UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA: INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de: INGENIEROS ELECTRÓNICOS

TEMA:
ANÁLISIS Y DISEÑO DE BRING YOUR OWN DEVICE SOBRE LA RED INALÁMBRICA DE LA UNIVERSIDAD POLITÉCNICA SALESIANA CAMPUS SUR

AUTORES:
ANDREA ESTEFANIA DÍAZ SUBIA
LINO DANILO LAMAR TENELEMA

DIRECTOR:
JOSÉ LUIS AGUAYO MORALES

Quito, marzo del 2015

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE TITULACIÓN

Nosotros, autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su reproducción sin fines de lucro.

Además declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Quito, marzo del 2015

_____	_____
Andrea Estefania Díaz Subia	Lino Danilo Lamar Tenelema
CC: 1721881892	CC: 1716332372

DEDICATORIA

Dedico este proyecto de titulación a Dios y a mis padres que son mi apoyo para seguir adelante, que con su confianza y comprensión me han ayudado a cumplir mis metas y han hecho de mí una mejor persona con su ejemplo de lucha y superación.

También dedico a todas aquellas personas que con su apoyo incondicional han formado parte te este sueño.

Andrea Estefania Díaz Subia

Dedicado a Dios, por concederme la salud y el tiempo para alcanzar una de las metas propuestas. A mis padres y hermanas por su amor, ejemplo y compresión para protegerme, guiarme por este sendero, estando en las buenas y malas conmigo, apoyándome en todas las decisiones de mi vida. A mis familiares y amigos a todos aquellos que influenciaron mis pasos y acciones; por sus consejos, ayuda, compañía y sobre todo por el tiempo compartido con ellos. A mis catedráticos por haber contribuido a mi formación personal y profesional. A la universidad por bridarme la oportunidad de haber estudiado en sus aulas.

Todo lo que soy es gracias a ustedes.

Lino Danilo Lamar Tenelema

AGRADECIMIENTO

A la Universidad Politécnica Salesiana Campus Sur por habernos abierto sus puertas para que nos podamos formar como profesionales y personas de bien para la sociedad, además de pertenecer a tan selecto grupo de profesionales. Buscaremos siempre mantener en alto su nombre donde sea que nos encontremos.

A sus docentes quienes nos impartieron sus experiencias y conocimientos a lo largo de nuestra vida universitaria.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

La tendencia en las redes de ordenadores es gestionar tanto las normas de seguridad inalámbrica como sus equipos de red, con el fin de obtener la granularidad en la misma, proporcionando una mejor gestión por el departamento de Tecnología de la Información (TI) mediante la mejora de las políticas actuales o mediante la implementación de nuevas reglas.

Traiga su propio dispositivo (BYOD), es una tendencia de diseño de redes de infraestructura basada en Cisco que apunta a través de la red inalámbrica de la Universidad Politécnica Salesiana, Campus Sur, dando una respuesta al aumento de los dispositivos, proporcionando una calidad de servicio y seguridad en toda la red inalámbrica, mediante la creación de políticas o en los usuarios o en los dispositivos. El análisis y el diseño de la infraestructura de la red piloto se basa en la solución de Cisco Meraki usando gestión de dispositivos móviles (MDM) y el sistema de gestión de Meraki Z1, que están alojados en la nube.

Las pruebas se llevaron a cabo con diferentes dispositivos de usuario conectados a la red piloto y gestionados por Cisco Meraki, tanto para la navegación y aplicaciones en tiempo real, mostrando: facilidad de conexión, QoS, la flexibilidad, la seguridad en toda la red, la configuración de las políticas y mejor ancho de banda para cada conjunto de dispositivos que pertenecen una red inalámbrica.

ABSTRACT

The trend in computer networks is manage both the wireless security rules as their network equipments, in order to gain granularity in the networking by providing a better management by Information Technology department (IT) management by improving current policies or by implementing new rules.

Bring your Own device (BYOD), is a networking trend design by infrastructure based on Cisco that aims to over the wireless network of Universidad Politécnica Salesiana, South Campus, giving a response to increased of devices, providing quality of service and security in the whole wireless network, by creating policies or in users or in devices . The analysis and design of the pilot network infrastructure is based on Cisco Meraki's solution using: Mobile Device Management (MDM) and Meraki Z1 management system, which are housed in the cloud.

Tests were conducted with different user devices connected to the pilot network and managed by Cisco Meraki, both for navigation and real time applications, showing: ease of connection, QoS, flexibility, security in whole network, policies shaping and better bandwidth for each set of devices that belong at wireless network.

INTRODUCCIÓN

A raíz del gran crecimiento que experimentan los usuarios de dispositivos móviles, se puede observar como ellos aprovechan su portabilidad y las facilidades de conexión para utilizarlos como una herramienta de trabajo o estudio, esto se debe al auge de las tecnologías de la información. Muestra de estos son el ejecutivo que ha adquirido un dispositivo móvil, para mejorar su productividad personal, hasta el profesor universitario que ha adaptado el diseño de su curso para aprovechar las ventajas de las nuevas aplicaciones educativas basadas en tablet.

Hoy en día muchas universidades y empresas a nivel mundial están cambiando su enfoque al uso de dispositivos móviles en el campus, para abrazar Bring Your Own Device (BYOD) como una ayuda tecnológica que puede mejorar la enseñanza y el aprendizaje, mejorar el rendimiento del estudiante, contribuir con la eficiencia operativa, aumentar la productividad del personal, ampliar la colaboración e incrementar las capacidades de las infraestructuras tecnológicas existentes.

Este proyecto consiste en realizar un análisis y diseño de la red inalámbrica de la Universidad Politécnica Salesiana, para que soporte BYOD. El cual está divido en cinco capítulos.

En el capítulo uno, se dará una idea del porqué de la realización de este proyectó, con la descripción del problema, su planteamiento, además de justificación, junto con sus objetivos, el alcance y la metodología de investigación a seguir.

El capítulo dos, trata acerca del marco teórico que se involucra en este proyecto.

El capítulo tres, contiene toda la recopilación de la información sobre la infraestructura actual de la red inalámbrica.

En el capítulo cuatro, se realizará el diseño y simulación de la red inalámbrica con BYOD.

En el capítulo cinco, se realizará el análisis de pruebas obtenidos de los resultados, junto con el análisis de costos, para de esta manera llegar finalmente a las conclusiones y recomendaciones, producto de la realización de este proyecto.

CAPÍTULO 1
ANTECEDENTES

1.1 Descripción del problema.

Cada vez son más las personas que desean utilizar sus propios ordenadores portátiles, tablets, smartphones y otros dispositivos móviles en el sector educativo, empresarial, entre otros. Esto hace que los gestores de tecnologías de la información tengan que rediseñar su infraestructura de red en función de las necesidades de los usuarios, es por esto que aparece esta tendencia conocida como Bring Your Own Device (BYOD), que en español es "Traiga su propio dispositivo", la cual se está propagando a nivel mundial, debido al gran incremento que sufre la tecnología móvil y en la cual la Universidad Politécnica Salesiana también es un escenario propicio para que se de este fenómeno, el cual afectará a la red inalámbrica, por lo que el presente proyecto busca analizar y diseñar una red inalámbrica para que soporte BYOD en dicha institución.

1.2 Planteamiento del problema.

En la actualidad, con el incremento de la población estudiantil en la Universidad Politécnica Salesiana en el Campus Sur, aumenta también el número de dispositivos móviles, según el departamento de Tecnologías de la Información en los últimos cinco años se registra una tendencia al incremento de dispositivos móviles conectados a la red inalámbrica de la Universidad Politécnica Salesiana Campus Sur.

Por otro lado, los recursos de la red son aprovechados por las personas que habitan en lugares aledaños a la institución, quienes se conectan a esta red sin tener ningún tipo de vinculación con la universidad prueba de ello es el aumento del consumo de los recursos que se tiene en la noche, y no se puede saber quién se conecta a la red sin tener los permisos, ante esta problemática este proyecto pretende contribuir al control de la red.

1.3 Justificación.

Debido a la masificación de los dispositivos móviles personales por parte de la comunidad Salesiana, surge la necesidad de conocer qué equipos están conectados a la red de la institución, así como tener el control con una mejor conexión y que esta sea segura, ante la exigencia de que la red inalámbrica esté apta para recibir tal incremento en las conexiones. En este proyecto pretende con Bring Your Own Device, satisfacer las conexiones a la red institucional, aplicando mejores políticas en el uso de los recursos de red, simplificando de esta manera la administración por parte del departamento de Tecnologías de la Información de la Universidad, en la red inalámbrica de la UPS Campus Sur.

1.4 Objetivos.

1.4.1 Objetivo general.

Analizar y diseñar Bring Your Own Device sobre la red inalámbrica de la Universidad Politécnica Salesiana Campus Sur.

1.4.2 Objetivos específicos.

- Levantar la información de la red inalámbrica de la UPS.
- Analizar la infraestructura de la red actual que tiene la UPS.
- Aplicar políticas sobre la red inalámbrica de la UPS para cumplir BYOD de manera en que los administradores del departamento de Tecnologías de la Información pueden administrar la red.
- Diseñar y simular una infraestructura de red basada en BYOD con los requerimientos de la universidad sobre una red piloto.
- Realizar las pruebas de funcionamiento de BYOD y su análisis de resultados.
- Proponer recomendaciones al departamento de Tecnologías de la Información de la Universidad Politécnica Salesiana campus Sur para cumplir BYOD.

1.5 Alcance y limitaciones.

El análisis y diseño de BYOD sobre la red inalámbrica de la Universidad Politécnica Salesiana Campus Sur, se limita a dicho centro educativo, y en el cual se realizará:

- El estudio de la infraestructura de red.
- El diseño de la red inalámbrica para que soporte BYOD.
- Se simulará sobre una red piloto una topología física y lógica de acuerdo a los requerimientos anteriormente determinados, luego se generarán las políticas necesarias para el correcto funcionamiento de BYOD junto con las pruebas respectivas.
- Se realizará la factibilidad tanto técnica como económica del proyecto en base a toda la información obtenida y a los requerimientos de la universidad para una arquitectura de red basada en BYOD. Finalmente, de los datos obtenidos, se generarán una serie de recomendaciones para cumplir con BOYD.

Este proyecto no realizará lo siguiente:

- Implementación de BYOD sobre la red inalámbrica de la Universidad Politécnica Salesiana Campus Sur, ni en hardware ni en software.
- Cambios sobre las políticas actuales de la red inalámbrica de la UPS Campus Sur.

1.6 Metodología de la investigación.

Todo este proceso investigativo utilizará varias técnicas de recolección de datos como: la observación, entrevistas, encuestas, etc. Cada una de las cuales se aplicarán en el proyecto dependiendo de la información a adquirirse. A continuación se describen de manera general las actividades a realizar:

Para realizar este proyecto se empezará con una previa recolección de fuentes bibliográficas y tecnológicas, en las cuales se revisarán las características de las comunicaciones inalámbricas, además de los factores que exige BYOD.

Se realizará la recopilación de información a través de una investigación de campo acerca de la infraestructura de red, para poder determinar el perfil del funcionamiento actual de la red inalámbrica que posee la Universidad en el Campus Sur, los cuales permitirán realizar el diseño de red para que soporte BYOD, luego con los aspectos relevantes se podrán aplicar BYOD sobre la red piloto, a la cual se le realizarán

pruebas para ver su comportamiento y con esto obtener los resultados, conclusiones y de esta manera se finalizará con la documentación del proyecto.

CAPÍTULO 2
MARCO TEÓRICO

2.1 Redes inalámbricas.

Las redes inalámbricas utilizan ondas electromagnéticas para enviar y recibir datos, usan el aire como medio de transmisión, tienen varios tipos de cobertura facilitando el acceso a lugares donde es imposible utilizar cables (Telcommunity, 2014).

2.1.1 Clasificación de las redes inalámbricas.

En la figura 1 se observa la clasificación de estas de redes según el área de cobertura.

Clasificación de las redes inalámbricas.

