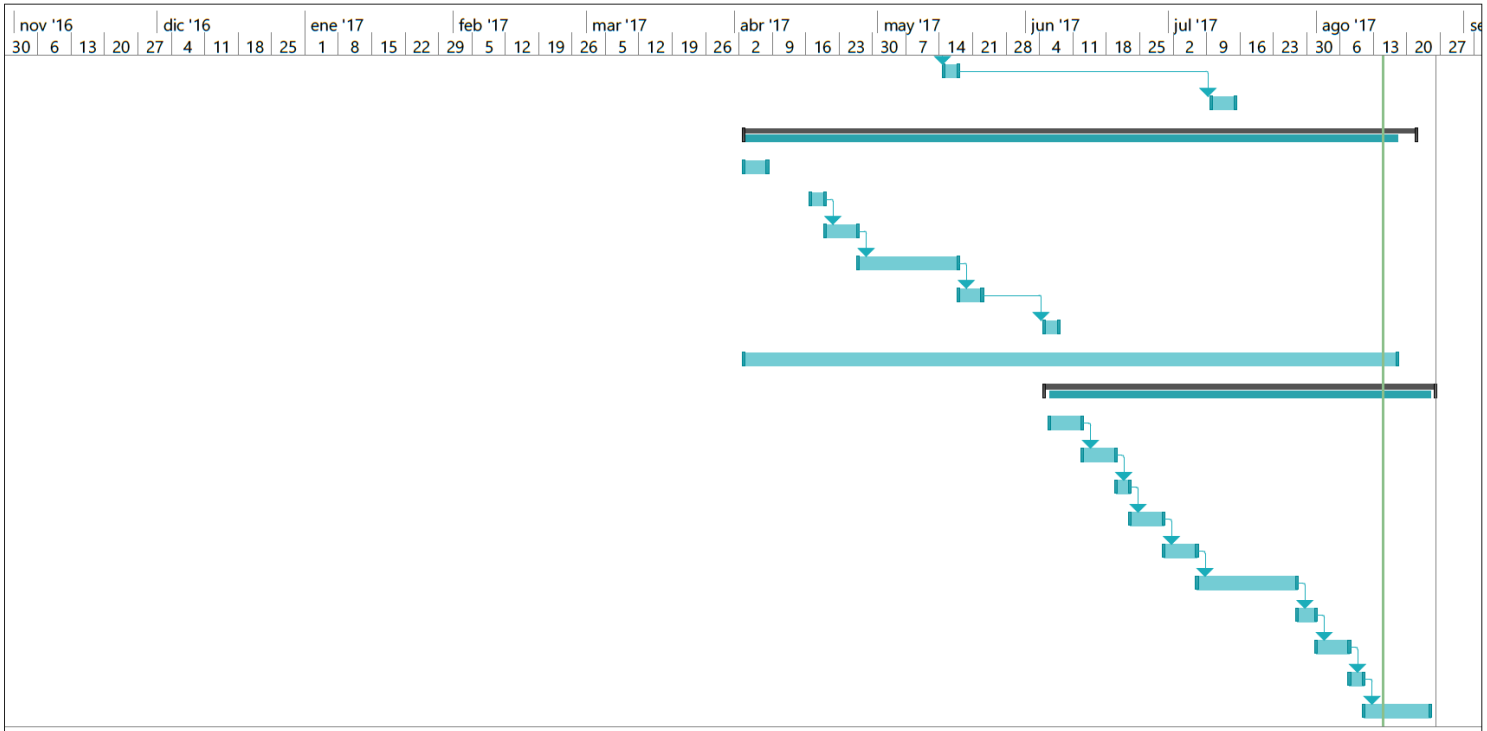
8.8 Apéndice VIII. Cronograma en MS Project

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		**Propuesta para la actualización de la red y sus equipos de comunicación de la sede de Escazú de SteinCorp**				
2		**Administrativo de la Universidad**	**235 días**	**lun 3/10/16**	**vie 25/8/17**	
3		Pre matricula de Proyecto de Graduación	14 días	lun 3/10/16	jue 20/10/16	
4		Entrega de la propuesta	16 días	jue 20/10/16	vie 11/11/16	3
5		Respuesta de la universidad	21 días	vie 11/11/16	lun 12/12/16	4
6		Matricula de Proyecto de Graduación	14 días	lun 12/12/16	vie 30/12/16	5
7		Inicio de Seminario	50 días	vie 30/12/16	vie 10/3/17	6
8		Inicio de Tutoría	105 días	lun 3/4/17	vie 25/8/17	7
9		**Planificación del Proyecto**	**105 días**	**lun 3/4/17**	**vie 25/8/17**	
10		**Calculo de impacto al ejecutar el proyecto**	**71 días**	**lun 17/4/17**	**lun 24/7/17**	
11		Levantar lista con los aplicativos principales	3 días	lun 17/4/17	mié 19/4/17	
12		Categorizar las prioridades en los aplicativos	3 días	lun 24/4/17	mié 26/4/17	11
13		Identificar periodos de desconexión	3 días	lun 8/5/17	mié 10/5/17	
14		Crear tres diferentes comunicados informativos	2 días	lun 22/5/17	mar 23/5/17	
15		Identificar ventanas de trabajo	5 días	lun 12/6/17	vie 16/6/17	13
16		Crear la documentación entregable	5 días	lun 17/7/17	vie 21/7/17	15
17		**Análisis de Proveedor**	**76 días**	**lun 3/4/17**	**lun 17/7/17**	
18		Buscar proveedores HP en Costa Rica	3 días	lun 3/4/17	mié 5/4/17	
19		Buscar proveedores WatchGuard en Costa Rica	3 días	lun 10/4/17	mié 12/4/17	
20		Crear documento con los requerimientos	2 días	lun 17/4/17	mar 18/4/17	
21		Enviar documentación	1 día	lun 24/4/17	lun 24/4/17	20
22		Recepción de ofertas	10 días	mié 26/4/17	mar 9/5/17	21
23		Análisis de ofertas	2 días	jue 11/5/17	vie 12/5/17	22

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
24		Crear cuadro comparativo de ofertas	3 días	lun 15/5/17	mié 17/5/17	23
25		Crear la documentación entregable	5 días	lun 10/7/17	vie 14/7/17	24
26		**Diseño de Cronograma de trabajo**	**101 días**	**lun 3/4/17**	**lun 21/8/17**	
27		Identificar tareas a realizar	5 días	lun 3/4/17	vie 7/4/17	
28		Identificar recursos humanos	3 días	lun 17/4/17	mié 19/4/17	
29		Planear con el proveedor las actividades	5 días	mié 19/4/17	mié 26/4/17	28
30		Crear el cronograma entregable	15 días	jue 27/4/17	mié 17/5/17	29
31		Identificar responsables por tarea	3 días	jue 18/5/17	lun 22/5/17	30
32		Revisar feriados, asuetos y vacaciones	3 días	lun 5/6/17	mié 7/6/17	31
33		Actualizar datos	99 días	lun 3/4/17	jue 17/8/17	
34		**Documentación**	**60 días**	**lun 5/6/17**	**vie 25/8/17**	
35		Revisar la documentación del proveedor	5 días	mar 6/6/17	lun 12/6/17	
36		Revisar la documentación del impacto	5 días	lun 12/6/17	lun 19/6/17	35
37		Revisar cronograma de implementación	3 días	lun 19/6/17	jue 22/6/17	36
38		Solución de imprevistos	5 días	jue 22/6/17	jue 29/6/17	37
39		Solución de pendientes	5 días	jue 29/6/17	jue 6/7/17	38
40		Unificar documentación	15 días	jue 6/7/17	jue 27/7/17	39
41		Revisión con Gerencia de TI	2 días	jue 27/7/17	lun 31/7/17	40
42		Solución de cambios	5 días	lun 31/7/17	lun 7/8/17	41
43		Cambios finales	3 días	lun 7/8/17	jue 10/8/17	42
44		Revisión de documento final	10 días	jue 10/8/17	jue 24/8/17	43




nov '16
dic '16
ene '17
feb '17
mar '17
abr '17
may '17
jun '17
jul '17
ago '17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual
Proyecto: Projectv1
Fecha: mar 15/8/17
Página 3



Proyecto: Projectv1 Fecha: mar 15/8/17	Tarea	Resumen inactivo		Tareas externas	
	División	Tarea manual		Hito externo	
	Hito	solo duración		Fecha límite	
	Resumen	Informe de resumen manual		Progreso	
	Resumen del proyecto	Resumen manual		Progreso manual	
	Tarea inactiva	solo el comienzo			
	Hito inactivo	solo fin			

8.9 Apéndice IX. Presentación PPT para la Dirección Financiera

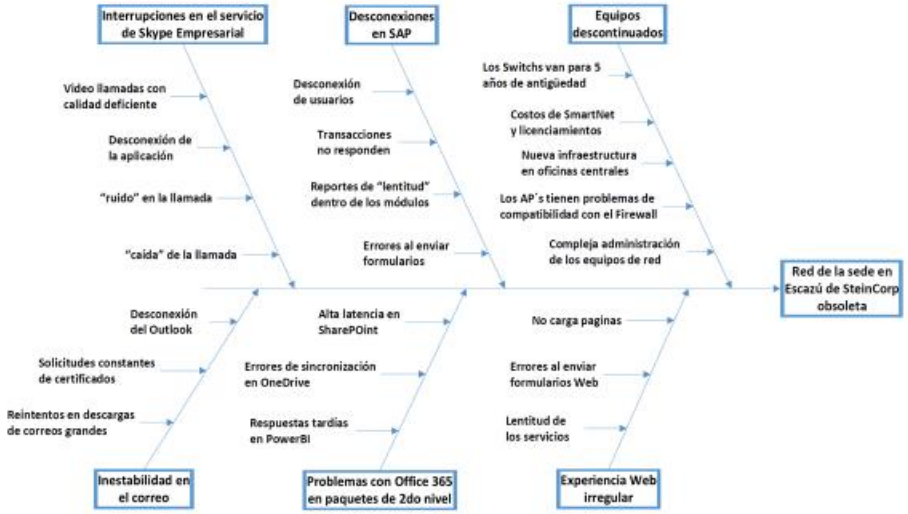
STEINCORP.

Antecedentes

- Equipos descontinuados
- Desconexiones de SAP
- Degradación de Skype Empresarial
- Inestabilidad del correo electrónico
- Mala experiencia Web
- Servicios de O365 inestables.

STEINCORP.

Antecedentes



STEINCORP.

Situación Actual

- Equipos sin garantía
- WiFi ineficiente
- Colapso tecnológico
- Redes saturadas
- Crecimiento mayor al 70%
- Red con +5 años de antigüedad
- Documentación del diseño actual inexistente

STEINCORP.

Situación Actual

Descripción	Cantidad	Modelo	Puertos	Antigüedad	Garantía
5to Piso					
Switch	1	Cisco 2960	48	+ 5 años	No
Switch	1	Cisco 2960	48	+ 5 años	No
Switch	1	3Com 4226T	24	+ 5 años	No
Switch PoE	1	Linksys LGS318P	18	- 1 año	Si
Access Point	4	AIR-CAP1602I-A-K9		+ 5 años	No
4to Piso					
Switch	1	Cisco 2960-X	24	+ 3 años	No
Switch	2	Catalyst 2960-C	12	+ 3 años	No
Wireless Controler	1	Cisco 2504		+ 3 años	No
Access Point	3	AIR-CAP1602I-A-K9		+ 5 años	No

STEINCORP.