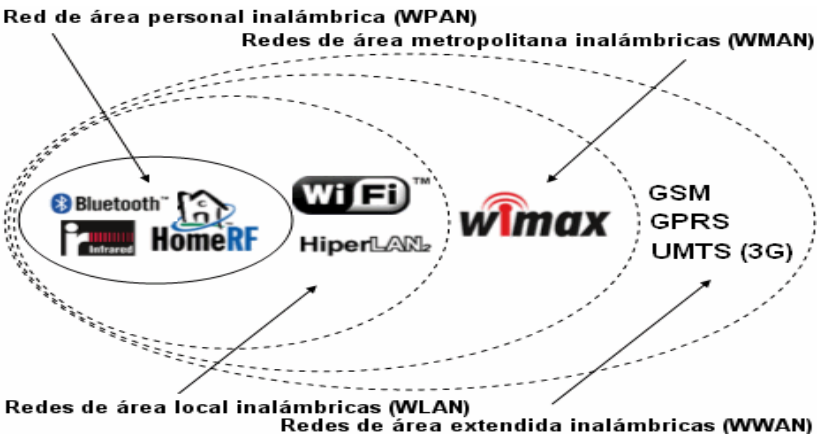


Figura 1. Clasificación de las redes inalámbricas. Fuente: Kioskea.net.

2.2 Red de área local inalámbrica (Wireless Local Area Network WLAN).

WLAN es una clasificación de la redes inalámbricas, ofrecen frente a la red cableada movilidad, flexibilidad para realizar cambios en la red de forma sencilla y rápida, reduce el costo de recursos para implementar este tipo de red. Se la utiliza en hogares, oficinas, campus, etc. (Stallings, 2005, pág. 406).

2.2.1 Estándar IEEE 802.11 y sus principales variantes para WLAN.

El estándar IEEE 802.11 define como se utiliza radiofrecuencia en la capa física y la capa de enlace de datos. Hay algunas variantes del estándar 802.11 que se las puede ver en la tabla 1.

Tabla 1.
Principales variantes del estándar IEEE 802.11.

Estándar	Velocidad	Frecuencia	Compatibilidad	Observaciones
802.11	2 Mbps	2.4 GHz	----------	Estándar original
802.11a	54 Mbps	5 GHz	----------	Poco utilizado
802.11b	11 Mbps	2.4 GHz	----------	Interferencia
802.11g	54 Mbps	2.4 GHz	802.11b	Interferencia
802.11n	600 Mbps	2.4 GHz y 5 GHz	802.11a/b/g	Utiliza MIMO
802.11ac	1.3 Gbps	5 GHz	802.11a/n	Beamforming
802.11ad	7 Gbps	2.4 GHz, 5 GHz y 60 GHz	802.11a/b/g/n/ac	"WiGig"

Nota. Variantes del estándar IEEE 802.11.
Elaborado por: Andrea Díaz y Danilo Lamar.

2.3 Seguridad en redes inalámbricas.

En redes inalámbricas, se corre el riesgo de que se vulnere la seguridad, ya que la información se percibe en cualquier equipo que esté dentro del área de cobertura. Algunas amenazas son: acceso no autorizado, intercepción de datos, interferencia, ataques de denegación de servicio, etc. (Creative Commons, 2007, págs. 158 - 161).

2.3.1 Métodos de seguridad en redes inalámbricas.

Existen varios métodos para proteger una red inalámbrica, los cuales se pueden usar en conjunto o por separado. A continuación se revisan los más conocidos.

2.3.1.1 Identificador de conjunto de servicios (Service Set Identifier, SSID)

El SSID es un identificador de red, que se difunde a través de un punto de acceso (Lewis & Davis, 2004, pág. 191).

2.3.1.2 Control de acceso al medio (Media Access Control, MAC)

El filtrado MAC permite especificar una lista de las direcciones físicas de los adaptadores de red que pueden acceder a la red inalámbrica a través de un punto de acceso (Lewis & Davis, 2004, págs. 191 - 193).

2.3.1.3 Privacidad equivalente al cableado (Wired Equivalent Protocol, WEP).

WEP fue diseñado para proteger los datos en las redes inalámbricas, usando mecanismos de encriptación y autenticación por medio de clave, estas pueden ser de 64 bits, 128 bits y 256 bits, deben estar en el punto de acceso y ser compartidas con los diferentes clientes móviles (Tortosa, 2005, págs. 11 - 13).

2.3.1.4 Estándar IEEE 802.1X.

Se encarga del control de acceso y autenticación a la red, estableciendo una conexión punto a punto para transportar la información de identificación del usuario. La arquitectura IEEE 802.1X está formada por tres entes (Geier, 2008, págs. 33 - 40):

- El suplicante que se une a la red (cliente).
- El autenticador que hace el control de acceso (punto de acceso).
- El servidor de autenticación toma las decisiones de autorización (RADIUS).

2.3.1.5 Acceso protegido Wi-Fi (Wi-Fi Protected Access, WPA).

WPA es una versión del protocolo 802.11i y del algoritmo TKIP (Temporal Key Integrity Protocol), provee una encriptación fuerte y utiliza una clave privada compartida, la cual cambia cada cierto tiempo. Los datos del usuario se chequean usando el protocolo 802.1X, en un servidor de autenticación como RADIUS (Stallings, 2005, pág. 453).

2.3.1.6 Estándar IEEE 802.11i.

El estándar IEEE 802.11i (WPA2), se basa en el cifrado TKIP, también admite AES (Advanced Encryption Standard) considerado como una técnica de encriptación de alta seguridad debido a que su algoritmo es complejo al tener claves robustas, utiliza CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), que surgió para remplazar a TKIP, y el cual es obligatorio en el estándar 802.11i (Lehembre, 2006, págs. 17 - 22). WPA2 define dos modos de trabajo:

- **WPA-Personal:** utiliza una clave compartida, llamada PSK (Pre-Shared Key) que está tanto en el punto de acceso como en el dispositivo del usuario.

- **WPA-Enterprise:** requiere de una arquitectura de autenticación 802.1X.

2.3.1.7 Red privada virtual (Virtual Private Network, VPN).

Es una red de privada construida dentro de una infraestructura de red pública, usando distintos protocolos se crea un canal seguro (Universidad Iberoamericana, 2014).

2.4 Traiga su propio dispositivo (Bring Your Own Device, BYOD).

BYOD es una tendencia tecnológica que permite a los usuarios aprovechar los recursos de la red mediante el uso de sus dispositivos móviles, la red puede ajustarse de forma dinámica y segura en tiempo real al crecimiento exponencial de dispositivos y aplicaciones, que demandan conectividad inmediata y segura, en una red de acceso unificado. Los usuarios se ubican en la red por: su identidad, la postura del dispositivo u otros factores. El acceso se da sobre la base del control de acceso IP o por MAC, contando con una reserva de recursos y confiabilidad en la red. La seguridad combina la autenticación, autorización y contabilidad (AAA). El objetivo de BYOD es unificar, simplificar la creación y gestión de políticas con flexibilidad y escalabilidad. El departamento de TI debe habilitar BYOD haciendo que la red sea más inteligente y segura. Algunos de los aspectos necesarios para BYOD, según (Cisco Systems, 2014), son:

Gestión unificada de políticas: permite identificar y administrar todos los dispositivos móviles y usuarios que acceden a la red, con esta gestión se protegen los datos, aplicaciones y los sistemas.

Protección del acceso y los servicios de la red: el departamento de TI debe ofrecer un nivel idóneo de acceso a la red teniendo en cuenta el dispositivo y el perfil del usuario.

Protección de dispositivos: proteger la información de dispositivos extraviados o robados, mediante la gestión de los dispositivos.

Transmisión segura de datos: los datos pueden estar a disposición de los usuarios independientemente del dispositivo o la ubicación, esto con la seguridad y el cifrado entre el dispositivo y la infraestructura de red.

Colaboración móvil con independencia del dispositivo: las herramientas de colaboración permiten tener una sola interfaz para varias cuentas de un mismo usuario con cualquier dispositivo.

Intercambio de escritorios y vídeo móvil: con las herramientas basadas en nube se tendrá mayor colaboración y movilidad dentro de toda la red.

Sólida infraestructura de red: la red debe ser unificada y convergente, capaz de asumir, el aumento del ancho de banda, el incremento de dispositivos móviles y garantizando que los usuarios accedan a la red.

Virtualización de escritorios, compatibilidad entre dispositivos: con la virtualización se soluciona la compatibilidad, ya que aplicaciones y datos se transmiten desde el Data Center, gestionando las aplicaciones, como los datos de manera eficiente y segura.

2.4.1 BYOD y administración.

La administración de la red es una consideración primordial para BYOD, mediante una gestión unificada se proporcionará una visibilidad centralizada y control sobre toda la red, optimizando el rendimiento, la disponibilidad, productividad y satisfacción del usuario (HP, 2013, pág. 4). BYOD toma varios aspectos basado en la identidad y el control de acceso, algunos de estos se resumen en la tabla 2.

Tabla 2.
Aspectos que involucran BYOD.

¿Quién?	¿Qué?	¿Dónde?	¿Cuándo?	¿Cómo?	¿Otros?
Usuario conocido o desconocido	Dispositivo su perfil y postura.	Ubicación geográfica.	Inicio/Fin de acceso, fecha y hora.	Acceso cableado, inalámbrico o VPN.	Atributos del usuario, equipo y Apps, etc.

Nota. Aspectos involucrados en BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

La mejor gestión de BYOD según HP debe incluir la gestión de la infraestructura e implementación simplificada, identificación de dispositivos para desarrollar y aplicar las mejores políticas, políticas definidas por dispositivo y usuario, control de la red de núcleo a extremo, capacidad de gestión y planificación de los recursos, visibilidad

en tiempo real del consumo de ancho de banda, auditoría de comportamiento en línea, cumplimiento de la política de seguridad y monitoreo de tráfico de red (HP Networking, 2013).

2.4.1.1 Perfil del dispositivo.

En BYOD se debe ser capaz de colectar datos a través del tráfico que genera el dispositivo, estos se utilizarán para identificarlos y crear perfiles. Se pueden asignar privilegios de acceso de red basado en el perfil del dispositivo (Isaacson, 2013, pág. 40). El perfil se basa en los datos mostrados en la figura 2.

Datos para generar perfiles.

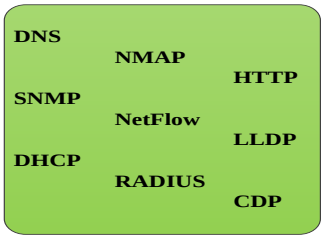


Figura 2. Datos para generar perfiles.
Elaborado por: Andrea Díaz y Danilo Lamar.

2.4.1.2 Postura del dispositivo.

En BYOD es necesario verificar la postura del dispositivo que se conecta a la red, se realiza para que esté acorde a las políticas de seguridad. Se evalúa: parches del sistema operativo, antivirus, antispyware, certificados digitales, actualizaciones, etc. Para ver el estado se usa Network Access Control (NAC) (Woland & Heary, 2013).

Características de NAC.

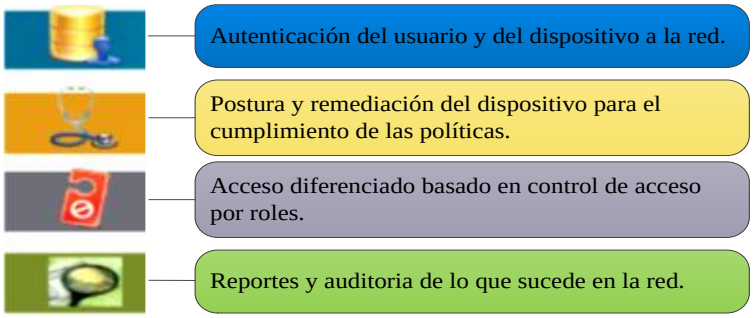


Figura 3. Características de NAC.
Elaborado por: Andrea Díaz y Danilo Lamar.

2.4.1.3 Una política, una administración y una red.

Al unir la política, la administración y la red en una sola infraestructura se puede proporcionar una gestión completa del acceso, la conectividad y el rendimiento de toda la red para de esta forma satisfacer las necesidades del usuario o de la institución. Esto ofrece una solución de BYOD completa.

Figura 4. Unificación. Fuente: Aruba Networks.

2.4.1.4 Control y gestión eficiente.

BYOD ofrece una eficiencia operativa tanto en seguridad, políticas y control en la red tanto para el usuario como para el departamento de TI.

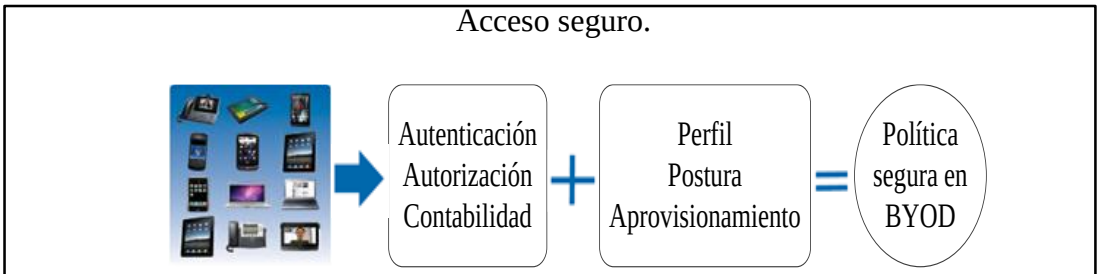


Figura 5. Acceso seguro. Fuente: Cisco.

2.4.2 BYOD y políticas.

Las políticas son fundamentales para hacer cumplir BYOD exitosamente, ya que mejora la infraestructura de seguridad de la red y el control de acceso de los usuarios, con la capacidad de aplicar una política a través de redes cableadas, inalámbricas y VPN, gestionando toda la red desde una única plataforma de seguridad. La generación de políticas proporciona acceso a la red, la postura, el acceso de invitados, empleados, servicios de aprovisionamiento y de perfiles. Dependiendo de varios parámetros como la autenticación, el medio de acceso, la localización y el tipo de dispositivo se puede generar una política de acceso como se muestra en la tabla 3.

Tabla 3.
Parámetros de BYOD en política.

Usuario	Dispositivo	Acceso	Localización	Política
▪ Empleado jornada completa / temporal ▪ Invitados	▪ Apple ▪ Iphone ▪ Android ▪ Windows ▪ Impresora	▪ Cableado ▪ Inalámbrico ▪ VPN	▪ Sitio de trabajo ▪ Departamento ▪ Ubicación geografica	▪ Acceso completo limitado ▪ Solo Internet ▪ Denegar Acceso ▪ Cuarentena

Nota. Parámetros para una política en BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

En la figura 6 se puede observar un ejemplo de política en BYOD.

Ejemplo de política.

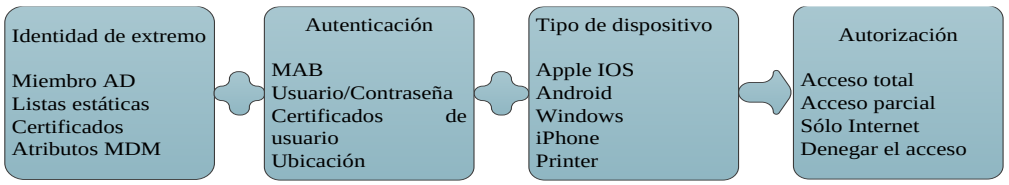


Figura 6. Ejemplo de política.
Elaborado por: Andrea Díaz y Danilo Lamar.

2.4.2.1 Componentes de una política unificada.

La unificación de las políticas en toda la infraestructura de red, permite al departamento de TI consolidar una única plataforma, lo cual garantiza una mayor consistencia en la gestión de las políticas. En la tabla 4 se puede observar los componentes para una política unificada.

Tabla 4.
Componentes.

Criterio	Software o Hardware
Gestión de política	Infraestructura de perfiles y posturas, MDM, etc.
Información de las política	AD, NAC, Infraestructura de perfiles y posturas, RADIUS, etc.
Aplicación de las política	Switches, Routers, Firewalls, Wireless Controllers
Contexto de la política	Identidad de usuario, dispositivos, activos institucionales, etc.

Nota. Componentes para una política unificada.
Elaborado por: Andrea Díaz y Danilo Lamar.

2.4.2.2 Gestión centralizada.

El departamento de TI define y gestiona normativas desde una ubicación central. Esto incluye los servicios de un servidor de políticas en conjunto con un Mobile Device Management (MDM) (Kaminski, 2013) y se lo puede observar en la figura 7.

Servidor de políticas y MDM.

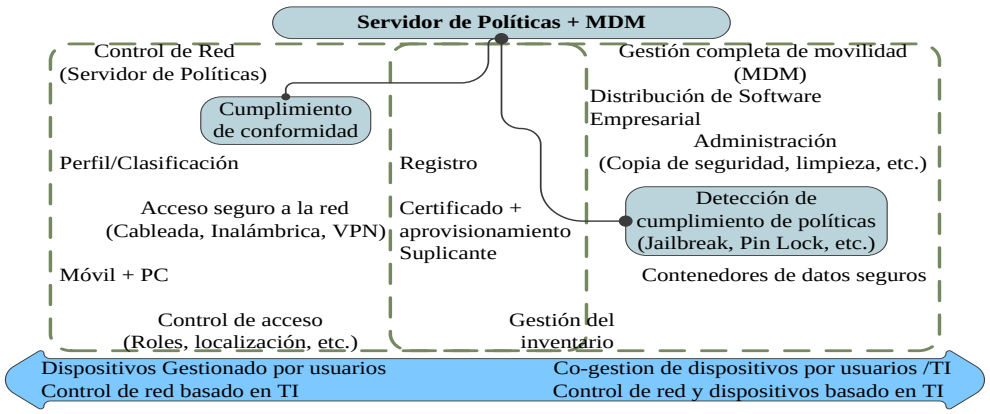


Figura 7. Servidor de políticas y MDM. Fuente: DHSES.

2.4.3 BYOD y seguridad.

En BYOD las políticas de seguridad para los diversos tipos de usuarios o dispositivos en cualquier lugar y momento, se complementan con la gestión de redes. Mejora la experiencia del usuario y de TI, sin poner en riesgo la seguridad, la visibilidad y el control. Según (Cisco Systems, Inc, 2012) BYOD ofrece una experiencia para cualquier usuario y dispositivo, con la posibilidad de colaborar desde cualquier lugar, seguridad unificada, una sola política, que abarca la gestión y el acceso a la red tanto de los usuarios como de los dispositivos, operación y administración simplificada para agilizar la resolución de problemas y reducir los costos operativos.

2.4.3.1 Riesgos en los dispositivos.

Los principales riegos de seguridad según Kaspersky se plantean a continuación.

Riesgo en el hogar del usuario: otro riesgo es la sincronización y copia de seguridad, es probable que el usuario sincronice su dispositivo con su PC en casa y este haya sido infectado comprometiendo la seguridad del dispositivo (Kaspersky, 2013).

Complementando la encriptación a nivel del dispositivo: es conveniente elegir una solución de seguridad móvil, que puede aplicar una capa adicional de cifrado, incluida la encriptación propia del dispositivo (Kaspersky, 2013).

Robo de datos a través de las vulnerabilidades: vulnerabilidades debido a parches presentes en los sistemas operativos y aplicaciones de uso común (Kaspersky, 2013).

La pérdida de un dispositivo móvil: debido al reducido tamaño y peso son muy fáciles que se pierdan o se los roben. (Kaspersky, 2013)

2.4.3.2 Seguridad en los dispositivos.

El departamento de TI debe administrar la seguridad en todos los dispositivos ya que pueden acceder a la red de distinta manera.

Las soluciones de seguridad deben ser simples, rentables, fáciles de implementar y administrar. A continuación se describen aspectos a tomar en cuenta.

- **Anti-malware:** ofrece una defensa en tiempo real frente a virus informáticos, spyware, troyanos, gusanos, etc.
- **Anti-spam:** se utiliza para prevenir el correo basura.
- **Anti-phishing:** evita que los cibercriminales tengan acceso a los datos.
- **Protección basada en firmas:** se basa en las firmas de malware que se añaden a un fichero de identificadores de malware, de manera automática y transparente para el usuario.
- **Protección basada en investigaciones de nuevas amenazas:** analizar las acciones maliciosas llevadas a cabo por un nuevo malware que aún no tiene una firma publicada.
- **Protección asistida usando Cloud:** la nube puede agregar otra capa de la seguridad anti-malware protegiendo contra amenazas en cuestión de minutos.

Separación de los datos personales y corporativos tanto a nivel personal como corporativo es esencial que los datos y las aplicaciones estén separados. Existen varias maneras como:

- **Virtualización Smartphone/Tablet:** logra que un dispositivo sea tratado como dos, el uno original y el otro virtual.

- **Contenedores:** se puede crear y configurar contenedores corporativos. Los datos pueden ser compartidos a través de las aplicaciones de contenedores, pero los datos no se comunican a los programas sin contenedores.
- **Interfaces separadas:** implica el uso de dos interfaces diferentes para el dispositivo, una para los datos corporativos y otra para los datos personales.

Control de aplicaciones para BYOD, es esencial reconocer que algunos usuarios tendrán una o más aplicaciones personales en sus dispositivos móviles. Es importante elegir una solución de seguridad que controle las aplicaciones. A menudo se da una selección de las políticas como:

- **Denegar por defecto:** esto bloquea todas las aplicaciones de funcionamiento con la excepción de las aplicaciones que están en listas blancas.
- **Permitir por defecto:** esto permite que cualquier aplicación se ejecute en el dispositivo a excepción de las que han sido incluidas en listas negras.

Control de acceso a internet, con el control de acceso a la web se evita la fuga de datos corporativos o la transferencia del malware a la red corporativa.

Manejo de dispositivos móviles perdidos o robados con un acceso remoto al equipo móvil, se puede ayudar a la seguridad, algunas de estas características son:

- **Bloquear el dispositivo:** impide el acceso a la red y al uso del dispositivo.
- **Encontrar el dispositivo:** muestra la ubicación aproximada del dispositivo.

Borrado de datos con el acceso remoto se pueden eliminar los datos del equipo, es aconsejable seleccionar una solución de seguridad que ofrezca opciones como:

- **Selectivo:** Esto ayuda a los administradores eliminar los datos corporativos, sin afectar a los datos personales del usuario.
- **Limpieza total y restablecimiento del dispositivo:** se utiliza para eliminar toda la información corporativa y personal en el dispositivo y para devolver el dispositivo a su configuración de fábrica.
- **Características adicionales antirrobo:** estas funciones adicionales, incluyen la capacidad de mostrar un mensaje en la pantalla del dispositivo para indicar a la persona que lo está usando a que lo devuelva.

Administrador de dispositivos móviles (Mobile Device Management, MDM): soluciones totalmente integradas que combinan las funciones de administración y tecnología de seguridad móvil con las cuales se pueden instalar y desinstalar software, crear y gestionar las políticas, normas de acceso a la red corporativa, administrar la configuración de la protección anti-malware, habilitar el cifrado de datos y proteger los datos corporativos en el caso de pérdida o robo.

2.4.3.3 Acceso seguro a la red.

BYOD genera normas basadas en la función de un usuario, el lugar desde el que se conecta y el modo en que lo hace, así como el dispositivo que utiliza. Para poner en práctica este nivel de diferenciación del acceso en un entorno BYOD, la solución ideal debe incluir las siguientes funciones:

- **Provisión y gestión dinámica de dispositivos:** BYOD ofrece la incorporación dinámica de dispositivos para automatizar el registro de usuarios y la asignación de credenciales, al mismo tiempo que permite a TI revocar de forma automática y sencilla los privilegios y certificados de dispositivos. Los certificados digitales y la autenticación son dos factores que proporcionan un método más seguro para tener acceso a la red.
- **Creación de perfiles de dispositivos:** Una solución BYOD debe ser capaz de identificar cada dispositivo, reconocer dónde se conecta a la red y determinar quién lo está usando. Al mismo tiempo, el departamento de TI debe ser capaz de crear normativas de acceso exclusivas tanto para dispositivos de la empresa como para los dispositivos del usuario.

Dada la variedad de dispositivos disponibles y la velocidad a la que cambian, la creación de perfiles de dispositivos dinámica proporciona la visibilidad necesaria para determinar si un dispositivo es nuevo o la versión de un sistema operativo está causando problemas. Al organizar el tráfico e implantar parámetros de seguridad adaptados a los dispositivos, una empresa disfruta de mayor control sobre la red. Del mismo modo, la capacidad de crear perfiles de dispositivos de forma instantánea resulta de gran ayuda al departamento de TI para saber qué equipo accede a la red.

La autenticación: usa un navegador que redirige a un portal web el cual contiene una página de inicio de sesión donde solicita las credenciales para acceder a la red.

La autorización: después de una autenticación exitosa, el usuario tendrá la autorización de acceso a la red o será redirigido a otro sitio web.