Situación Actual

Desde: Departamento Legal, 5to piso

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 62, recibidos = 61, perdidos = 1
    (1% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 30ms, Máximo = 1695ms, Media = 317ms
```

WiFi - Escazú

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 61, recibidos = 61, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 76ms, Media = 7ms
```

LAN - Escazú

```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 59, recibidos = 59, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 5ms, Máximo = 3714ms, Media = 487ms
```

Wi Fi - Hasta Cartago

```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 62, recibidos = 61, perdidos = 1
    (1% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 3ms, Máximo = 117ms, Media = 13ms
```

LAN - Hasta Cartago

STEINCORP.

Situación Actual

Desde: Departamento de Tesorería, 4to piso

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 60, recibidos = 60, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 640ms, Media = 80ms
```

Wi Fi - Escazú

```
Estadísticas de ping para 192.168.112.254:
    Paquetes: enviados = 57, recibidos = 57, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 12ms, Media = 3ms
```

LAN - Escazú

```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 59, recibidos = 59, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 3ms, Máximo = 539ms, Media = 87ms
```

Wi Fi - Hasta Cartago

```
Estadísticas de ping para 10.10.3.30:
    Paquetes: enviados = 59, recibidos = 59, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 3ms, Máximo = 20ms, Media = 5ms
```

LAN - Hasta Cartago

STEINCORP.

Situación Actual

Antes							
Pregunta	1	2	3	4	5	6	
Calificación	3	2	3	4	2	1	Ricardo Pacheco
	3	2	2	3	3	2	Jerry Meléndez
	4	2	3	2	3	2	Jean Carlo Corrales
Total	10	6	8	9	8	5	46

Mejor Nota	18
Peor Nota	72

52% de errores

4% de errores

Plan Piloto							
Pregunta	1	2	3	4	5	6	
Calificación	1	1	1	2	1	1	Ricardo Pacheco
	2	1	1	1	1	1	Jerry Meléndez
	1	1	1	1	1	1	Jean Carlo Corrales
Total	4	3	3	4	3	3	20

Mejor Nota	18
Peor Nota	72

STEINCORP.

Fases del Proyecto

- Plan de comunicación
- Análisis de Riesgos
- Configuración de equipos
- Pruebas Pre-Implementación
- Plan Vuelta Atrás
- Implementación
- Plan de Pos-Implementación

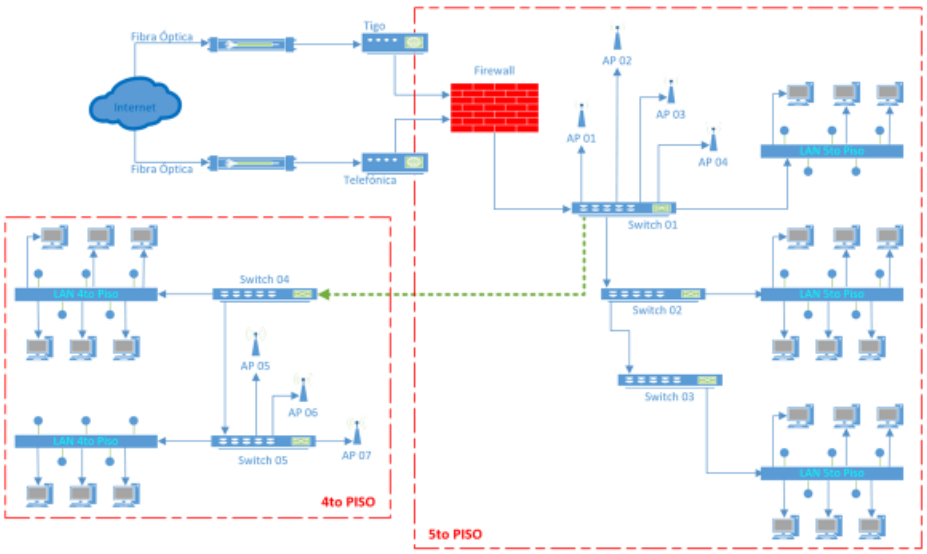
STEINCORP.

Requerimientos

Cantidad	Descripción	Marca	Modelo	Garantía
4to Piso				
1	Aruba 2530 24G PoE+ Switch	Aruba	2530	5 Años
1	Aruba 2530 48G PoE+ Switch	Aruba	2530	5 Años
3	Puntos de Acceso Inalámbrico (AP's)	WatchGuard	AP120	3 Años
5to Piso				
3	Aruba 2530 48G PoE+ Switch	Aruba	2530	5 Años
4	Puntos de Acceso Inalámbrico (AP's)	WatchGuard	AP120	3 Años
Adicional				
1	Servicio de Instalación Física de los AP's			
1	Servicio de Soporte de Ingeniero			

STEINCORP.

Requerimientos



STEINCORP.

Requerimientos

STEINCORP.

Requerimientos

STEINCORP.

Proveedores Invitados

	Cantidad	Articulo	Precio	IV	SubTotal
El Orbe	1	Aruba 2530 24G Poe	$ 989,37	$ 128,62	$ 1 117,99
	1	Garantía NBD - 5 años	$ 561,15	$ 72,95	$ 634,10
	4	Aruba 2530 48G Poe	$ 1 888,39	$ 245,49	$ 8 535,52
	4	Garantía NBD - 5 años	$ 710,12	$ 92,32	$ 3 209,74
				ARUBA	$ 13 497,35
	7	WatchGuard AP120 + Kit de montaje	$ 775,36	$ 100,80	$ 6 133,10
	1	Garantía NBD - 3 años	Incluida		
				TOTAL	**$ 19 630,45**
Alfatec	1	Aruba 2530 24G Poe	$ 962,00	$ 125,06	$ 1 087,06
	1	Garantía NBD - 5 años	$ 370,00	$ 48,10	$ 418,10
	4	Aruba 2530 48G Poe	$ 1 835,00	$ 238,55	$ 8 294,20
	4	Garantía NBD - 5 años	$ 695,00	$ 90,35	$ 3 141,40
				ARUBA	$ 12 940,76
	7	WatchGuard AP120 + Kit de montaje	$ 786,00	$ 102,18	$ 6 217,26
	1	Garantía NBD - 3 años			
				TOTAL	**$ 19 158,02**

STEINCORP.

Proveedores Invitados

	Cantidad	Articulo	Precio	IV	SubTotal
Tecnova	1	Aruba 2530 24G Poe	$ 1 058,00	$ 137,54	$ 1 195,54
		Garantía NBD - 5 años	Incluida		
	4	Aruba 2530 48G Poe	$ 2 200,00	$ 286,00	$ 9 944,00
		Garantía NBD - 5 años	Incluida		$ -
				ARUBA	$ 11 139,54
	7	WatchGuard AP120 + Kit de montaje	$ 765,00	$ 99,45	$ 6 051,15
		Garantía NBD - 3 años	Incluida		
				TOTAL	**$ 17 190,69**
Grupo Sega	1	Aruba 2530 24G Poe	$ 994,32	$ 129,26	$ 1 123,58
	1	Garantía NBD - 5 años	$ 390,91	$ 50,82	$ 441,73
	4	Aruba 2530 48G Poe	$ 1 897,73	$ 246,70	$ 8 577,74
	4	Garantía NBD - 5 años	$ 390,91	$ 50,82	$ 1 766,91
				ARUBA	$ 11 909,96
		No vende WatchGuard			
				TOTAL	**$ 11 909,96**

STEINCORP.

Presupuesto Solicitado

Detalle	Presupuesto
Compra de insumos tecnológicos	$17 200,00
Apoyo Técnico de Proveedor Experto	$850,00
Insumos y mano de obra para colocación de AP´s	$1 000,00
Variación del 5%	$950,00
Total	**$20 000,00**

STEINCORP.

Conclusiones

- La homologación es urgente por temas técnicos (red obsoleta) y de competitividad.
- Equipos de calidad comprobada.
- Proveedor con experiencia y aliado estratégico de TI.
- Disminución de tiquetes por temas de redes.
- Inversión realista.

STEINCORP.

8.10 Apéndice X. Correo con Aprobación y gestión del Presupuesto

martes 22/8/2017 08:10 a.m.

Marcos Solano

RE: Nueva Red Escazú

Para Rosana Acuña

CC Jonathan Cruz; Jefry Carballo Castro; Mario Gomez

Buenas, Estimada.

Detallo lo solicitado.

12000299 RENOVACIÓN REDES ESCAZÚ.

Saludos, Gracias

Marcos solano Camacho. | Encargado De Activos | STEIN CORP.
Tel: (506) 2550-6500 | Email: m.solano@lbs-cr.com

LBS logistics business services
UNA EMPRESA DE STEINCORP.

De: Rosana Acuña
Enviado el: lunes, 21 de agosto de 2017 13:31
Para: Marcos Solano <m.solano@labstein.onmicrosoft.com>
CC: Jonathan Cruz <jcruz@labstein.com>; Jefry Carballo Castro <j.carballo@lbs-cr.com>; Mario Gomez <m.gomez@labstein.onmicrosoft.com>
Asunto: RV: Nueva Red Escazú

Buenas Tardes Marcos,

Según la aprobación adjunta de don Mario, por favor crear el número de activo para el proyecto. Para ello el presupuesto solicitado y aprobado para 2017 fue el siguiente:

Plantilla para solicitud CAPEX 2017
Proceso presupuesto año 2017

AREA SOLICITANTE	RESPONSABLE	CUENTA CAPEX	PROYECTO	JUSTIFICACIÓN	ACTIVO	ESPECIFICACIONES TÉCNICAS	CANTIDAD	VALOR DE COMPRA
TI	TI	EQUIPO DE COMPUTO	Actualización Redes y Telecomunicaciones Escazú	Mejorar y estabilizar las redes en escazú que permita una navegación y comunicación fluida en las oficinas de 4to y 5to piso		Switches y AP's		20.000,00

Cualquier duda con gusto.
Slds.
Rosana

De: Mario Gomez
Enviado el: lunes, 21 de agosto de 2017 12:51 p. m.
Para: Jonathan Cruz <jcruz@labstein.com>
CC: Rosana Acuña <racuna@labstein.com>
Asunto: RE: Nueva Red Escazú

OK procedamos como CAPEX

De: Jonathan Cruz
Enviado el: lunes, 21 de agosto de 2017 11:14
Para: Mario Gomez <m.gomez@labstein.onmicrosoft.com>
CC: Rosana Acuña <racuna@labstein.com>
Asunto: RV: Nueva Red Escazú

Buenos días don Mario.

Como lo conversamos la semana pasada, le comparto la cotización de los equipos para la red de Escazú, para su aprobación.

Muchas gracias.

Saludos,

Jonathan Cruz Hidalgo | Infraestructura y Telecomunicaciones | Costa Rica y Filiales | SteinCORP.
Cel: (506) 7075-3494 | Tel: (506) 2550-6500 Ext: 506 636 | Email: **jcruz@labstein.com**

STEINCORP.

8.11 Apéndice XI. Carta de aprobación: Gerencia de TI

STEIN CORP.

22 de agosto, 2017
San José, Costa Rica

Facultad de Ingeniería
Dirección Escuela de Ingeniería Informatica.
Universidad Hispanoamericana.
A quien interese:

Por medio de la presente, hago constar en mi potestad de Gerente de Tecnologías de Información de SteinCorp, que Jonathan Cruz Hidalgo realizó su proyecto de graduación "*Propuesta de la arquitectura de la red de comunicaciones de la empresa SteinCorp en Escazú para su homologación con la red de la sede central en Cartago, aplicando métodos de diseño de redes, para el primer trimestre del 2018*", dicho proyecto fue presentado a la Dirección Financiera, resultando ser de gran interés, aprobado en su momento y consolidando el presupuesto necesario para la ejecución.

De manera conjunta trabajaremos en la implementación del proyecto, siendo Jonathan Cruz el responsable de la ejecutoria, administración y puesta en marcha, logrando hacer realidad la propuesta presentada.

Sin más por el momento, agradezco la atención brindada a la misma.

LABORATORIOS STEIN S.A.
STEIN CORP.
Recursos Humanos

Rosana Acuña Ostos
Ced.: 186200202207
Gerente de TI
SteinCorp

Laboratorios Stein, una compañía de Stein Corp. - Cartago - Costa Rica
Teléfonos: 2550 6500 - 2550 6565 Fax: (506) 2550-6552
Correo Postal: 930-1007 Centro Colón, San José Costa Rica.
Correo electrónico: cliente@labstein.com

CAPÍTULO XI

ANEXOS

9.1 Anexo I. Especificaciones WG AP200

Datasheet

WatchGuard® AP100 and AP200

Wireless Access Points

AP Technology at a Glance
What's behind the AP100 and AP200

Best-in-class hardware
WatchGuard's wireless access points are built using the latest generation of wireless hardware, incorporating advanced technologies to deliver 2x2 MIMO with dual spatial streams capable of handling data rates up to 600 Mbps.

Ease of management
With unified management tools, administrators can easily manage both their AP devices and XTM appliances from a single console.

Strong security
Features like MAC filtering, client reporting, Captive Portal technology, 802.1X authentication, and PCI compliant scan and reporting, ensure a strong WLAN security stance.

Simple roaming
WatchGuard AP devices have you covered, with up to 16 SSIDs, and seamless network access when roaming between access points.

Great coverage, low profile
Powerful radios and internal antennas housed in a sleek design allow for maximum coverage with a subtle deployment profile, suitable for any space.

Flexible power options
Power options include Power Over Ethernet (PoE), A/C adapter (included), and PoE injector (optional) for maximum deployment flexibility. AP200's plenum enclosure offers safety code compliance for those who need it.

Lower TCO
Realize big cost savings, with no separate controller hardware costs, no per-AP "seat" charges, and no controller software license fees.

The mass adoption of smart wireless devices like tablets, smartphones and notebooks is driving the BYOD (bring your own device) explosion, putting ever increasing demands on wireless networks. This pressure, coupled with the "wild west" nature of WLAN, means it is now more important than ever to have control of your entire network – both wired and wireless – with best-in-class security, integrated security policies, and increased visibility.