Inscripción de certificados y aprovisionamiento del dispositivo móvil: para implementar certificados digitales en los dispositivos móviles se necesita una infraestructura de red que proporcione seguridad y flexibilidad en la aplicación de diferentes políticas sin importar el lugar donde se origine la conexión, garantizando una inscripción de certificados y aprovisionamiento según la política que le corresponda. Cuando el usuario realiza el proceso de autenticación desde su dispositivo móvil, y esta autenticación es correcta se inicia la inscripción de certificados y el perfil de aprovisionamiento el cual adquiere información sobre el dispositivo móvil (Cisco Bring Your Own Device (BYOD) CVD, 2013).

Clave y almacenamiento de certificados: los dispositivos deben ser capaces de almacenar certificados digitales y las claves asociadas de forma segura. El almacenamiento depende del sistema operativo o de los medios de comunicación.

2.4.4 BYOD y servidores.

BYOD, debe proveer una solución unificada y completa para cumplir con los retos que trae (Arbor networks, 2012, pág. 3). En la tabla 5 se muestran algunos de los componentes que son necesarios para proporcionar una solución completa.

Tabla 5.
Servicios en BYOD.

Control de acceso a red (Network Access Control, NAC)	Permiten autenticar al dispositivo o usuario, en función de la identidad o postura. Además lo ubica en remediación hasta que cumpla con la política de acceso a la red.
Administrador de dispositivos móviles (Mobile Device Management, MDM)	Se encarga de gestionar los dispositivos móviles, aplicaciones y datos, para dar cumplimiento a la seguridad (Anderson, 2013, pág. 21).
Directorio activo de Microsoft (Microsoft Active Directory, AD)	Proporciona una base de datos de identidades y grupos centralizada (Anderson, 2013, pág. 22).
Autoridad de certificación	Emite certificados digitales a los dispositivos para establecer la

(Certificate Authority, CA)	confianza cuando accede a la red (Anderson, 2013, pág. 21).
Autorizacion de cambios en Radius (Radius Change of Authorization , COA)	Proporciona un mecanismo para cambiar los atributos de una sesión que tiene autenticación, autorización y contabilidad, después de que se ha autenticado (Cisco Systems, Inc, 2012).
RSA SecurID	Proporciona dos factores (PIN secreto y código de contraseña) de autenticación de una sola vez para una gran seguridad cuando se conecta a través de una VPN (Anderson, 2013, pág. 21).
Firewall and IPS/IDS	Se incorporan para impedir ataques a la red, dar seguimiento y bloqueo a las solicitudes de conexión atípicos desde hosts remotos (Arbor networks, 2012, pág. 4).
Servidor de nombres de dominio (Domain Name Sever, DNS)	Se utiliza para controlar y bloquear las consultas DNS a los dominios de botnets (barners, 2013).
Infraestructura de escritorios virtuales (Virtual Desktop Infrastructure, VDI)	Permite implementar arquitecturas de servicios de escritorio remotas que ofrecen flexibilidad y mantener la seguridad del entorno corporativo (Microsoft, 2014).
Protocolo de configuración dinámica de host (Dynamic Host Configuration Porotocol , DHCP)	DHCP puede hacer de la integración de los dispositivos BYOD menos caótico y más seguro, además se puede restringir la provisión de direcciones IP sólo para los usuarios autorizados de estos dispositivos (Kinnear, 2014).

Nota. Servicios para una solución de BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

2.4.5 BYOD y administración de dispositivos móviles (Mobile Device Management, MDM).

MDM es una infraestructura que asegura, monitoriza y administra cualquier tipo de dispositivo móvil, independientemente del modelo y sistema operativo. Esto se realiza mediante la instalación de un agente en el propio dispositivo móvil, que permite acciones como la instalación de aplicaciones a distancia, geolocalización, sincronización de archivos, bloqueo y borrado remoto del dispositivo, etc (TRC, 2014, pág. 3). Algunos componentes del MDM se los puede observar en la figura 8.

Componentes del MDM.

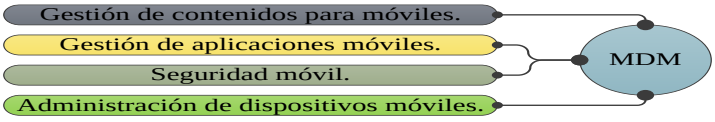


Figura 8. Componentes del MDM. Fuente: Mobisec.

MDM tiene la capacidad de trabajar con un repositorio cifrado donde se ejecuta el correo, la navegación segura y las aplicaciones corporativas. Todo esto se puede combinar con funcionalidades de gestión, que se las puede observar en la tabla 6.

Tabla 6.
Funciones del MDM.

Provisión • Grupos y Roles de usuario. • Eliminar/Ocultar aplicaciones no deseadas. • Configuración WiFi y VPN. • Aplicaciones y contenido de inserción. • Correo electrónico, Contactos y Calendarios.	**Soporte** • Bloqueo remoto. • Reseteo de clave remoto. • Detección de pérdida de información. • Múltiples plataformas. • Pérdida o robo del dispositivo.
Asegurar • Hacer cumplir Contraseña. • Hacer cumplir Cifrado de datos. • Actualizaciones de sistema operativo. • Detección de un fallo de seguridad.	**Monitoreo** • Registros de dispositivos. • Seguimiento y Elaboración de Informes de Activos. • Geo-localización.
Aplicaciones y contenido • Tienda de App privadas. • Aplicaciones web.	**Retiro** • Borrado Selectivo. • Limpieza completa.

Nota. Funciones que puede tener un MDM.
Elaborado por: Andrea Díaz y Danilo Lamar.

MDM puede interactuar con repositorios centralizados tipo SharePoint, SAP Portal y similares para integrar las capacidades de seguridad, en especial en referencia a la mitigación de las fugas de información (Luna & Martín, 2013, págs. 69 - 71). Para la implementación de MDM se incluyen propuestas flexibles adaptadas a la necesidad del departamento de TI, como son:

- **On – Premise:** en los servidores del cliente.
- **SaaS:** basado en cloud.
- **ASP:** servicio administrado por proveedor en cloud.

2.4.6 BYOD y virtualización.

La virtualización trata los recursos de red como un conjunto de servicios compartidos que se combinan para aumentar la eficiencia. El objetivo de la virtualización es

construir una infraestructura global y escalable (Cisco, 2011, pág. 9). En la tabla 7 se resumen algunos elementos involucrados.

Tabla 7.
Aspectos involucrados en virtualización.

Infraestructura	Se puede tener una virtualización de la red o de alguno de sus componentes y mejorar la gestión de la infraestructura (Virtualización, 2013).
Escritorio	La virtualización de escritorios ofrece movilidad y flexibilidad al usuario, mientras que para el departamento de TI se tiene una gestión centralizada (Microsoft, 2008).
Aplicaciones	Aplicaciones de clientes y colaboración tanto en los dispositivos como en la Web (Citrix, 2013, pág. 4).
Seguridad	Se garantiza el manejo de los datos y la protección, además se gestiona los riesgos (Sullivan, 2012).
Colaboración	Las personas pueden iniciar o unirse a reuniones desde cualquier lugar, compartir archivos, mejorar la productividad, etc (Cisco, 2010, pág. 6).

Nota. Aspectos que pueden estar involucrados en virtualización.
Elaborado por: Andrea Díaz y Danilo Lamar.

2.4.7 BYOD e infraestructura.

La movilidad es fundamental en cualquier institución, esto implica que deben tener acceso a la información corporativa mediante dispositivos móviles. BYOD obliga a los administradores a plantearse la infraestructura de red, para dar soporte a dispositivos como tablets, portátiles o smartphones, se debe tener en cuenta la convivencia entre la red cableada y la red inalámbrica. Para gestionar de forma integral la convivencia ambos tipos de redes (cableadas e inalámbricas) se deben tomar algunas consideraciones (Martínez, 2012):

Seguridad consistente y garantizada: a través de la red cableada o Wi-Fi.

Soporte de los estándares de la industria: esto significa que las redes trabajarán con la infraestructura de TI que se tenga y por lo tanto el impacto en el TCO (coste total de propiedad) será menor.

Uso de interfaces comunes: se podrán sustituir todas las herramientas, por una única plataforma de gestión que soporta protocolos consistentes a través de toda la red.

Mejor soporte para crecer: permitirá usar tecnologías nuevas como Cloud Computing, virtualización y nuevos puntos de acceso.

Simplificación y mayor rapidez en los servicios de TI: a través del centro de datos o de la infraestructura de red de la empresa.

BYOD: se dispondrá de una amplia gama de características de seguridad tales como políticas de usuario, gestión de dispositivos y control de acceso.

La solución al momento de implementar una infraestructura de BYOD, no solo se basa en un equipo, enfoque, proveedor, etc. Se necesitan algunos elementos para tener una solución completa y que cumpla con las necesidades de BYOD. Esta infraestructura involucra aspectos de equipos propios como de: virtualización, cloud, proveedores de servicio, etc.

Infraestructuras convergentes.

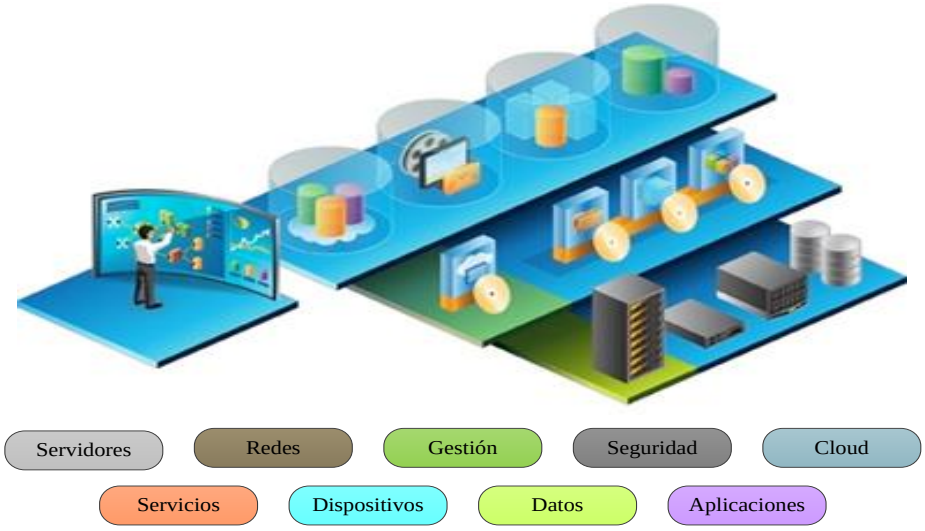


Figura 9. Infraestructuras convergentes.
Elaborado por: Andrea Díaz y Danilo Lamar.

CAPÍTULO 3
ESTUDIO DE LA SITUACIÓN ACTUAL DE LA RED INALÁMBRICA DE LA UNIVERSIDAD POLITÉCNICA SALESIANA PARA DISEÑAR BYOD

3.1 Levantamiento de información.

Se recolectará información del estado actual de la red de la UPS Campus Sur. La recopilación de datos incluirá algunos puntos como son: la ubicación, infraestructura de red inalámbrica, direccionamiento lógico y otros parámetros importantes, los cuales permitirán conocer e identificar como está constituida dicha red.

3.1.1 Ubicación.

El Campus Sur de la UPS se encuentra ubicada al sur de la ciudad de Quito, entre las calles Rumichaca y Morán Valverde s/n, la figura 10 muestra su localización.

Localización UPS Campus Sur.

Figura 10. Localización UPS. Fuente: Gloogle Earth.

El campus Sur de la universidad cuenta con 8 bloques los cuales son:

- Bloque A: Recepción y Biblioteca (Planta baja), Cecasis (Quinto piso) y Data center (Sexto piso).

- Bloque B: Secretaria.
- Bloque C: Departamento de Idiomas y Laboratorios.
- Bloque D: Auditorio y Laboratorios de Cisco.
- Bloque E: Laboratorio de Suelos.
- Bloque F: Ambiental.
- Bloque G: Nuevo Bloque.
- Bloque H: Pastoral.

La distribución de los bloques en el campus se muestra en la figura 11.

Distribución de bloques de la UPS Campus Sur.

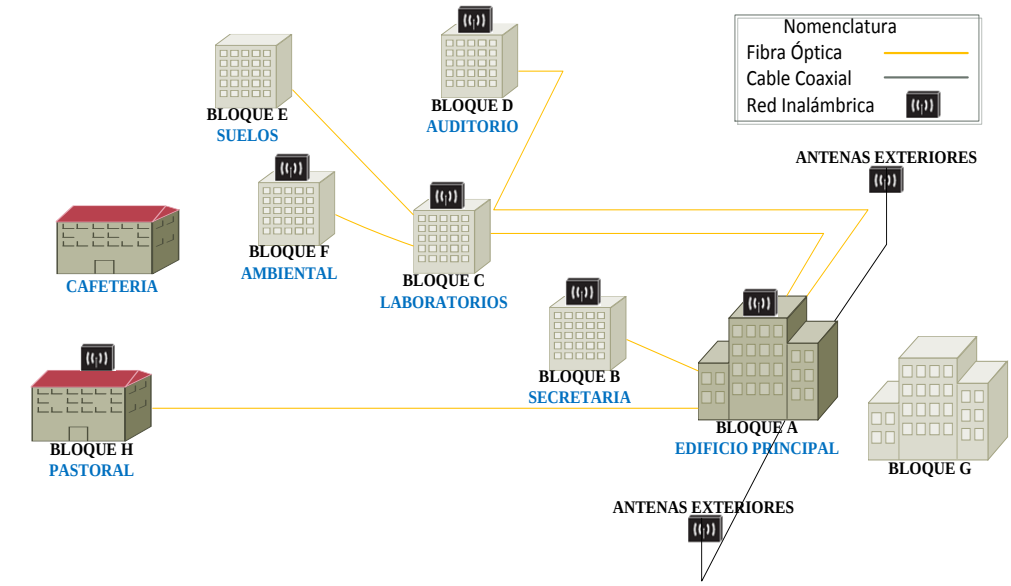


Figura 11. Distribución de bloques de la UPS Campus Sur.
Elaborado por: Andrea Díaz y Danilo Lamar.

3.1.2 Diagrama físico de red.

El modelo de diseño de red del Campus Sur de la Universidad Politécnica Salesiana se basa en el modelo jerárquico, donde los bloques anteriormente mencionados se conectan directamente con el bloque principal (Bloque A) en el cual está el Data Center (Domínguez, 2014). En la figura 12 se presenta el diagrama físico de la red.

Diagrama físico de la red de la UPS Campus Sur.

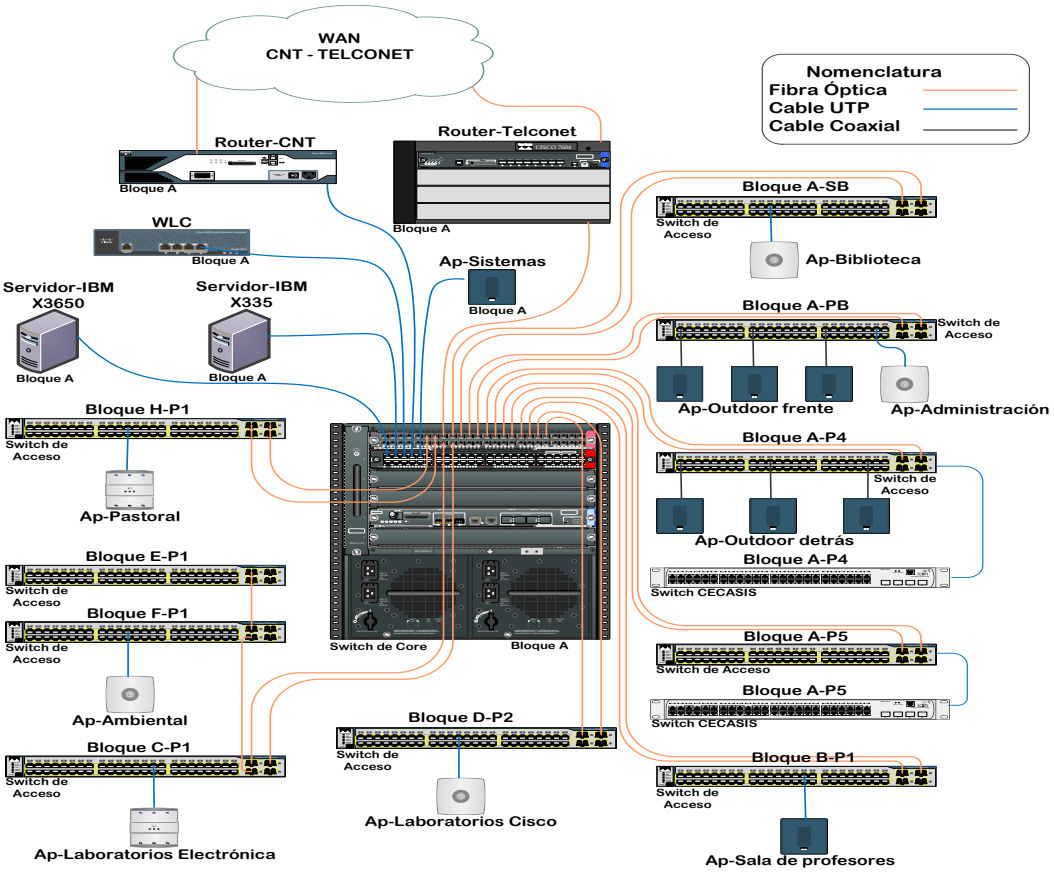


Figura 12. Diagrama físico de la red de la UPS Campus Sur.
Elaborado por: Andrea Díaz y Danilo Lamar.

3.1.2.1 Infraestructura del cableado estructurado.

La infraestructura del cableado está conformada por (Departamento TI UPS, 2013):

Cableado vertical: está conformada por fibra óptica multimodo 62.5/125 um, con longitud de onda de 1300 nm, un ancho de banda de 500 MHz/Km y una atenuación máxima de 1.5 db/Km, además está recubierta con material de protección. Se tienen dos enlaces, hacía cada cuarto de telecomunicaciones, para dar redundancia.

Cableado horizontal: está conformado por cables UTP categoría 6 y conectores RJ-45 de acuerdo a la norma EIA/TIA 568-B. De forma general se utiliza escalerilla o tubería para que pasen los cables en los diferentes bloques que conforman la universidad. Se utilizan patch panel que cumplen con la norma TIA/EIA 568-B categoría 6 de 24 puertos RJ-45 cada uno, las conexiones entre los diferentes patch panel y los switches se realizan con patch cord certificados.

3.1.2.2 Capa núcleo.

Esta capa está compuesta por equipos pertenecientes tanto a la universidad como a los proveedores, y se presentan a continuación.

Equipo de Telconet: proporciona los servicios de internet, datos y voz. El equipo utilizado es un router Cisco 7604 que se conecta por fibra óptica al proveedor y se vincula por fibra óptica al switch de core de la universidad.

Router Cisco 7604.

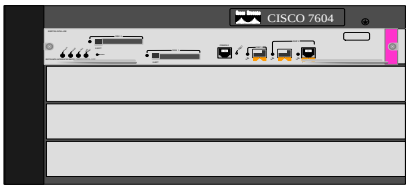


Figura 13. Router Cisco 7604. Fuente: Cisco.

Tabla 8.
Características principales del equipo Cisco 7604.

- Diseño compacto 5 unidades de rack.
- Interfaces Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet y módulos de fibra óptica.
- Módulos de seguridad IPSec, firewall, Secure Sockets Layer.
- Sistema de detección de intrusos (IDS).
- Protección de denegación de servicio (DoS).

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Equipo de CNT: se utiliza un equipo router Cisco 2851, tiene un rendimiento de alta velocidad por cable UTP, el cual provee servicio de datos para la Universidad, se conecta por fibra óptica al proveedor y mediante un conversor de medios de fibra a utp al switch de core de la universidad.

Router Cisco 2851.

Figura 14. Router Cisco 2851. Fuente: Cisco.

Tabla 9.
Características principales del equipo Cisco 2851.

• Este equipo tiene una memoria por defecto de 256 MB y soporta hasta 1 GB. • Tiene dos puertos con capacidad Ethernet, Fast Ethernet y Gigabit Ethernet. • En seguridad este equipo soporta Secure Sockets Layer (SSL), VPN, sistema de prevención de intrusos (IPS). • Diseñado para 2 unidades de rack. • Soporta MPLS.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Switch Core: el Switch de Core marca Cisco Catalyst 6506-E Series Switches, es el dispositivo fundamental en la comunicación de toda la red y a este equipo se conectan los dos routers de los proveedores, el grupo de servidores, los switches de acceso y el WLAN Controller.

Switch Cisco 6506-E.

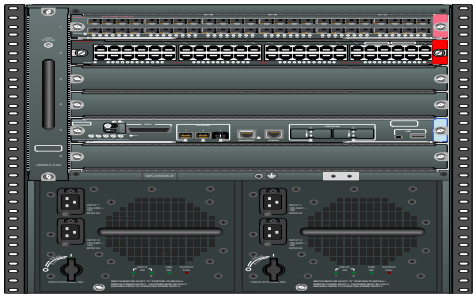


Figura 15. Switch Cisco 6506-E. Fuente: Cisco.

Wireless LAN Controller: marca Cisco 2504, es el encargado de administrar la red inalámbrica, dar calidad de servicio (QoS), confiabilidad y seguridad en la administración los access point ubicados en el campus. Este equipo es el encargado de administrar los access point de la universidad.

Wireless LAN Controller Cisco 2504.

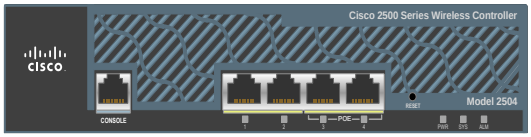


Figura 16. Wireless LAN Controller Cisco 2504. Fuente: Cisco.

Tabla 10.
Características principales del equipo Cisco 2504.

- Versión de software 7.0
- Cuatro puertos Ethernet de 1 Gbps, un puerto de consola, dos puertos soportan PoE.
- Estándares inalámbricos soportados: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11r, IEEE 802.11u, etc.
- Estándares de seguridad: WPA, IEEE 802.11i, etc.
- Encriptación: WEP, AES, DES, Secure Sockets Layer, etc.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

3.1.2.3 Capa distribución.

El Cisco Catalyst 6506-E Series Switches, antes mencionado cumple también la función de switch de distribución, ya que se tiene un modelo de red colapsado entre núcleo y distribución. A él se conectan los swicth de acceso del Campus.

Tabla 11.
Características principales del equipo Cisco 6506-E.

- Versión de software 15.1 (1) SY.
- 2543 K bytes en memoria no volátil.
- 2 Tbps en ancho de banda, 80 Gbps pro cada módulo, en VSS tiene 4 Tbps de capacidad.
- Puertos del tipo 10/100/1000 Gigabit Ethernet,
- Tipo de chasis modulado cual simplifica, unifica y economiza la red.
- Encriptación: WEP, AES, DES, Secure Sockets Layer, etc.
- Protocolos de red estándar entre los cuales están: IEEE 802.3, IEEE 802.1d, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.3x, IEEE 802.3ab, IEEE 802.3ad y IEEE 802.3ah.
- Módulos de interfaz de fibra basados en Ethernet del tipo 10 y 100 Mbps.
- Módulos SPF de 48 puertos 100 BASE-X E y módulos de fibra clásica 100BASE-X, 100BASE-FX y 10 BASE-FL

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

3.1.2.4 Capa acceso.

A continuación se describen los diferentes equipos de red en esta capa:

Switch de acceso: Son varios switch de modelo Cisco Catalyst 3750G 48P.

Catalyst 3750G– 48P.

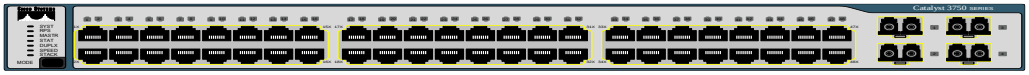


Figura 17. Catalyst 3750G– 48P. Fuente: Cisco.

Tabla 12.
Características principales del equipo Cisco 3750G– 48P.

- Versión del software 12.2 (25)
- 4 Puertos 1000 BASE-SX del tipo SPF.
- 1 Interfaz de administración.
- 48 interfaces 10/100/1000 Ethernet con PoE.
- Memoria no volátil de 64 MB.
- Memoria flash de 128 MB.
- Tecnología de apilamiento (Stackwise).
- Soporta enrutamiento dinámico IPv6.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Switch de acceso: Son varios switch de modelo Cisco Catalyst 2960S 48P.

Catalyst 2960S – 48P.

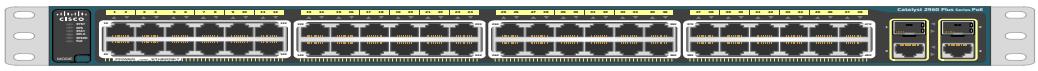


Figura 18. Catalyst 2960S – 48P. Fuente: Cisco.