Extend best-in-class UTM security to the WLAN

Protecting against today's sophisticated blended threats requires multiple security capabilities, and these threats don't discriminate between a wired or wireless network path to their targets. WatchGuard's AP100 and AP200 meet this challenge by extending best-in-class UTM security – including application control, intrusion prevention, URL and web content filtering, virus and spam blocking and more – from the XTM to the WLAN. With the AP100 and AP200, businesses can harness the power of mobile devices without putting network assets at risk.

Integrate wired and wireless security policies

WatchGuard's AP100 and AP200 allow users to easily apply security policies to wired and WLAN resources simultaneously , which is critical to enforcing security standards across the entire network infrastructure. And updating integrated policies couldn't be simpler – creating huge IT time-savings.

Unified device management

Unified device management tools offer a "single pane of glass" view into network security activities and allow users to configure and manage their AP100/AP200 and XTM devices from one place – reducing both setup time and maintenance costs.

AP100 and AP200 Technical Specifications

	AP100	AP200	
Hardware Details			
Number of Radios	1	2	
Supported Frequencies (summary)	2.4GHz or 5GHz (selectable)	Radio 1 = 5GHz	Radio 2 = 2.4GHz
Radio characteristics	2x2 MIMO Dual Spatial Streams		
Supported frequencies*	2,400-2.474GHz, 5.150-5.250GHz, 5.250-5.350GHz, 5.470-5.725GHz, 5.725-5.850GHz		
Antenna	4 internal, omnidirectional		
Peak Antenna Gain	3 dBi	4 dBi	3 dBi
Maximum TX Power*	2.4GHz = 17dBm 5GHz = 20DBm	5GHz = 20dBm	2.4GHz = 21dBm
Data Rate	300 Mbps	600 Mbps	
SSID	8	16	
Plenum Enclosure (fire resistant)	No	Yes	
Security Settings	WPA-PSK, WPA2-PSK, WPA2-PSK Mixed, WPA2-Enterprise 802.1x, TKIP, AES		
Ethernet	1GBe		
Power Options	PoE, A/C Adapter		
MTBF	> 500,000 Hours		
Physical Security	Kensington Lock		
IEEE Standards Supported	802.11a/b/g/n, 802.11i, 802.1x, 802.3af/at, 802.1Q		
Support & Maintenance	1-year or 3-year subscription to LiveSecurity® Service for hardware warranty with advance hardware replacement, technical support, software updates - included with purchase		
Deployment	Indoors		

*Country-specific restrictions apply

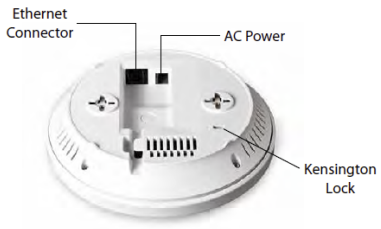
Environmental Information	
Operating Temperature	32 to 104 F° (0 to 40° C)
Operating Relative Humidity	5% to 90% Non-condensing
Storage Temperature	-40 to 158° F (-40° to 70° C)
Non-Operating Relative Humidity	5% to 90% Non-condensing
AC Power Adapter	
Input Voltage	100 - 240V AC
Frequency	50/60Hz
Input Current Maximum	400mA
Output Voltage	12V
Output Current	1250mA
PoE Injector (optional)	
IEEE Standard	802.3af
Input Voltage	100 - 240V AC
Output Voltage	56V
Output Power	15.4W
Dimensions	
Product Dimensions	6.5" RD x 1.75" H (16.5 x 4.4 cm)
Shipping Dimensions	7" x 7.25" x 4.5" (17.8 x 18.4 x 11.4 cm)
Product Weight	.75 lbs (.34 kg)
Shipping Weight (includes A/C adapter, mounting kit, etc.)	2 lbs (.91 kg)
Mounting Kit	Included
Certifications	
Wireless	FCC, IC, CE
Safety	NRTL/C, CB, CE
Control of Hazardous Substances	WEEE, RoHS, REACH

Suggested† Number of Access Points by XTM Model and XTMv Edition

XTM Models	2 Series**	3 Series	5 Series	8 Series	800 Series	XTM 1050	1500 Series	XTM 2050	XTM 2520
Number of Access Points	up to 5	up to 15	up to 35	up to 70	up to 100	up to 100	up to 100	up to 100	up to 100

XTMv (virtual) Editions	Small Office	Medium Office	Large Office	Datacenter
Number of Access Points	up to 25	up to 50	up to 75	up to 100

†Number of Access Points is not restricted by license **Not available on XTM 21, 22, 23 models



To learn more about the WatchGuard AP100 and AP200, contact your WatchGuard reseller, or visit us at www.watchguard.com/AP

U.S. SALES: 1.800.734.9905 INTERNATIONAL SALES: +1.206.613.0895 WEB: www.watchguard.com

9.2 Anexo II. Especificaciones WG AP120

AP 120 & AP320 Technical Specifications

WatchGuard

IEEE 802.11b/g/n			
Frequency Band	Scanning	Transmission	
	All regions	USA & Canada (FCC/IC)	Europe (ETSI)
	2400 ~ 2483.5 MHz	2400 ~ 2473.5 MHz	2400 ~ 2483.5 MHz
Modulation Type	DSSS, OFDM		
Data Rates	Up to 450 Mbps (MCS 0-23) with automatic rate adaptation		
Antenna	Integrated modular high efficiency PIFA omnidirectional antenna		

IEEE 802.11a/n/ac			
Frequency Band	Scanning	Transmission	
	All regions	USA & Canada (FCC/IC)	Europe (ETSI)
	4.92 ~ 5.08 GHz 5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.47~ 5.725 GHz 5.725~ 5.825 GHz	5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.725~ 5.82 5GH	5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.47~ 5.725 GHz
Dynamic Frequency Selection	DFS and DFS2		
Modulation Type	OFDM		
Data Rates	AP120 Up to 866 Mbps (MCS 0-9) for 11ac with automatic rate adaptation Up to 300 Mbps (MCS 0-23) for 11n with automatic rate adaptation	AP320 Up to 1.3 Gbps (MCS 0-9) for 11ac with automatic rate adaptation Up to 450 Mbps (MCS 0-23) for 11n with automatic rate adaptation	
Antenna	Integrated modular high efficiency PIFA omnidirectional antenna		

Maximum Transmit Power for 5 GHz

AP 120	
MCS Index	Transmit Power(dBm)
802.11a (legacy)	
6Mbps - 24Mbps	20
36Mbps	20
48Mbps	18
54Mbps	17
802.11n HT20 (legacy)	
MCS 0,1,2,3,4	20
MCS 5,6,7	17
MCS 8	15
802.11n HT40	
MCS 0,1,2,3,4	20
MCS 5,6,7	17
MCS 8,9	15
802.11ac 256QAM VHT80	
MCS 0,1,2,3,4	20
MCS 5,6,7	17
MCS 8,9	15

AP 320	
MCS Index	Transmit Power(dBm)
802.11a (legacy)	
6Mbps	18
36Mbps	18
48Mbps	18
54Mbps	17
802.11n HT20 (legacy)	
MCS 0,1,2,3,4,8,9 ,10,11,12,16,17,1 8,19,20	18
MCS 5,13,21	18
MCS 6,14,22	18
MCS 7,15,23	17
802.11n HT40	
MCS 0,1,2,3,4,8,9 ,10,11,12,16,17,1 8,19,20	18
MCS 5,13,21	18
MCS 6,14,22	18
MCS 7,15,23	17
802.11ac 256QAM VHT80	
3/4 Code Rate	15
5/6 Code Rate	14

Maximum Transmit Power for 2.4 GHz

AP 120	
MCS Index	Transmit Power(dBm)
802.11b (legacy)	
1Mbps - 11Mbps	20
802.11g (legacy)	
6Mbps - 24Mbps	20
36Mbps	20
48Mbps	20
54Mbps	20
802.11n HT20 (legacy)	
MCS	20
MCS 6,7,14,15	18
802.11n HT40	
MCS	20
MCS 6,7,14,15	18

AP 320	
MCS Index	Transmit Power(dBm)
802.11a (legacy)	
6Mbps	20
54Mbps	18
802.11n HT20 (legacy)	
MCS 0/8/16	20
MCS 7/15	18
MCS 23	17
802.11n HT40	
MCS 0/8/16	20
MCS 7/15	17
MCS 23	16

AP 120 & AP320 Technical Specifications

MCS Index	Receive Sensitivity 5 GHz	
	AP120	AP 320
802.11a (legacy)		
64Mbps	-89	-90
36Mbps	-	-77
48Mbps	-	-74
54Mbps	-72	-72
802.11n HT20 (legacy)		
MCS 0/8	-89	-
MCS 0,1,2,3,4,8,9,10,11,12,16,17,18 ,19,20	-	-90
MCS 5,13,21		-73
MCS 6,14,22		-71
MCS 7,15	-69	-
MCS 7,15,23	-	-70
802.11n HT40		
MCS 0/8	-87	-
MCS 0,1,2,3,4,8,9,10,11,12,16,17,18 ,19,20	-	-86
MCS 5,13,21	-	-69
MCS 6,14,22	-	-68
MCS 7,15	-66	-
MCS 7,15,23	-	-67
802.11ac 256QAM VHT80		
HT20 MCS 8 @ 3/4 Code rate	-	-59
HT20 MCS 9 @ 5/6 Code Rate	-	-57
HT40 MCS 8 @ 3/4 Code Rate	-	-56
HT40 MCS 9 @ 5/6 Code Rate	-	-54
HT80 MCS 8 @ 3/4 Code rate	-	-53
HT80 MCS 9 @ 5/6 Code Rate	-	-51
802.11ac		
VHT20 MCS0	-87	-
VHT20 MCS8	-66	-
VHT40 MCS0	-85	-
VHT40 MCS9	-61	-
VHT80 MCS0	-84	-
VHT80 MCS9	-58	-

MCS Index	Receive Sensitivity 2.4 GHz	
	AP120	AP 320
802.11a (legacy)		
1Mbps	-92	-95
6Mbps	-89	-91
11Mbps	-84	-87
54Mbps	-72	-74
802.11n HT20 (legacy)		
MCS 0/8	-89	-
MCS 0/8/16	-	-91
MCS 7,15	-69	-
MCS 7,15,23	-	-70
802.11n HT40		
MCS 0/8	-87	-
MCS 0/8/16	-	-87
MCS 7,15	-66	-
MCS 7,15,23	-	-67

Country-Wise Max Transmit Powers (dBm)		
Countries	2.4 GHz	5 GHz
Australia	20	23
Canada	30	23
India	20	20
Israel	20	20
Japan	20	20
UAE	20	17
USA	20	23

***Note:** The actual transmit power will be the lowest of:
- Value specified in the Device Template
- Maximum value allowed in the regulatory domain
- Maximum power supported by the radio

Regulatory Specifications RF and Electromagnetic	
Countries	Certification
USA	FCC Part 15.247, 15.407
Canada	IC
Europe	**CE EN300.328, EN301.893** **Countries covered under Europe certification:** Austria, Belgium, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Iceland, Luxembourg, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Slovakia, Slovenia, Switzerland, The Czech Republic, UK.

Information Technology Equipment - Safety	
Countries	Certification
USA	UL 60950
Canada	cUL 60950
European Union (EU)	EN 60950 RoHS

9.3 Anexo III. Especificaciones Switch Core 5130ei

Serie de conmutadores HP 5130 EI

La serie de conmutadores HP 5130 EI ofrece flexibilidad, escalabilidad y bajo coste total de propiedad en la capa de acceso de las redes de complejos de edificios de medianas y grandes empresas. Ofrece calidad de servicio y seguridad de clase empresarial, apilamiento mediante HP Intelligent Resilient Framework (IRF), enrutamiento estático de capa 3 y RIP, prácticos puertos de enlace ascendente fijos de 10 GbE, PoE+, ACL, IPv6 y ahorro de energía con Ethernet de eficiencia energética.

La serie de conmutadores HP 5130 EI lista para SDN con soporte OpenFlow 1.3 puede administrarse con HP Intelligent Management Center (IMC) para acceder a una sola vista de toda la red.

Novedades

- Conmutadores administrados escalables con enrutamiento estático de capa 3, RIP y apilamiento IRF en 9 chasis.
- Cuatro enlaces ascendentes fijos de 10 GbE (SFP+).
- Modelos PoE+ para dispositivos de voz, de vídeo e inalámbricos.
- Compatible con OpenFlow 1.3.
- Garantía de por vida limitada 2.0 con soporte telefónico 24x7 durante 3 años.

Características

Conmutadores de nivel de acceso seguros y escalables

La serie de conmutadores HP 5130 EI ofrece flexibilidad, escalabilidad y bajo coste total de propiedad en la capa de acceso de las redes de complejos de edificios de empresas medianas y grandes. EI 5130 es compatible con puertos de 10 GbE fijos, enrutamiento estático de nivel 3 y RIP v1/v2, PoE+, ACL, IPv6 y ahorro de potencia con Ethernet de eficiencia energética.

HP Intelligent Resilient Framework (IRF) virtualiza hasta nueve conmutadores físicos en un dispositivo lógico para redes más sencillas, planas y ágiles.

Los cuatro enlaces ascendentes fijos de 10 GbE (SFP+) ofrecen rendimiento para aplicaciones intensivas de ancho de banda.

Incluye funciones de red definida por software (SDN) con soporte OpenFlow 1.3 para garantizar el futuro de la red.

Garantía 2.0 limitada de por vida con soporte telefónico 24x7 durante 3 años y sin necesidad de licencias de software.

Mejora de la calidad de servicio con la gestión de tráfico

La serie de conmutadores HP 5130 EI es compatible con QoS basada en un clasificador avanzado que agrupa el tráfico mediante múltiples criterios de coincidencia basados en información de capa 2 y 3; aplica normativas QoS, tales

como el establecimiento del nivel de prioridad y el límite de velocidad para seleccionar el tráfico por puerto, por VLAN o en todo el conmutador.

Proporciona asignación de prioridades de tráfico con acciones de congestión compatibles que incluye: cola de prioridad estricta (SP), cola de ponderación por turnos (WRR) y detección anticipada aleatoria ponderada (WRED) y SP+WRR y supervisión de tráfico con velocidad de línea y velocidad de acceso confirmada (CAR).

Reduzca el tráfico de red no deseado con control de difusión que le permite limitar la tasa de tráfico de difusión para reducir el tráfico de difusión no deseado de la red.

Control de seguridad completa

La serie de conmutadores HP 5130 EI es compatible con los métodos de autenticación flexibles incluyendo 802.1X y autenticación MAC para una mayor seguridad y autenticación basada en políticas de la aplicación. Las listas de control de acceso por usuario (ACL) proporcionan el control de seguridad y el acceso por identidad.

Las ACL ofrecen filtrado de tráfico de capa 2 a capa 4 de IP; admite ACL, VLAN ACL, puerto ACL y IPv6 ACL global.

Seguridad con cifrado de los métodos de acceso (CLI, GUI o MIB) a través de SSHv2, SSL y/o SNMPv3 y otras funciones que incluyen protección de DHCP, protección de la fuente IP, protección de ARP y RADIUS/HWTACAS.

Vista única de la red

La serie de conmutadores HP 5130 EI puede administrarse perfectamente con HP Intelligent Management Center (IMC) para proporcionar transparencia de red integral con experiencia de red uniforme, a través de configuración completa, cumplimiento y administración de políticas.

RMON y sFlow ofrecen funcionalidades avanzadas de monitorización y notificación para estadísticas, historiales, alarmas e incidencias

9.4 Anexo IV. Especificaciones Switch 2530

Serie de conmutadores HP 2530

La serie de conmutadores HP 2530 ofrece facilidad de uso, seguridad y confianza para implementaciones en empresarial, sucursales y pequeñas y medianas empresas. Los conmutadores totalmente gestionables ofrecen capacidades completas de capa 2 con PoE+ opcional, enlaces ascendentes de 10 GbE, seguridad de acceso mejorada, priorización de tráfico, sFlow, compatibilidad con host IPv6 e incluyen garantía limitada 2.0 de por vida con 3 años de atención telefónica 24x7.

La serie de conmutadores HP 2530 es fácil de usar y de implementar y puede gestionarse con el HP Intelligent Management Center (IMC) para obtener una sola vista de toda la red.

Novedades

- Conmutadores de nivel 2 totalmente administrados, rentables, fiables y totalmente administrados
- Vínculos superiores de 10 Gigabit, ACL, EEE, priorización de tráfico
- Modelos Fast Ethernet o Gigabit de 8, 24 y 48 puertos
- Modelos PoE+ para dispositivos de voz, de vídeo e inalámbricos
- Garantía de por vida limitada 2.0 con soporte telefónico 24x7 durante 3 años

Características

Conmutadores de nivel de acceso seguro, fiables y rentables

La serie de conmutadores HP 2530 ofrece un uso seguro y de confianza para implementaciones de borde de empresa, sucursales y pequeñas y medianas empresas.

Los conmutadores totalmente gestionables ofrecen capacidades completas de capa 2 con PoE+ opcional, enlaces ascendentes de 10 GbE, seguridad de acceso mejorada, priorización de tráfico, sFlow, compatibilidad con host IPv6 e incluyen garantía limitada 2.0 de por vida con 3 años de atención telefónica 24x7.

Implementación del tamaño adecuado con la posibilidad de 8, 24 y 48 modelos de puertos disponibles con puertos Gigabit o Fast Ethernet, PoE+ opcional y enlaces ascendentes de 10 GbE opcionales.

Ahorro de energía con los modelos sin ventilador, Ethernet de consumo eficiente de energía (IEEE 802.3az) y capacidad para desactivar los LED y permitir el modo de bajo consumo de energía de puertos.

Garantía 2.0 limitada de por vida con soporte telefónico 24x7 durante 3 años y sin necesidad de licencias de software.

Seguridad y calidad de servicio

La serie de conmutadores HP 2530 es compatible con los métodos de autenticación flexibles, incluyendo 802.1X, MAC y con autenticación de web para una mayor seguridad y una autenticación basada en políticas de la aplicación.

Protección avanzada de denegación de servicio (DOS), como protección DHCP, protección dinámica ARP y bloqueo dinámico de IP, y controles de tráfico flexible incluyendo ACL y QoS.

La asignación de prioridades de tráfico con IEEE 802.1o permite clasificar el tráfico en tiempo real con compatibilidad con ocho niveles de prioridad asignados a dos o cuatro colas utiliza cola de ponderación de déficit por turnos (WDRR) o de prioridad estricta (SP),

Defienda la red IPv6 con la protección de DHCPv6.

Implementación y administración sencillas

La serie de conmutadores HP 2530 es compatible con la elección de interfaz de administración con Web GUI, interfaz de línea de comandos (CLI) y Simple Network Management Protocol (SNMP), con consola o puertos micro USB.

Funcionamiento silencioso con modelos sin ventilador y velocidad variable;

Implementación flexible con opciones de montaje en pared, mesa y bastidor.

TR-069 ofrece una implementación sin intervención para dispositivos con direcciones IP dinámicas y en redes privadas.

Vista única de la red

La serie de conmutadores HP 2530 puede administrarse perfectamente con HP Intelligent Management Center (IMC) para proporcionar la transparencia de red integral con la experiencia de red uniforme, a través de una amplia configuración, cumplimiento y administración de políticas.

RMON, y sFlow ofrecen funcionalidades avanzadas de monitorización y notificación para estadísticas, historiales, alarmas e incidencias.

QuickSpecs

HP 2530 Switch Series

Overview

HP 2530 Switch Series

Models

HP 2530-48G-PoE+ Switch	J9772A
HP 2530-24G-PoE+ Switch	J9773A
HP 2530-8G-PoE+ Switch	J9774A
HP 2530-48-PoE+ Switch	J9778A
HP 2530-24-PoE+ Switch	J9779A
HP 2530-8-PoE+ Switch	J9780A
HP 2530-48G Switch	J9775A
HP 2530-24G Switch	J9776A
HP 2530-8G Switch	J9777A
HP 2530-48 Switch	J9781A
HP 2530-24 Switch	J9782A
HP 2530-8 Switch	J9783A
HP 2530-48G-PoE+-2SFP+ Switch	J9853A
HP 2530-24G-PoE+-2SFP+ Switch	J9854A
HP 2530-48G-2SFP+ Switch	J9855A
HP 2530-24G-2SFP+ Switch	J9856A
HP 2530-8-PoE+ Internal Power Supply Switch	JL070A

Key features

- Cost-effective, reliable, secure, and fully managed L2 switches
- 8, 24, or 48 Gigabit or Fast Ethernet ports with up to four Gigabit or two 10 Gigabit uplink ports
- PoE+ models for voice, video, and wireless deployments
- Access control lists (ACLs), EEE, and IPv4/IPv6 host support
- Limited Lifetime Warranty 2.0 with 3 years 24x7 phones support

QuickSpecs

Overview

Introduction

The HP 2530 Switch Series consists of 17 fully managed L2 edge switches that deliver cost-effective, reliable, secure, and easy-to-use connectivity to business networks. Designed for entry-level to midsize enterprise networks, these Gigabit and Fast Ethernet switches deliver full L2 capabilities with optional Power over Ethernet (PoE), enhanced access security, traffic prioritization, and IPv6 host support.

The HP 2530 Switch Series offers uplink flexibility with either four Gigabit or two 10 Gigabit Ethernet uplinks on some 24- and 48-port models. The Gigabit 24- and 48-port models have either two small form-factor pluggable plus (SFP+) or four small form-factor pluggable (SFP) slots for fiber connectivity. The Fast Ethernet 24- and 48-port models have two SFPs and two RJ-45 Gigabit uplinks. The compact and fan-less 8-port switches offer additional flexibility with two dual-personality ports that can be used as either RJ-45 Gigabit Ethernet or SFP ports. Moreover, the HP 2530 PoE+ Switches are IEEE 802.3af and IEEE 802.3at compliant with up to 30 W per port, making them suitable for voice, video, or wireless deployments with PoE+.

The switch series is easy to use, deploy, and manage via the SNMP, CLI, and Web GUI. It offers flexible wall, table, and rack mounting options; quiet operation with fan-less and variable-speed fan models; and improved power savings with features such as IEEE 802.3az energy-efficient Ethernet. And it includes Limited Lifetime Warranty 2.0 with 3 years 24x7 phone support and includes all software releases.

Features and Benefits

Quality of Service (QoS)

- **Traffic prioritization (IEEE 802.1p)**
  allows real-time traffic classification with support for eight priority levels mapped to either two or four queues, and uses weighted deficit round robin (WDRR) or strict priority
- **Simplified QoS configuration**
  - **Port-based**
    prioritizes traffic by specifying a port and priority level
  - **VLAN-based**
    prioritizes traffic by specifying a VLAN and priority level
- **Class of Service (CoS)**
  sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
- **Rate limiting**
  establishes per-port ingress-enforced maximums for all ingressed traffic or for broadcast, multicast, or unknown destination traffic
- **Layer 4 prioritization**
  enables prioritization based on TCP/UDP port numbers
- **Flow control**
  helps deliver reliable communication during full-duplex operation

Management

- **Choice of management interfaces**
  - **HTML-based easy-to-use Web GUI**
    allows configuration of the switch from any Web browser
  - **Robust CLI**
    provides advanced configuration and diagnostics
  - **Simple network management protocol (SNMPv1/v2c/v3)**
    allows the switch to be managed with a variety of third-party network management applications
- **Virtual stacking**
  provides single IP address management for up to 16 switches
- **sFlow (RFC 3176)**
  delivers wire-speed traffic accounting and monitoring, configured by SNMP and CLI with three terminal encrypted

receivers

- **IEEE 802.1AB Link Layer Discovery Protocol (LLDP)**
  automates device discovery protocol for easy mapping by network management applications
- **Logging**
  provides local and remote logging of events via SNMP (v2c and v3) and syslog; provides log throttling and log filtering to reduce the number of log events generated
- **Port mirroring**
  allows traffic to be mirrored on any port or a network analyzer to assist with diagnostics or detecting network attacks