Tabla 13.
Características principales del equipo Cisco 2960S– 48P.

- Versión del software 12.2 (25)
- 1 Interfaz de administración.
- 48 interfaces 10/100/1000 Ethernet con PoE.
- 4 puertos 1000 BASE-SX del tipo SPF.
- Memoria no volátil de 64 MB.
- Memoria flash de 128 MB.
- Tecnología de apilamiento (Stackwise).

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Access Point (AP): se encuentran distribuidos de la siguiente manera, en el bloque A (9 AP) y en los bloques B, C, D, F, H (1 AP por bloque).

Cisco Aironet 1131AG: es un punto de acceso que ofrece una conectividad inalámbrica de alto rendimiento, está encargado de interactuar con los dispositivos finales. Este tipo de Access Point se encuentra en el: Bloque A primer piso (Biblioteca y Área Administrativa), Bloque D segundo piso (Auditorio).

Cisco Aironet 1131AG.

Figura 19. Cisco Aironet 1131AG. Fuente: Cisco.

Tabla 14.
Características principales del equipo Cisco 1131AG.

- Posee una memoria RAM de 32 MB.
- 16 MB en memoria Flash.
- Tiene dos antenas una para 2.4 GHz y la otra para 5 GHz.
- Soporta IEEE 802.11i, IEEE 802.1X, WPA2 y WPA.
- Cisco IOS Software Release 12.3 (2) J o superior.
- Soporta los estándares IEEE 802.11 a/b/g.
- Soporta una tasa de datos de 54 Mbps.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Cisco Aironet 1310: es un modelo para exteriores, tiene antenas externas integradas u opcionales, estas proporcionan mayor cobertura de red inalámbrica al campus. Este modelo de Access Point se ubica en: Bloque A (tres Access Point en la parte exterior frontal y tres en la parte exterior posterior), Bloque B (Sala de Profesores).

Cisco Aironet 1310.

Figura 20. Cisco Aironet 1310. Fuente: Cisco.

Tabla 15.
Características principales del equipo Cisco 1310.

- Soporta estándares IEEE 802.11 b/g.
- Banda de frecuencia de 2.4 GHz.
- Tiene tres canales sin superposición.
- Soporta Autenticación.
- Memoria flash de 8 MB.
- Puede funcionar como: modo puente, punto de acceso o grupo de trabajo modo puente.
- Contiene una interfaz para administración.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Cisco Aironet 1252: es un punto de acceso para interiores diseñado para entornos de RF difíciles. Este AP se encuentra en el: Bloque C (Laboratorios de Electrónica) y Bloque H (Pastoral).

Cisco Aironet 1252.

Figura 21. Cisco Aironet 1252. Fuente: Cisco.

Tabla 16.
Características principales del equipo Cisco 1252.

- Su frecuencia de trabajo es de 2.4 GHz y 5 GHz.
- Soporta una tasa de datos de 54 Mbps.
- Tolera estándares IEEE 802.11 a/b/g e inclusive IEEE 802.11n.
- Posee una memoria de 64 MB en DRAM.
- 32 MB en memoria flash.
- En seguridad trabaja con WPA y WPA2.
- Soporta IEEE 802.1X

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

3.1.2.5 Servidores.

Físicamente la universidad posee dos servidores principales el IBM SYSTEM X335 M2 y el IBM SYSTEM X3650 M3 que son utilizados para dar servicios a la red. En la tabla 17 se muestras algunas características que se presentan en los servidores.

Tabla 17.
Características principales de los equipos IBM.

IBM SYSTEM X335 M2	IBM SYSTEM X3650 M3
• Memoria mínima 512 MB máxima 4 GB, expandibles a 8 GB. • 3 Puertos USB, un serial, 2 puertos 10/100/1000 Ethernet. • Intel Pentium 4. • Máximo dos discos duros. • Posee diskette y CD-ROM. • 8 MB de memoria de video.	• Procesador 6 Core Xeon. • 8 MB en cache. • Memoria 8 GB, máxima 24 GB. • Disco duro de 8 TB. • Posee lector óptico. • Memoria de video de 16 MB. • Un puerto serial, USB y gigabit Ethernet. • Soporta Microsoft y RHEL.

Nota. (IBM).
Elaborado por: Andrea Díaz y Danilo Lamar.

El Data Center de TI provee los servicios de (Domínguez, 2014):

Servidor Proxy: este servicio es utilizado como intermediario entre el explorador web y el internet, da seguridad a la red ya que filtra contenido web y software maligno. Está instalado en un equipo IBM SYSTEM X335 M2.

Microsoft Active Directory: administra los equipos conectados a la red, así como maneja ciertas políticas para los usuarios y los recursos de red. Está instalado en el equipo IBM SYSTEM X3650 M3.

Servidor de Archivos: está en el equipo IBM SYSTEM X3650 M3 y es utilizado para tener una ubicación central de documentos, en la cual se pueden almacenar y compartir archivos con los usuarios de la red.

Servidor F-Secure: está instalado en una máquina virtual en el equipo IBM SYSTEM X3650 M3, se usa para bajar las actualizaciones de antivirus desde la página principal y para después distribuirlas a los demás equipos de la red.

Los servidores citados anteriormente son los más relevantes, existen otros servidores, los cuales cubren el área de investigación de la universidad. También se ofrecen diversos tipos de servicios, los cuales son provistos por la Matriz (Cuenca) y otros a través de nube (Domínguez, 2014). Los cuales se mencionan en la tabla 18.

Tabla 18.
Servicios en la U.P.S Campus Sur.

Servicio	Usuario	Proveedor	Detalle del servicio
SNA	Administrativos Docentes	Matriz UPS	Sistema nacional académico registra información y record académico del alumno.
SIGAC	Administrativos	Matriz UPS	Sistema contable.
SQUAD	Administrativos	Matriz UPS	Sistema para la gestión del talento humano.
AVAC	Alumnos Docentes	Matriz UPS	Ambientes virtuales de aprendizaje cooperativo se basan en herramientas e-learning y multimedia.
Correo	Administrativos Alumnos Docentes Investigación	Microsoft	Correo electrónico institucional.
Página Web	Administrativos Alumnos Docentes Investigación	Matriz UPS	Proporciona información acerca de la universidad, permite acceso a otros servicios como AVAC, correo institucional, Quipux gestión documetal,etc
F-Secure	Administrativos Docentes Investigación	Campus Sur	Servicio de antivirus para los equipos de la universidad.
Internet	Administrativos Alumnos Docentes Investigación	CNT TELCONET	Navegación Web, entre otros servicios.
Datos	Administrativos Docentes	CNT	Interconexión entre campus.

Nota. (Diego & Jonathan, 2013).
Elaborado por: Andrea Díaz y Danilo Lamar.

3.1.2.6 Clasificación de usuarios según TI.

Los tipos de usuarios a los que se debe brindar acceso tanto a los servicios institucionales como a internet se subdividen en tres grupos los cuales son:

Personal Administrativo: cuenta hoy con alrededor de 70 usuarios como personal administrativo distribuidos entre las áreas de Financiero, Secretaria, Administración, Biblioteca, Soporte y las diversas áreas de mantenimiento.

Personal Docente: cuenta con alrededor de 185 docentes los cuales están encargados de la docencia, tutorías, investigación, etc. Y están en varias áreas del campus como son las aulas, laboratorios, biblioteca y sala de profesores.

Alumnado: actualmente la UPS cuenta con alrededor de 3500 alumnos en la sede Quito Campus Sur. Ellos utilizan el internet, correo institucional y la plataforma AVAC como servicios que la universidad les brinda.

3.1.2.7 Modo de acceso de usuarios.

El acceso brindado por la Universidad Politécnica Salesiana esta segmentado en alámbrico e inalámbrico. Cabe mencionar que ambos tipos de acceso tienen diferencias según sea el tipo de usuario antes mencionado y otros detalles que se mencionaran a continuación (Domínguez, 2014):

Modo Alámbrico: diseñado para ofrecer una conectividad a zonas fijas, hace uso de cables UTP categoría 6 y está implementado actualmente en todos los bloques de la universidad. Es el principal medio de acceso a la red por parte del personal administrativo y para cierta parte de docentes y alumnos.

Modo Inalámbrico: destinado para la toda la comunidad salesiana que requiera movilidad dentro del Campus. Las conexiones inalámbricas al usuario llegan a través de Access Point con los switches de borde para llegar al data center de manera similar a las conexiones alámbricas.

3.1.2.8 Seguridad en la red.

La seguridad en la red se da por diferentes formas como son: a nivel de configuración (ACL), creación de Vlan específicas, usando un servidor Proxy, un servidor antivirus (F-SECURE), autenticación web para la red inalámbrica de docentes, ocultar los SSID para usuarios no autorizados, filtrado MAC en la red inalámbrica, etc (Domínguez, 2014).

3.1.2.9 Administración de la red.

El departamento de TI para la gestión de la red de la Universidad Politécnica Salesiana Campus Sur cuenta con una persona encargada de monitorear la infraestructura de red así como proveer soluciones de mantenimiento y prevención a los problemas relacionados con los equipos de la institución. Este departamento se encuentra ubicado en el sexto piso del bloque A, aquí también se encuentra el data center, en el cual están los principales equipos de red como son: swicthes, routers, servidores, etc.

3.1.3 Diagrama lógico de red.

El diseño de red lógico del Campus Sur de la Universidad Politécnica Salesiana, solo se basará en las redes inalámbricas que se tienen, además de los equipos intermediarios que intervienen en esta red. En la figura 22 se presenta el diagrama lógico de la red.

Esquema lógico de red.

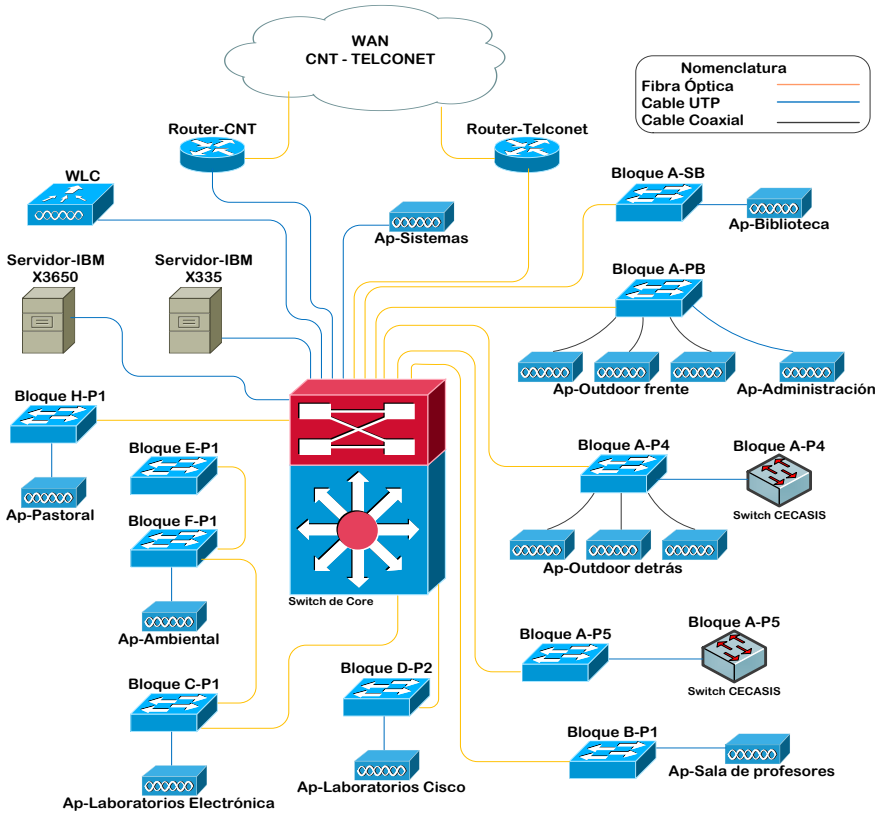


Figura 22. Esquema lógico de red.
Elaborado por: Andrea Díaz y Danilo Lamar.

3.1.3.1 Direccionamiento lógico.

La topología física de la Universidad tiene forma de estrella extendida. Lo que quiere decir que todos los switches de acceso, routers de proveedores, servidores y wlan controller están conectados a un switch principal (Switch de Core). Este permite la comunicación con todos los bloques del campus (Domínguez, 2014). En la tabla 19 se listan los equipos que intervienen en la red inalámbrica así como las redes inalámbricas que se difunden y las cuales se las administra a través del WLC.