- **Remote monitoring (RMON)**
  provides advanced monitoring and reporting capabilities for statistics, history, alarms, and events
- **Find, fix, and inform**
  finds and fixes common network problems automatically, and then informs the administrator
- **Friendly port names**
  allows assignment of descriptive names to ports
- **Dual flash images**
  provides independent primary and secondary operating system files for backup while upgrading
- **Multiple configuration files**
  are easily stored with a flash image
- **Front-panel LEDs**
  - **Locator LEDs**
    allows users to set the locator LED on a specific switch to turn on, blink, or turn off; and simplifies troubleshooting by making it easy to locate a particular switch within a rack of similar switches
  - **Per-port LEDs**
    provides an at-a-glance view of the status, activity, speed, and full-duplex operation
  - **Power and fault LEDs**
    display issues, if any
- **Comware CLI**
  - **Comware-compatible CLI**
    bridges the experience of HP Comware CLI users who are using the HP ProVision software CLI
  - **Display and fundamental Comware CLI commands**
    are embedded in the switch CLI as native commands; display output is formatted as on Comware-based switches, and
    fundamental commands provide a Comware-familiar initial switch setup
  - **Configuration Comware CLI commands**
    when Comware commands are entered, CLI help is elicited to formulate the correct ProVision software CLI command
- **Download Software via DHCP**
  adds the option to specify the location of switch software via DHCP
- **TR-069 support**
  enables zero-touch configuration for switches

Connectivity

- **IPv6**
  - **IPv6 host**
    allows the switch to be deployed and managed at the edge of an IPv6 network
  - **Dual stack (IPv4/IPv6)**
    supports connectivity for both protocols; provides a transition mechanism from IPv4 to IPv6
  - **MLD snooping**
    f orwards IPv6 multicast traffic to appropriate interface; prevents IPv6 multicast traffic from flooding the network
  - **IPv6 ACL/QoS**
    supports ACL & QoS for IPv6 network traffic on Gigabit & 48 port 10/100 models
  - **Security**
    RA Guard, DHCPv6 Protection, Dynamic IPv6 Lockdown (YA only)

Overview

- **IEEE 802.3af Power over Ethernet (PoE)**
  provides up to 15.4 W per port to IEEE 802.3af-compliant PoE-powered devices such as IP phones, wireless access points, and security cameras
- **IEEE 802.3at PoE+**
  provides up to 30 W per port to IEEE 802.3 for PoE/PoE+-powered devices such as video IP phones, IEEE 802.11n wireless access points, and advanced pan/tilt/zoom security cameras (refer to the product specifications for the total PoE power availability)
- **Auto-MDIX**
  adjusts automatically for straight-through or crossover cables on all ports
- **Pre-standard PoE support**
  detects and provides power to pre-standard PoE devices (refer to the list of supported devices in the product FAQs, which can be accessed at http://www.hp.com/networking/support)
- **SFP slots**
  provides fiber connectivity such as Gigabit-SX, -LX, -LH, and -BX with four SFP slots on all 24- and 48-port Gigabit Ethernet models. Fast Ethernet 24- and 48-port models have two SFP slots and two RJ-45 Gigabit uplinks; 8-port models have two dual-personality ports supporting either SFP or RJ-45 Gigabit uplinks
- **Dual-personality (RJ-45 or USB micro-B) serial console port**
  gives easy access to switch CLI with front-of-switch location and the flexibility of using either an RJ-45 or USB micro-B serial console port

Layer 2 switching

- **VLANs**
  provides support for 512 VLANs and 4,094 VLAN IDs
- **Jumbo packet support**
  supports up to 9,220-byte frame size to improve the performance of large data transfers; 8- and 24-port Fast Ethernet models automatically support up to 2,000-byte frames with no configuration needed
- **16K MAC address table**
  provides access to many Layer 2 devices
- **GARP VLAN Registration Protocol**
  allows automatic learning and dynamic assignment of VLANs
- **Rapid Per-VLAN Spanning Tree (RPVST+)**
  allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+

Security

- **ACLs**
  accommodates IPv4/IPv6 port and VLAN-based ACLs (IPv6 ACL is supported only on Gigabit Ethernet and 48-port models.)
- **Source-port filtering**
  allows only specified ports to communicate with each other
- **RADIUS/TACACS+**
  eases switch management security administration by using a password authentication server
- **Secure Sockets Layer (SSL)**
  encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch
- **Port security**
  allows access only to specified MAC addresses, which can be learned or specified by the administrator
- **MAC address lockout**
  prevents particular configured MAC addresses from connecting to the network
- **Multiple user authentication methods**
  - **IEEE 802.1X**
    uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards
  - **Web-based authentication**

provides a browser-based environment, similar to IEEE 802.1X, to authenticate clients that do not support the IEEE 802.1X supplicant
    - **MAC-based authentication**
      authenticates the client with the RADIUS server based on the client's MAC address
- **Secure shell (SSH) v2**
  encrypts all transmitted data for secure remote CLI access over IP networks
- **Secure shell**
  encrypts all transmitted data for secure remote CLI access over IP networks
- **STP BPDU port protection**
  blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks
- **STP root guard**
  protects the root bridge from malicious attacks or configuration mistakes
- **Secure management access**
  delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2 and SNMPv3
- **Custom banner**
  displays security policy when users log in to the switch
- **Secure FTP**
  allows secure file transfer to and from the switch; protects against unwanted file downloads or unauthorized copying of a switch configuration file
- **Protected ports CLI**
  offers intuitive CLI to configure the source-port filter feature, by allowing specified ports to be isolated from all other ports on the switch; the protected port or ports can communicate only with the uplink or shared resources
- **Authentication flexibility**
    - **Multiple IEEE 802.1X users per port**
      provides authentication for up to eight IEEE 802.1X users per port; prevents a user from "piggybacking" on another user's IEEE 802.1X authentication
    - **Concurrent IEEE 802.1X and Web or MAC authentication schemes per port**
      allows a switch port to accept any IEEE 802.1X and either Web or MAC authentications
- **Switch management logon security**
  helps secure switch CLI logon by optionally requiring either RADIUS or TACACS+ authentication
- **DHCP protection**
  blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attacks
- **Dynamic ARP protection:**
  blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data
- **Dynamic IP lockdown**
  works with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing

Convergence

- **LLDP-MED (Media Endpoint Discovery)**
  defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones
- **IP multicast (data-driven IGMP)**
  prevents flooding of IP multicast traffic
- **IEEE 802.1AB Link Layer Discovery Protocol (LLDP)**
  facilitates easy mapping using network management applications with LLDP automated device discovery protocol
- **PoE and PoE+ allocations**
  support multiple methods—automatic, IEEE 802.3at dynamic, LLDP-MED fine grain, IEEE 802.3af device class, or user specified—to allocate and manage PoE/PoE+ power for more efficient energy use
- **Voice VLAN**
  uses LLDP-MED to automatically configure a VLAN for IP phones
- **IP multicast (data-driven IGMPv3)**
  prevents flooding of IP multicast traffic
- **LLDP-CDP compatibility**

receives and recognizes CDP packets from Cisco's IP phones for seamless interoperation

- **Local MAC Authentication**
  assigns attributes such as VLAN and QoS using locally configured profile that can be a list of MAC prefixes

Unified Wired and Wireless

- **HTTP redirect function**
  supports HP Intelligent Management Center (IMC) bring your own device (BYOD) solution

Resiliency and high availability

- **Port trunking and link aggregation**
  - **Trunking**
    supports up to eight links per trunk to increase bandwidth and create redundant connections; and supports L2, L3, and L4 trunk load-balancing algorithm (L4 trunk load balancing is supported only on Gigabit Ethernet and 48-port models.)
  - **IEEE 802.3ad Link Aggregation Control Protocol (LACP)**
    eases configuration of trunks through automatic configuration
- **IEEE 802.1s Multiple Spanning Tree**
  provides high link availability in multiple VLAN environments by allowing multiple spanning trees; provides legacy support for IEEE 802.1d and IEEE 802.1w
- **SmartLink**
  provides easy-to-configure link redundancy of active and standby links

Product Architecture

- **Energy-efficient design**
  - **IEEE 802.3az**
    reduces power consumption during periods of low data activity on Gigabit Ethernet switches
  - **Port low power mode**
    enables the port to automatically go into low-power mode to conserve energy when no link is detected
  - **Fanless and variable-speed fans**
    decreases power consumption in fanless (all 8-port, 2530-24, and 2530-48 PoE+ switches) as well as variable-speed fan switches
  - **Port LEDs**
    conserves energy by optionally turning off port link and activity LEDs
- **Switch on a chip**
  provides a highly integrated, high-performance switch design with a non-blocking architecture

Flexibility

- **Flexible mounting**
  - **Rack mountable**
    allows the switch to be mounted on a standard 19-inch rack, with the hardware included
  - **Wall mountable**
    allows the switch to be mounted on a wall, using the hardware included
  - **Surface mountable**
    allows the switch to be mounted above or below a surface (such as a desk or table), using the hardware included
- **Quiet operation**
  lowers noise, making it suitable for deployments in acoustically sensitive environments such as conference rooms and office spaces
- **Compact size**

reduces space requirements (refer to the product specifications for the exact dimensions)

Warranty and support

- **Limited Lifetime Warranty v2.0**
  Advance hardware replacement with next-business-day delivery (available in most countries). See www.hp.com/networking/warrantysummary for duration details.
- **Electronic and telephone support (for Limited Lifetime Warranty 2.0)**
  limited 24x7 telephone support is available from HP for the first 3 years; limited electronic and business hours telephone support is available from HP for the entire warranty period; to reach our support centers, refer to www.hp.com/networking/contact-support; for details on the duration of support provided with your product purchase, refer to www.hp.com/networking/warrantysummary
- **Software releases**
  to find software for your product, refer to www.hp.com/networking/support; for details on the software releases available with your product purchase, refer to www.hp.com/networking/warrantysummary

9.5 Anexo V. Tecnología IRF de HP

Reducing network complexity, boosting performance with HP IRF technology

White paper

What you will learn in this white paper

The fundamental nature of networking is changing, especially in enterprise data centers. With new, integrated applications deployed against large scale, highly virtualized server farms, server-to-server-center communications are demanding a completely new level of intra-data-center performance. Traditional three-tier networks—designed to support data-center-in/data-center-out traffic and built using legacy, poor-performing redundancy protocols—can't deliver the server-to-server capacity required for these types of workloads.

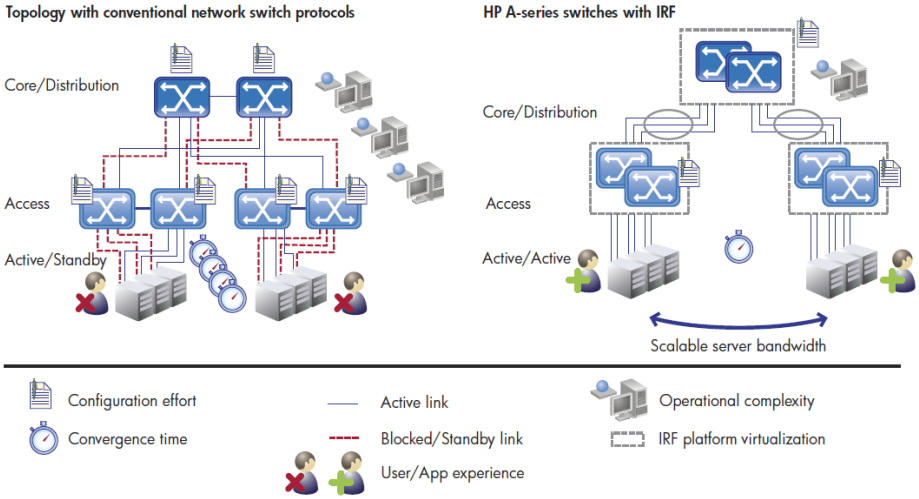
Purpose-built HP networking solutions, system architecture, and technology are streamlining the design of next-generation data centers and campus networks to ensure the superior resiliency, performance, and agility that enterprise networks now require. One HP innovation is Intelligent Resilient Framework (IRF), a technology that far outstrips ordinary protocols designed to improve the performance of network switches. In this white paper you will learn about the challenges associated with conventional switch solutions; the advantages of IRF in terms of manageability, performance, and resiliency; and the very real business benefits that can result from installing HP A-series switches that employ this technology.

HP IRF is an innovative technology that lets you 'flatten' data center and campus networks, eliminating the need for a dedicated aggregation layer and providing more direct, higher capacity connections between users and network resources. And IRF helps customers achieve these goals in a cost-effective, easy-to-manage way.

Traditional network design and resiliency

In a broad spectrum of industries—from healthcare to education, from manufacturing to transportation, from banking to government—organizations depend on their networks to deliver fast, reliable access to information. To provide this speed and reliability, large and enterprise-level networks today are constructed in (typically three) multiple layers: access (also known as network edge) layer; aggregation or distribution layer; and network core layer. The access layer is usually a mesh of network switches, linked to other switches in the aggregation layer, which in turn is linked to the core. The lattice of switches provides multiple paths for network traffic, so if one link or switch goes down, traffic can continue to flow using an alternate path.

Within this web of interlinked switches, Spanning Tree Protocol (STP) is used to detect and prevent loops—a highly undesirable, sometimes disastrous situation that can occur when there are multiple active paths to the same switch. To eliminate loops, STP and its more modern



variants, such as Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP), are designed to allow only one active path from one switch to another, regardless of how many actual connections might exist in the network. If the active path fails, the protocol automatically selects a backup connection and makes that the active path.

What Spanning Tree Protocol is—and is not

STP is widely used, and is fairly effective at making a network resilient—that is, dealing with a sudden failure of a link between switches. In a network that is operating normally, when a link or switch goes down, STP automatically chooses a backup path, and the network reconverges. After a short period, the network is operating normally again. But for modern, high-speed, mission-critical networks, this approach may not be the best solution. Here is why:

Slow network convergence: One problem is that the reconvergence time for STP can be several seconds—a lifetime by modern computing standards. When a garden-variety laptop computer can execute millions of instructions in the blink of an eye, a multi-second network hiccup will have end users cursing the spinning hourglass on their monitors. And a financial transaction that executes in milliseconds cannot wait several seconds for an outdated network protocol to do its job.

Management complexity: Even though MSTP and RSTP converge more quickly than the original STP, all of these protocols can be devilishly difficult to configure properly, especially in a large network. You must manage the switches individually, and need to set up spanning-tree instances on each switch in turn, making sure that the parameters for one switch match those of its neighbor. What's more, troubleshooting spanning-tree-related issues is no easy task, usually requiring a great deal of time to locate the root cause of the failure.

Poor performance: Because it blocks all parallel paths except the one it has selected as active, even when the network is operating normally STP actually reduces the effective bandwidth. In fact, half (or more) of the available system bandwidth can be squandered in a backup role, off-limits to data traffic—not a very good use of the network equipment investment.

Too many tradeoffs: Even the choice of which protocol to use is difficult. For example, consider the decision of how to handle traffic forwarding over redundant links: should you implement MSTP, which is highly efficient but complex, or should you use STP or RSTP, which are less efficient but easier to configure?

HP IRF: a better way

Fortunately, HP networking offers a better way. We call it the Intelligent Resilient Framework, or IRF for short. It's an innovative technology that can actually give you a network that is fully resilient, yet is also simpler to set up and manage, faster to converge, and easier to scale. Let's have a look.

HP IRF platform support

IRF runs on the HP A-series of high-end switches. Developed for customers with large or complex deployments who seek the most advanced, full-featured networking capabilities, the HP A12500, A9500, A7500, A58XX, and A55XX all come with HP IRF technology built-in at no additional cost.

With features like IRF, a common operating system (Comware), and single-pane-of-glass management via HP Intelligent Management Center (IMC), HP networking solutions can help customers simplify the design and operations of their networks.

How it works

IRF technology extends network control over multiple active switches. Management of a group of IRF-enabled switches is consolidated around a single management IP address, which vastly simplifies network configuration and operations. You can combine as many as nine HP A-series switches to create an ultra-resilient virtual switching fabric comprising hundreds or even thousands of 1-GbE or 10-GbE switch ports.

One IRF member operates as the primary system switch, maintaining the control plane and updating forwarding and routing tables for the other devices. If the primary switch fails, IRF instantly selects a new primary, preventing service interruption and helping to deliver network, application, and business continuity for business-critical applications.

Within the IRF domain, network control protocols operate as a cohesive whole to streamline processing, improve performance, and simplify network operation. So routing protocols calculate routes based on the single logical domain rather than the multiple switches it represents. Moreover, edge or aggregation switches that are dual homed to IRF-enabled core or data center switches "see" the associated switches as a single entity, eliminating the need for slow convergence technologies such as STP. And operators have fewer layers to worry about, as well as fewer devices, interfaces, links, and protocols to configure and manage.

Where IRF offers advantages

Employing IRF offers a number of benefits over conventional networking. You will find advantages in three major areas: simplicity, performance, and resiliency.

Advantages in simplicity

- **Design and operational simplification**: With IRF, no longer must you laboriously connect to, configure, and manage switches individually. You perform a configuration on the primary switch, and that configuration is distributed to all associated switches automatically, considerably simplifying network setup, operation, and maintenance. And while all HP A-series switches can be provisioned via the command line, adding HP Intelligent Management Center (IMC) makes management even easier. IMC lets you see and control the entire network from a single console by consolidating management of multiple, discrete devices into a single, easy-to-manage, virtual switch that operates at every layer of the network.
- **Flatter topology**: IRF makes possible a simplified, higher performing, more resilient, and flatter network design. In fact thanks to IRF and HP A-series switches, enterprise networks can be designed with fewer devices and fewer networking layers—a big improvement over the low performance, high cost, and crippling latency of conventional multi-tier legacy solutions, which often rely on a variety of different operating systems and complex resiliency protocols.

Advantages in performance

- **Higher efficiency**: IRF's loop-free, non-blocking architecture keeps all links active, enabling highly efficient, high-bandwidth connectivity throughout the switching plane. Simply stated, you get all the bandwidth you are paying for.
- **Scalable performance**: IRF and Link Aggregation Control Protocol (LACP) used together can further boost performance by bundling several parallel links between switches and servers, allowing scalable "on-demand" performance and capacity to support critical business applications.