Tabla 19.
Direccionamiento de la red inalámbrica.

Equipo o SSID	Direccionamiento IP	Submáscara	Gateway	Vlan ID
Router CNT	187.10.X.X	255.255.X.X	187.10.X.X	
Router TELCONET	186.10.X.X	255.255.X.X	186.10.X.X	
Servidor Proxy	172.17.X.X	255.255.X.X	186.10.X.X	
Active Directoy	172.17.X.X	255.255.X.X	172.17.X.X	
Servidor de Archivos	172.17.X.X	255.255.X.X	172.17.X.X	
Servidor F-Secure	172.17.X.X	255.255.X.X	172.17.X.X	
Switch de Core	172.17.X.X	255.255.X.X	186.3.X.X	
WLC	172.17.X.X	255.255.X.X	186.10.X.X	
cima	172.17.X.X	255.255.X.X	172.17.X.X	19
eventos	172.17.X.X	255.255.X.X	172.17.X.X	26
fisicauios	172.17.X.X	255.255.X.X	172.17.X.X	27
gietec	172.17.X.X	255.255.X.X	172.17.X.X	29
managment	172.17.X.X	255.255.X.X	172.17.X.X	24
wlan-docentes	172.17.X.X	255.255.X.X	172.17.X.X	7
wlan-estudiantes	172.17.X.X	255.255.X.X	172.17.X.X	10
wlan-ups-adm	172.17.X.X	255.255.X.X	172.17.X.X	3
wlc-biblioteca	172.17.X.X	255.255.X.X	172.17.X.X	8

Nota. (Diego & Jonathan, 2013).
Elaborado por: Andrea Díaz y Danilo Lamar.

3.1.4 Otros parámetros.

Existen varios aspectos que deben tomarse en cuenta con relación a la infraestructura de red: acceso, seguridad, usuarios, proveedores, etc. Porque intervienen en el funcionamiento de la red de la universidad.

3.1.4.1 TIER del Data Center UPS.

El nivel de disponibilidad que tiene el Data Center se clasifica en TIER, creada por el Uptime Institute, este instituto estableció cuatro niveles de TIER, desde el nivel menor (TIER I) hasta el de mayor nivel (TIER IV). En la tabla 20 se presenta el nivel de TIER que posee el Data Center de la universidad.

Tabla 20.
Tipo de TIER Data Center.

TIER	**Características técnicas y operativas que se debe cumplir.**	**Características técnicas y operativas que se cumplen el Data Center de la UPS.**
TIER I	• Infraestructura básica. • Tiene componentes no redundantes y un solo paso no redundante de distribución sirviendo a los equipos. • Una falla en cualquier componente impactará al sistema. • Para los trabajos de mantenimiento deben detenerse las operaciones del Data Center. • El servicio puede interrumpirse por actividades planeadas o no.	• Posee infraestructura básica. • Tiene planta eléctrica y un sistema de alimentación ininterrumpida (ups). • Tiene refrigeración. • El Data Center debe apagarse por completo cuando necesite mantenimiento correctivo o predictivo. • El Data Center es susceptible a interrupción planeada o no. • No tiene componentes redundantes.

Nota. Tipo de TIER que se tiene en el Data Center de la universidad.
Elaborado por: Andrea Díaz y Danilo Lamar.

3.1.4.2 Cuarto de telecomunicaciones

Existen equipos de red de la marca Cisco (en la mayoría de los bloques) y pocos equipos de la marca 3COM. Los equipos de Cisco están conectados directamente al Data Center. Los cuartos de telecomunicaciones están distribuidos en la universidad de la siguiente manera: bloque A (3 cuartos de telecomunicaciones y 1 armario rack) y bloques B, C, D, E, F, H (1 armario rack por bloque).

Tipos de armarios racks.

Figura 23. Tipos de armarios racks.
Elaborado por: Andrea Díaz y Danilo Lamar.

3.1.4.3 Internet y proveedores.

Se dispone de enlace de datos para el acceso de internet contratado con las empresas Telconet y Corporación Nacional de Telecomunicaciones. En la figura 24 se puede ver el incremento del internet para los tres campus de la UPS en Quito (Departamento TI UPS, 2013).

Incremento de internet.

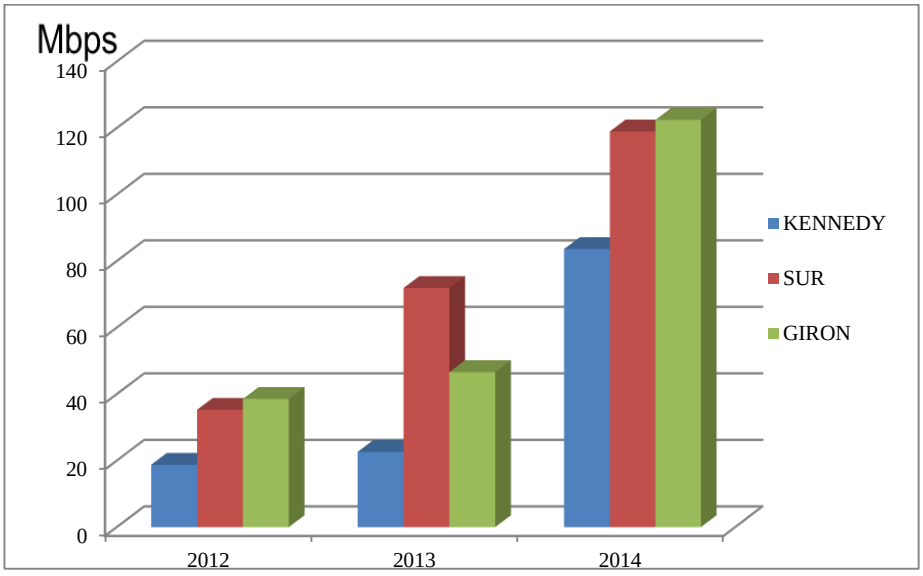


Figura 24. Incremento de internet. Fuente: Departamento TI UPS.

3.2 Soluciones de BYOD.

En la tabla 21 se presenta algunas soluciones para BYOD de diferentes proveedores de tecnología.

Tabla 21.
Soluciones de proveedores.

Cisco BYOD	HP BYOD	Citrix BYOD	Aruba BYOD	Meraki BYOD
La solución de cisco está compuesta de: Cliente Cisco AnyConnect Secure Mobility, RSA SedurID, Identity Services Engine (ISE), Cisco Scansafe Cloud Web Security, Cisco Mobility Servicies Engine, MDM, Certificate Authority, Microsoft Active Directory (AD), Cisco Prime, Prime network Control System NCS, Virtualization Experience Infraestructure. Todos estos elementos están involucrados en diferentes áreas como son: acceso, gestión de dispositivos, redes, seguridad, aplicaciones, colaboración, etc.	HP nos brinda una solución basada en: IMC User Access Manager (UAM), IMC Endpoint Admision Defense (EAD), IMC Network Traffic Analyzer (NTA), IMC User Behavior Auditor (UBA), IMC Wireless Services Manager (WSM). Estos componentes cubren áreas como: acceso y gestión de dispositivos, redes, seguridad, administración de dispositivos móviles, etc.	La propuesta de citrix se establece en: Citrix Receiver, Citrix Mobile Enroll (IOS solamente), Citrix Mobile Connect, NetScaler Access Gateway, Citrix XenMobile MDM, Citrix CloudGatteway, Citrix GoTo Meeting con HDFaces, Citrix GoToWebinar, Citrix GoTo Training, Citrix Podio, Citrix ShareFile, Storage Zones, Citrix XenApp, Citrix XenDesktop. Todos los recursos antes mencionados se ven inmersos en: aplicaciones virtuales, datos, colaboración, aplicaciones, administración de dispositivos, seguridad, gestión y acceso.	Aruba se enfoca en: acceso, gestión de dispositivos, redes y seguridad. Para esto emplea algunos módulos como son: ClearPass Policy, ClearPass QuickConnect, ClearPass Onboard, ClearPass Profile, ClearPass Guest, ClearPass OnGuard.	LA solución de Cisco Meraki está enfocada a dar servicio a través de Cloud, apoyados en un NAC y la función de administración de dispositivos móviles. Incluye una gestión de red poco compleja, además que permite clasificar automáticamente a los dispositivos móviles ya se han estos teléfonos inteligentes, tabletas, computadores portátiles. Permite aplicar políticas según el tipo de dispositivo, protege a toda la red y crea informes automáticos acerca de los equipos y su uso en la red.

Nota. (Aruba, s.f.), (Cisco, s.f.), (Citrix, s.f.), (HP, s.f.) , (Cisco System , 2014).
Elaborado por: Andrea Díaz y Danilo Lamar.

CAPÍTULO 4
DISEÑO Y SIMULACIÓN DE LA RED INALÁMBRICA CON BYOD

4.1 Introducción a la propuesta de diseño.

En el presente capítulo se citarán los requerimientos que debe cumplir la solución de BYOD para la universidad, junto a esto se detallará el diseño de la red propuesta para la institución, además se describirán las características principales y funciones de los principales equipos de red. Finalmente se desarrollará un piloto de la red con BYOD.

4.1.1 Densidad de usuarios.

La UPS Campus Sur cuenta con alrededor de 3800 usuarios, entre administrativos, docentes y estudiantes. Se puede decir que la parte administrativa tiene un lugar fijo donde realizar sus tareas diarias y cuentan con equipos apropiados para llevar a cabo su trabajo. Otra es la situación de docentes los cuales tienen algunos espacios asignados para sus labores diarias, al igual que el equipo que traen a la universidad depende de sus posibilidades. Por parte de los alumnos la situación también es diferente ya que están movilizándose por todo el campus dependiendo de las actividades que vayan a realizar. En la figura 25 se muestra la mayor cantidad de usuarios que se conectan a la red de la institución de manera inalámbrica en el día.

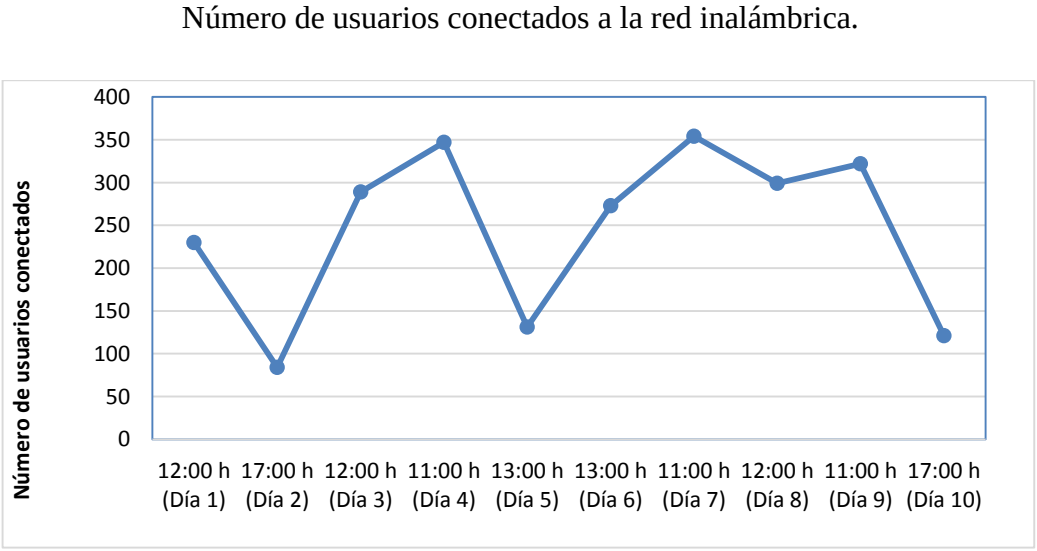


Figura 25. Número de usuarios conectados a la red inalámbrica.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.1.2 Dispositivos por usuarios.

Los dispositivos que se utilizan para acceder a la red, tienen una gran variedad como laptops, tablets, smartphones, etc. Los cuales trabajan con varios sistemas operativos como son: Windows, Android, iOS y Mac OS. Los estudiantes son el mayor grupo de la institución y en el cual se presenta un cambio tecnológico notorio, por tal motivo se les realizó una encuesta para recopilar información de la cantidad de dispositivos que utilizan dentro de la universidad. El total de alumnos encuestados son 300, encontrando que 154 utilizan al menos dos dispositivos, 77 utilizan tres dispositivos y 69 tan solo un dispositivo. En la figura 26 se puede observan el resultado de la encuesta, en la sección de anexos se puede ver el tipo de encuesta que se realizó.