- **Faster failover**: Should a network failure occur, IRF can deliver rapid recovery and network reconvergence in under 50 milliseconds—much faster than the several seconds required for STP.

Advantages in resiliency

- **Distributed high availability and resiliency**: For high availability, the IRF fabric can be configured for full N+1 redundancy, while mission-critical virtualization capabilities such as live migration and application mobility are available across the IRF domain and extend across the Layer 2 WAN infrastructure.
- **Geographic resiliency**: Within an IRF domain, the geographic location of switches does not matter. Switches can be extended horizontally, and they continue to function as a single logical unit whether they are installed locally, distributed regionally, or even situated at distant sites. Moreover, employing IRF can enhance disaster recovery by linking installations up to 70 kilometers apart and giving them the same fast failover as if they were sitting side by side within the data center. Such location independence is extremely important to support the global on-demand application access and dynamic traffic flows of today's technology-oriented businesses.
- **In-Service-Software-Upgrade**: IRF delivers a network-based In-Service-Software-Upgrade (ISSU) capability that allows an individual IRF-enabled switch to be taken offline for servicing or software upgrades without affecting traffic going to other switches in the IRF domain.

Table 1. Summing up the advantages of IRF compared to STP-based designs and other solutions

	HP IRF-based designs	STP-based designs	Competitive solutions
Rapid failover	Yes Sub 50 milliseconds	No Often measured in seconds	Varies by protocol
Design simplification—common across data center/campus core/edge	Yes Virtualizes up to 9 switches Common across layers/devices	No Switch by switch configuration	No Different protocols used at each layer and device type
Support for Layer 2/3, MPLS, IPv6 protocols	Yes	L2 only	Varies by protocol
Performance	Very high	Low	High Design/Device specific
Geographic resiliency	Yes Supported across 70 km	No L2 only, limited to site	Unclear Varies by protocol
Overall administration effort and cost	Low No extra cost	High No extra cost	High Often requires additional license and hardware

What you gain

Employing HP A-series switches with IRF offers a wide range of business benefits that are visible not only to network administrators, but to a company's accountants and C-level executives as well.

Greater availability for business-critical applications
HP Intelligent Resilient Framework is particularly well suited to providing the high availability and consistent service levels required in mission-critical deployments. Its simpler architecture, faster failover, and greater resilience add up to marked improvements in availability over architectures based on Spanning Tree and other conventional network protocols.

Increased performance and better network ROI
Because it allows redundant links to be active without creating loops, IRF technology can use the full capabilities and bandwidth of each switch, ensuring greater overall efficiency and maximizing return on the investment in networking infrastructure.

Lower operating costs
By allowing a flatter, fully resilient topology, IRF can actually reduce the number of components in the network; this has the advantage of lowering costs for power and cooling, greatly simplifying network planning and operation, and freeing staff for more productive tasks. The result is reduced overall operating and administrative expenses.

Investment protection

Using standards-based protocols such as LACP, HP IRF switches can interoperate with the existing switches deployed in your network, providing investment protection and seamless migration.

Summing up

The HP approach to networking is focused on driving innovation that reduces complexity, delivers breakthrough economic benefits, and empowers customers to deploy the network as a business enabler. This approach is fully developed in HP A-series switches with IRF, a technology that can deliver excellent resiliency along with less complexity and better performance throughout your switched network.

Want to learn more?

Visit the HP website to learn more about HP networking and how to contact us. See: **www.hp.com/go/networking**

9.6 Anexo VI. UTM WatchGuard

Unified Threat Management - Market Review

Price/performance comparison: WatchGuard vs. Juniper, Fortinet, Cisco, and SonicWall

April 2010

WHAT YOU LOOK FOR IN ANY NETWORK SECURITY PURCHASE

Choosing the right network security solution is one of the most important decisions you will make for your IT infrastructure. With so many factors to consider when selecting the right product, it's easy to lose sight of one of the most important goals: getting the best performance for your security dollar.

Comparing the major brands by this all important metric – price/performance – can become a difficult chore. Though Cisco, Fortinet, Juniper, and SonicWall make it possible to derive this metric based on their own published numbers, WatchGuard has taken the next step and put them all together for you – so you can make a direct comparison among Unifed Threat Management vendors.

UTM PERFORMANCE

As networks demand more and more efficiency, unified threat management (UTM) solutions have come to dominate the firewall/VPN market. Where once a network would have one firewall and a number of point solutions protecting the gateway, all the necessary security features – firewall, VPN, endpoint, web content filtering, spam blocking, virus protection, intrusion prevention, numerous networking features, and more – have become integrated into a single network security appliance. The efficiencies of a single solution securing a gateway from top to bottom are easy to imagine; it's why UTM dominates the market.

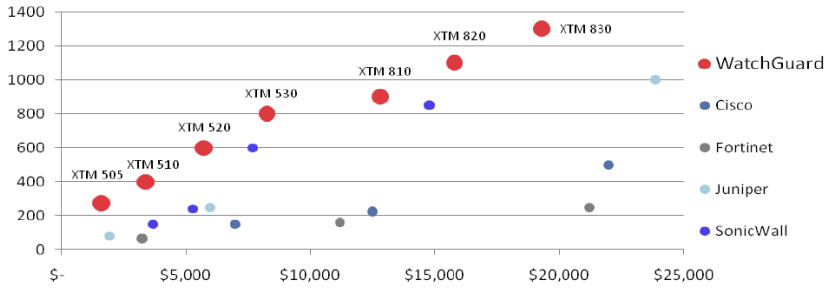
WatchGuard XTM solutions actually push beyond the UTM paradigm into what is called **extensible threat management**, offering features far beyond normal security functions, automating processes, and allowing future growth as security threats evolve.

The only potential downside of a single UTM appliance being responsible for so much of a network's security is that the processing demands placed on that appliance could result in slower performance.

Building on 14 years of experience, WatchGuard has been able to design solutions to handle threats more efficiently than our competitors and maintain strong performance no matter what you throw at it. With our latest release of WatchGuard XTM Series appliances, we have leap-frogged the competition in offering the best UTM performance per dollar spent.

Price/Performance - WatchGuard vs. the Competition

Note that the horizontal axis is a statement of price; the vertical axis is the measure of performance speed. Appliances with lower price and higher performance appear higher and further to the left in the charts.



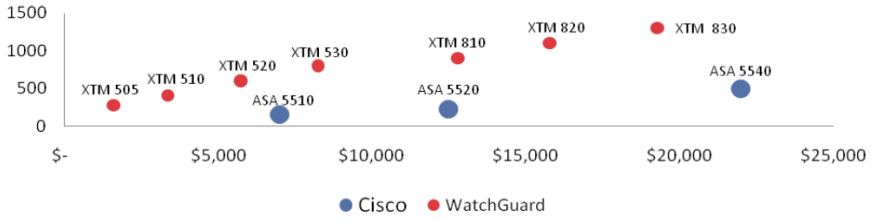
MSRP among major brands and corresponding UTM throughput performance in Mbps. Some brands do not offer full UTM functions. In these cases, performance with all available features is shown.

PUTTING THEM HEAD-TO-HEAD

Among all major brands, when you turn on every possible layer of protection at the gateway and start processing data, WatchGuard gives you the best performance per dollar spent. It is plain to see that no other brand comes close to the performance for the price.

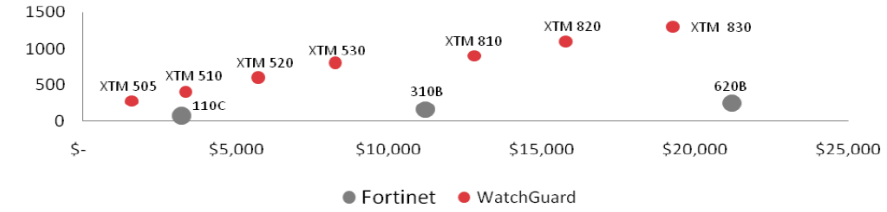
Our price/performance leadership position is even stronger when you consider that many of the competing solutions are not even true UTM devices. Many are missing crucial functions that require you to purchase additional servers and point solutions to build out your network security portfolio. WatchGuard does it all—without slowing down.

WatchGuard vs. Cisco



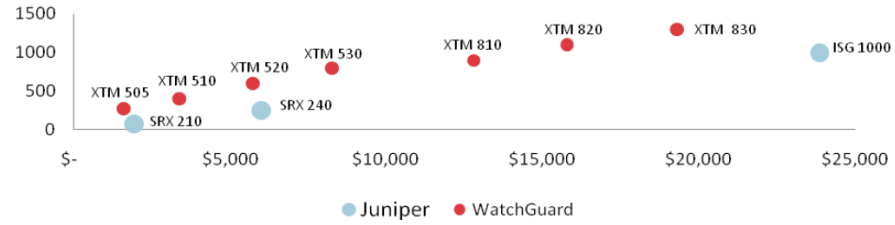
The old adage, "No one ever gets fired for buying Cisco" is showing its age. Cisco is not a true UTM: the ASA devices run either IPS or content security but not both. WatchGuard offers far more complete and in-depth security while still easily out-performing the ASA.

WatchGuard vs. Fortinet



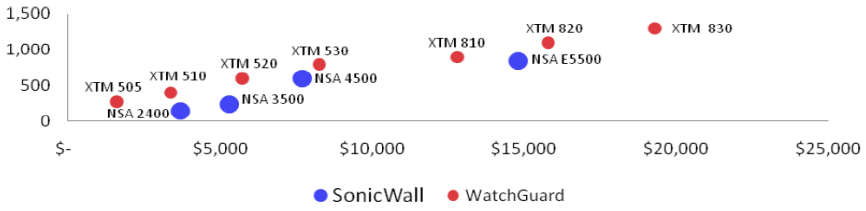
The most recent Fortigate appliances from Fortinet still suffer from the same issues their past products have. Their performance, when doing basic packet filtering, is strong. But as soon as basic functions such as AV and IPS scanning are turned on the performance takes a deep nose dive. Their technology is simply not well suited for UTM.

WatchGuard vs. Juniper



Juniper's lower end SRX devices lack some important features such as HTTPS inspection and integrated SSL VPN capabilities. The higher end ISG products are not even true UTM devices. They are limited to firewall, VPN, and intrusion detection and prevention.

WatchGuard vs. SonicWall



SonicWall touts "reassembly free inspection," which essentially does only part of the job. Without reassembling packets, common fragmented attacks pass right through their security undetected. Despite the gap in security this creates, it indeed reduces the processing needs of their boxes. However, even with this "advantage," the NSA products still can't match WatchGuard XTM, which doesn't sacrifice security for performance.

TOTAL COST OF OWNERSHIP

As anyone who has made a major IT infrastructure purchase knows, your initial outlay for a solution is not the whole story. The services and updates necessary to keep a UTM appliance at top performance add up over the life of the appliance and this must be taken into consideration before making a decision.

Typically, IT administrators pick solutions with a performance buffer so minor increases in network demands don't turn the solution into a bottleneck. Unfortunately this can exaggerate your total cost of ownership over the life of the product.

If you want to be sure your network won't push the solution's limits in the foreseeable future, you may have to pay for a solution sized for a much larger network. And you won't pay more just initially, but will continue to pay for more expensive services meant for larger networks.

Because WatchGuard solutions lead the industry in price/performance, you get the performance buffer you need without the outsized costs. The result is a solution that out performs any other and keeps you well within your budget.

WatchGuard also offers a unique model upgrade for those that grow even faster than they hope. A simple license key allows you to increase performance and capacity quickly and inexpensively, without ripping and replacing hardware.

YOUR NEXT STEPS

Even if you are not currently in the market for a security solution upgrade, the security and cost benefits offered by a WatchGuard XTM Series solution are well worth a look. (See WatchGuard Trade Up Program for more details on our attractive replacement program.) And if you are already shopping, here are resources to help you do your homework to find the right solution for you. WatchGuard Resource Center

We are confident that WatchGuard XTM solutions will more than meet your requirements but know you will want to compare products before you make a final choice. Speak with one of our certified resellers who can help you properly size a solution for your unique network environment. Then compare brands like Cisco, Fortinet, Juniper, and SonicWall to see what they have to offer. You are never going to know how a solution will perform until you have tested it under real world conditions so we also offer a free evaluation program.

If you would like assistance getting started, our dedicated WatchGuard experts would be happy to help.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

NORTH AMERICA SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.

9.7 Anexo VII. Cotización 01 para Propuesta de Escazú

Cotización #186062

Alfatec, S.A.

Teléfono (506) 2215-3850

Alfatec, S.A.

Numero de Documento		186062	Fecha de documento	12/07/2017
Socio de Negocio	C1257		Válido hasta	12/08/2017
Para	LABORATORIOS STEIN S.A.		Fecha	12/07/2017
Teléfono	2550-6500		Agente	Alfa03
Dirección de envío	LABORATORIOS STEIN S.A. Cartago 1 km sur cruze a taras		Condición de pago	30 dias
	COSTA RICA			
Correo Electrónico				

#	Código	Producto	Cantidad	Precio	Total
1	EP	WATCHGUARD PUNTO DE ACCESO AP120 CON 3 AÑOS DE SUSCRIPCION EN LA NUBE Y SOPORTE ESTANDAR	7	USD 770.00	USD 5,390.00
2	EP	WATCHGUARD KIT DE MONTAJE PARA INTERIORES PARA AP120	7	USD 16.00	USD 112.00
3	EP	ARUBA 2530 SWITCH 48G PoE+ J9772A	4	USD 1,835.00	USD 7,340.00
4	EP	HPE GARANTIA EXTENDIDA 5 AÑOS NBD PARA ARUBA 2530 48G	4	USD 695.00	USD 2,780.00
5	EP	ARUBA 2530 SWITCH 24G PoE+ J9773A	1	USD 962.00	USD 962.00
6	EP	HPE GARANTIA EXTENDIDA 5 AÑOS NBD PARA ARUBA 2530 24G	1	USD 370.00	USD 370.00
7	EP	SERVICIO DE CONFIGURACION E INSTALACION A 0 METROS DE 7 ACCESS POINT WATCH GUARD	1	USD 500.00	USD 500.00
8	EP	SERVICIO DE CONFIGURACION BASICA DE SWITCHES ARUBA	1	0.00	USD 0.00

Observaciones	PLAZO DE ENTREGA 3 SEMANAS	Subtotal	USD 17,454.00
		Impuesto	USD 2,269.02
		Descuento	*(% 0.00)* USD 0.00
		Total	USD 19,723.02

9.8 Anexo VIII. Cotización 02 para Propuesta de Escazú

COMPONENTES EL ORBE
San José, Costa Rica, Barrio Montelimar, 25mts.
este de Los Tribunales de Goicochea
Céd. Jurídica: 3-101-111502 - Central: 2545-4700

COMPAÑIA COTECNA ISO 9001 CERTIFICADA
COMPAÑIA COTECNA ISO 14001 CERTIFICADA
Hewlett Packard Enterprise Latin America Partner of the Year 2016
Partner First Platinum

OFERTA: 2168-17-07-04

Empresa:	**Laboratorios Stein S,A**
Dirección:	**Cartago**
Atención:	**Jonathan Cruz Hidalgo**
E-mail:	jcruz@labstein.com
Teléfono	**25506500** **Fax:**

Fecha:	**21-Jul-17**
Ejecutivo:	**Juan José Chanto**
Teléfono	**2545-47-37**
E-mail:	jchanto@orbe.co.cr

Cant.	Código	Descripción	Garantía (Meses)	Precio Unitario	Precio Total
7	WGA12701	WatchGuard AP120 - wireless access point - WatchGuard Trade Up Program / T/U TO AP120 AND 3YR WLS CLD SUB STD SUP/3 years warranty Wall/ceiling mounting plate/ WatchGuard Wi-Fi Cloud (3 years subscription)	36	$775.36	$5,427.52
4	J9772A	ARUBA 2530-48G-POE+ - SWITCH - 48 PORTS - MANAGED - RACK-MOUNTABLE Switch - managed - 48 x 10/100/1000 (PoE+) + 4 x Gigabit SFP - desktop, rack-mountable, wall-mountable - PoE+	60	$1,888.39	$7,553.55
4	H1KE8E?LA	HPE FOUNDATION CARE NEXT BUSINESS DAY EXCHANGE SERVICE - EXTENDED SERVICE AGREEMENT - 5 YEARS - SHIPMENT	60	$710.12	$2,840.48
1	J9773A?LA	ARUBA 2530-24G-POE+ - SWITCH - 24 PORTS - MANAGED - RACK-MOUNTABLE Aruba 2530-24G-PoE+ - Switch - managed - 24 x 10/100/1000 (PoE+) + 4 x Gigabit SFP - desktop, rack-mountable, wall-mountable - PoE+	60	$989.37	$989.37
1	H1HS9E?LA	HPE Foundation Care Next Business Day Service with Comprehensive Defective Material Retention - Extended service agreement - parts and labor - 5 years - on-site - 9x5 - response time: NBD - for Aruba 2530-24G-PoE+, 2530-24-PoE+	60	$561.15	$561.15
				Sub Total	$17,372.06
				13% I.V.	$2,258.37
				TOTAL	$19,630.43

CONDICIONES GENERALES:

Entrega: 22 a 30 días hábiles

Forma de Pago: Crédito
Vigencia de la Oferta: 8 días naturales

No incluye instalación.

No incluye transporte fuera del Area Metropolitana

THALES "Outstanding Partner of the Year Americas" · cisco · Distribuidor Autorizado · VEEAM · FORTINET · Lenovo
EPSON EXCEED YOUR VISION · aruba NETWORKS MCA networking partner of the year · Adobe GOLD Partner · Symantec. Gold Partner · vmware "Rising Star of the Year 2015 for Americas" · Microsoft CERTIFIED Partner

3653-1000 San José, Costa Rica Teléfono: 2545-4700 Fax: 2545-4701 Servicio Técnico: 2234-3462

9.9 Anexo IX. Cotización 03 para Propuesta de Escazú

Grupo SEGA

Microsoft Partner
Gold Server Platform
Gold Volume Licensing
Silver Customer Relationship Management

DELL CERTIFIED PARTNER SOLUTIONS

San José, 03 de Agosto, 2017

Señores:
SteinCORP
Atención: Jonathan Cruz Hidalgo
Presente

Estimado Señor Cruz:

GRUPO SEGA es una empresa con más de 25 años en el mercado de la tecnología y cuya filosofía es de una total orientación al servicio y soporte al cliente.

Como ***"Microsoft Licensing Solution Provider (LSP)"***, podemos proveerle de una solución completa de integración y automatización en su empresa. Abarcando desde la venta de equipo, software y herramientas, hasta la implementación de sistemas complejos, incluyendo soporte, asesoría y consultoría.

Adicionalmente, para atender sus necesidades regionales, contamos con servicio en cada país de Centro América desde El Salvador hasta Panamá. Agradecemos la confianza depositada en nosotros.

Para conocer más acerca de nuestros servicios, ingrese a nuestra página web http://www.gruposega.net/web/cr/inicio/

Quedamos a sus órdenes para resolver cualquier inquietud

Gustavo Núñez C.
Gerente de Cuentas
GRUPO SEGA
Centro Corporativo Atrium, Primer Piso
Escazú, San José, Costa Rica
Oficina: (506) 4052-8200
Móvil: (506) 7105-4055
Fax: (506) 2537-9558
Correo: gustavon@gruposega.net
Skype: gustavonunezc

Switch HP 2530-48G-POE - 48 puertos PoE

Especificaciones Técnicas	
Puertos	(48) Puertos RJ-45 PoE+ 10/100/1000 con detección automática (4) Puertos SFP Gigabit Ethernet fijos
Memoria y procesador	ARM9E a 800 MHz flash de 128 MB Tamaño de búfer para paquetes: 3 MB asignados dinámicamente 256 MB de DIMM DDR3
Latencia	Latencia de 100 Mb: < 7,4 µs Latencia de 1000 Mb: < 2.3 µs
Velocidad	hasta 77,3 Mpps
Capacidad de Switching	104 Gbps
Función PoE	382 W
Capacidad de apilado	Virtual 16 conmutadores
Funciones de gestión	Aruba AirWave Network Management IMC - Intelligent Management Center Interfaz de línea de comandos Navegador web Menú Configuración Administración fuera de banda (RS-232C serie o micro USB) MIB Ethernet IEEE 802.3 MIB de repetidor MIB de interfaz Ethernet
Voltaje de entrada	100 - 127 / 200 - 240 VCA, valor nominal
Margen de temperaturas operativas	De 0 a 45°C
Intervalo de humedad en funcionamiento	15 a 95% a 104°F (40°C), (sin condensación)
Consumo de energía	476 vatios (máximo)
Disipación del calor	236 BTU/h (248,98 kJ/h)
Dimensiones mínimas (anch. x prof. x alt.)	44,3 x 32,26 x 4,45 cm
Peso	4,72 kg

Switch HP 2530-24G-POE - 24 puertos PoE

Especificaciones Técnicas	
Puertos	(24) Puertos RJ-45 PoE+ 10/100/1000 con detección automática (4) Puertos SFP Gigabit Ethernet fijos
Memoria y procesador	ARM9E a 800 MHz flash de 128 MB Tamaño de búfer para paquetes: 1.5 MB asignados dinámicamente 256 MB de DIMM DDR3
Latencia	Latencia de 100 Mb: < 7,4 µs Latencia de 1000 Mb: < 2.3 µs
Velocidad	hasta 41,6 Mpps
Capacidad de Switching	56 Gbps
Función PoE	195 W
Capacidad de apilado	Virtual 16 conmutadores
Funciones de gestión	Aruba AirWave Network Management IMC - Intelligent Management Center Interfaz de línea de comandos Navegador web Menú Configuración Administración fuera de banda (RS-232C serie o micro USB) MIB Ethernet IEEE 802.3 MIB de repetidor MIB de interfaz Ethernet
Voltaje de entrada	100 - 127 / 200 - 240 VCA, valor nominal
Margen de temperaturas operativas	De 0 a 45°C
Intervalo de humedad en funcionamiento	15 a 95% a 104°F (40°C), (sin condensación)
Consumo de energía	247 vatios (máximo)
Disipación del calor	135 BTU/h (142,42 kJ/h)
Dimensiones mínimas (anch. x prof. x alt.)	44,3 x 33,02 x 4,45 cm
Peso	3,95 kg

Grupo SEGA

Microsoft Partner
Gold Server Platform
Gold Volume Licensing
Silver Customer Relationship Management

DELL CERTIFIED PARTNER

PROPUESTA ECONOMICA

Cantidad	Número de Parte	Descripción de Producto	Precio Unitario	Total
4	J9772A	Aruba 2530 48G PoE+ Switch	$1 897,73	$7 590,92
4	H1KE8E	HPE 5Y FC NBD Exch Aruba 2530 48G PO SVC	$732,95	$2 931,80
1	J9773A	Aruba 2530 24G PoE+ Switch	$994,32	$994,32
1	H1HS4E	HPE 5Y FC NBD Exch Aruba 2530 24G PO SVC	$390,91	$390,91
		--Ultima Linea--		

Sub total	$ 11 907,95
I.V.	$ 1 548,03
Transporte	$ 70,00
Total	$ 13 525,98

Nota:

- Los precios por transporte y otros insumos están calculados con los modelos y cantidades detalladas arriba, en caso de cambio de modelos o cantidades hay que realizar los cálculos nuevamente.

CONDICIONES GENERALES

FORMA DE PAGO:

Crédito a 30 días posterior a la fecha de facturación.
Emitir cheque o por medio de acreditamiento a cuenta, en dólares o colones a nombre de Segacorp de Costa Rica, S.A.

TIEMPO DE ENTREGA: Entre 3 y 4 semanas después de recibir la orden de compra

GARANTIA Y SERVICIO: 5 años, next business day

VENCIMIENTO DE LA OFERTA: 31 Agosto 2017

9.10 Anexo X. Cuadrante Mágico de Gartner para LAN 2014

9.11 Anexo XI. Cuadrante Mágico de Gartner para LAN 2015

9.12 Anexo XII. Cuadrante Mágico de Gartner para LAN 2016