Porcentaje de dispositivos por usuario.

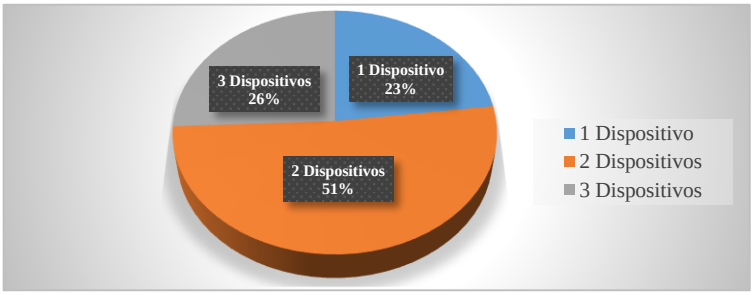


Figura 26. Porcentaje de dispositivos por usuario.
Elaborado por: Andrea Díaz y Danilo Lamar.

De aquí se pude decir que todos los encuestados usan al menos un dispositivo para acceder a la red, además que todos acceden a la red por lo menos una vez en el día.

4.1.3 Accesibilidad a los recursos de red.

Brindar accesibilidad a los recursos de red en el campus permite que los usuarios respondan más rápidamente a las necesidades propias o de la institución, sin tener en cuenta la ubicación de ellos, además de brindar una priorización a dichos recursos, dependiendo de las políticas implantadas por el departamento de TI a los distintos tipos de usuarios existentes en la universidad. El uso de internet en la universidad varía en la cantidad de usuarios dependiendo de la hora en la cual se conectan a la red. Hay un mayor uso del recurso por la mañana ya que existe mayor número de usuarios en este horario en comparación con los usuarios de la jornada vespertina.

4.1.4 Manejo centralizado.

Debido a que BYOD involucra a toda la infraestructura de red, se tendrá una administración centralizada es decir todos los equipos de networking están conectados a un dispositivo central, de esta forma el departamento de TI puede responder de forma efectiva y eficiente cuando se presenten problemas y fallas en la red. Además podrán ejecutar las políticas que sean más convenientes para la red.

4.2 Selección de la tecnología.

Para definir que tecnología de red es la más favorable para implementar BYOD en la universidad se tomaron en cuenta varios aspectos relacionados con la red actual, los lineamientos que persigue el departamento de TI y los parámetros descritos en anteriores capítulos de este trabajo de grado.

4.2.1 Equipos de red actual.

El equipamiento actual de la red de la Universidad Politécnica Salesiana cuenta en su mayoría con equipos de la marca Cisco, algunos de los cuales han sido adquiridos hace un par de años atrás (por ejemplo el Switch de Core). La red también cuenta con servidores de la marca IBM ubicados en el Data Center y switches en la marca 3COM situados en el cuarto de telecomunicaciones del cuarto y quinto piso respectivamente los cuales son utilizados para el departamento de CECASIS, los switches 3COM no actúan en la red inalámbrica y tampoco intervendrán en la propuesta de red para BYOD.

4.2.2 Departamento de TI del Campus Sur.

El departamento de TI del Campus Sur ha tenido una tendencia, en sus equipos de networking hacia la marca Cisco. Esto se observó en la realización del capítulo anterior en la cual se notó el uso de switches, routers, access point, etc, de la marca antes mencionada trabajando en la red actual de la universidad. Además acotar que el departamento de TI tiene un mayor conocimiento de estos equipos debido a que trabajan con ellos varios años.

4.2.3 BYOD y la implicación para la institución.

Hoy en día la planificación de la red se debe tomar muy en cuenta ya que se presenta un nuevo desafío donde varios dispositivos con varias aplicaciones intentan conectarse a la red en cualquier lugar. La solución de BYOD debe permitir a la institución proteger su inversión en tecnología mediante la construcción sobre lo que ya tiene, manteniendo la flexibilidad para adaptarse a los nuevos servicios, soluciones y dispositivos que van surgiendo, además con BYOD según (Cisco , 2014) se mejora la enseñanza y el aprendizaje, se incrementa la participación de los usuarios, se acrecienta la eficiencia operativa, aumentar la productividad del personal, amplia la colaboración y las capacidades de infraestructuras tecnológicas existentes. Además de tener consecuencias financieras favorables debido a BYOD. La solución de Cisco para BYOD se puede ajustar de forma dinámica, segura y gestionada en tiempo real a un crecimiento exponencial de dispositivos móviles y aplicaciones, brindando a cada usuario conectividad inmediata y segura a la red. Además facilita el despliegue de nuevas aplicaciones manteniendo un enfoque en el rendimiento académico y las necesidades presupuestarias de la institución. Todo esto se basa en equipos como: access point, routers, servidores, switches, firewalls, etc. Sumado a todo esto Cisco brinda el soporte respectivo a sus equipos al igual que se mantiene a la vanguardia para afrontar los nuevos retos que existen en el área de las redes. Debido a los factores antes mencionados el diseño de la red se inclina a la solución brindada por Cisco ya que cumple con las características, prestaciones y perspectivas que involucran a BYOD y a la institución.

4.3 Dimensionamiento.

Cisco impulsa un producto basado en un servidor AAA y un NAC combinados en un solo equipo el cual se denomina Motor de Servicios de Identidad (Identity Services Engine, ISE). ISE trabaja con una infraestructura de red que debe ser Cisco 100% para que tenga un funcionamiento correcto, además este equipo hace el uso de licenciamiento. La cantidad de licencias corresponde al número de direcciones IP por equipo a utilizarse, incluyendo tanto a dispositivos de red, dispositivos personales o de la institución y otros equipos que ocupan una dirección IP. Y por esto se debe dimensionar el uso de licencias. Además del equipo antes mencionado se necesitan

otros equipos de red para tener la solución de BYOD como son switches, routers, access point, wireless LAN controller, etc. En la tabla 22 se describen estos datos.

Tabla 22.
Dimensionamiento de la red.

Usuarios o Equipos	Actuales	Diseño
Administrativos	70	140
Docentes	185	370
Concurrencia promedio red inalámbrica	260	400
Equipos de networking	52	52

Nota. Dimensionamiento de la red a diseñar.
Elaborado por: Andrea Díaz y Danilo Lamar.

La universidad cuenta con alrededor de 3800 usuarios, pero en la etapa inicial se comenzará con un licenciamiento a 1000 dispositivos los cuales podrán tener todos los recursos de la red según sean las políticas, si se necesitan más licencias a futuro se podrán adquirir a Cisco. Los dispositivos que no tengan acceso a todos los recursos de la red debido al tema de licenciamiento, si tendrán acceso a la red solo que con limitaciones debido a las licencias.

Administrativos 140 licencias esto debido a que tienen su propio espacio de trabajo el cual consta de equipo de computación y telefonía IP, se asegura que se han participes de BYOD. Para los docentes se toma en cuenta el número de dispositivos que usan en este caso dos por cada docente 370 licencias, esto asegura que los docentes también participen en BYOD. La concurrencia a la red inalámbrica por parte de los dispositivos móviles es de 260 en promedio y la cual se elevara a 400, este número de licenciamiento se dará a todos los usuarios (administrativos, docentes, estudiantes e invitados) con dispositivos móviles que se conecten a la red inalámbrica. La parte de equipos de red se lleva 52 licencias y las restantes 38 licencias se tendrán para otros equipos o casos de uso especiales que pueden surgir en la institución.

4.3.1 Requerimientos de los componentes básicos para soporte de BYOD

Para que la red de la universidad soporte BYOD, se debe cumplir con la compatibilidad entre ISE y los componentes de la infraestructura que han sido

validados según (Cisco Systems, 2014), en la tabla 23 se observan algunos componentes que tienen compatibilidad con ISE.

Tabla 23.
Requerimientos de compatibilidad.

Componente	**Versión OS recomendada**	**Rol**
Cisco Identity Services Engine	1.2	Servidor
Switches		
Catalyst 2960-S y 2960-C	IOS v 12.2(55)-SE3	Switch de acceso/core
Catalyst 2960-SF y 2960Plus	IOS v 15.0.2-SE (ED) LAN BASE	
Catalyst 2960-XR y 2960P-X	IOS v 15.0.2-EX3 (ED)	
Catalyst 3560-C, 3560-E, ISR EtherSwitch ES3 Catalyst 3560-X	IOS v 15.0.2-SE2 (ED)	
Catalyst 3750-G	IOS v12.2(55)-SE3	
Catalyst 3750-E y 3750-X	IOS v 15.0.2-SE2 (ED) IP BASE	
Catalyst 3850-E y 3650	IOS XE 3.2.2 SE	
Catalyst 4500 Supervisor Engine 7-E, 7L-E	IOS-XE V 3.4.0 SG (ED)	
Catalyst 4500 Supervisor Engine 6-E, 6L-E	IOS v 15.1.2 SG (ED)	
Catalyst 6500 (Supervisor 32/Supervisor 720)	IOS v 12.2 (33)-SXJ5 (MD)	
Inalámbricos		
Wireless LAN Controller (WLC) 2100, 4000, WiSM1 y WiSM2 Blade for 6500	7.0.116.0(ED)	Controla los puntos de acceso de manera centralizada.
WLC 2500, 5500, 7500 y 8500	7.3.112.0(ED), 7.4.x, 7.5	
WLC 5760	IOS XE 3.2.2 SE	
Routers		
WLC ISR (ISR2 ISM, SRE700 y SRE900)	7.3.112.0(ED)	Enrutamiento.
ISR 88X, 89X Series, 19x, 29x, 39x Series	15.3.2T(ED)	
Firewalls		
Cisco ASA 5500 y 5500-X Series	ASA 9.2.1	Seguridad a la red.
Access Point		
Cisco Series AP 3700, 3600, 3500, 2600	----------	Puntos de acceso.
Servidores externos		
Microsoft Active Directory	2003, 2003R2, 2008, 2008R2, 2012 y 2012R2	Servidor.

Nota. (Cisco Bring Your Own Device (BYOD) CVD, 2013).
Elaborado por: Andrea Díaz y Danilo Lamar.

4.3.2 Equipos a utilizarse en la red.

Los equipos a utilizarse en la red propuesta son los siguientes:

Tabla 24.
Equipos para el diseño.

Equipo	Versión	Adquisición	Observaciones
IBM X3650M3	----------	No adquirir	No necesita licencia
ISE 3415	1.2	Comprar	Producto: SNS-3415-K9 Licencia de ISE: SW-3415-ISE-K9 Garantía: L-ISE-AD5Y-1K Licencia usuarios: L-ISE-BSE-1K Licencia suscripciones:L-ISE-ADV-S-1K
WLC 5508	7.5	Comprar	Producto: AIR-CT5508-50-K9
ASA 5515-X	9.1.1	Comprar	Producto: ASA5515-K9 Licencias AVC / WSE: ASA5515-AW5Y IPS: ASA5515-NI5Y
Switch 6506-E	15.1	No adquirir	No necesita licencia
Switch 3750G	12.2(25)SEE2	No adquirir	No necesita licencia
Switch 2960S	12.2(50)SE5	No adquirir	No necesita licencia
AP 3702P	7.6	Comprar	Producto: AIR-CAP3702P-x-K9

Nota. Equipos a utilizarse para el diseño.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.3.3 Justificación de equipos para el diseño.

Se seleccionaron estos dispositivos ya que sus capacidades son las adecuadas para su uso en la red según (Cisco, 2014) , a continuación se describen estas capacidades:

Versión de IOS: soporte del sistema operativo del equipo.

Bypass de autenticación MAC (MBA): utilizado cuando el punto final no puede autenticarse en la red.

802.1X: estándar IEEE para comunicar las credenciales de identidad que utiliza el protocolo de autenticación (EAP) a través de LAN.

Autenticación Web: acceso a la red a través de una página web, tiene dos modos de implementación:

- **Autenticación de Web central:** la opción más conocida, es controlada por ISE.
- **Autenticación de Web local:** realizado por el switch o el WLC, no realiza CoA, ni modifica la VLAN o el soporte al ID de sesión.

Cambio de autorización (CoA): Atributo RADIUS que la maneja ISE.

VLAN: LAN virtual, puede ser asignado a un dispositivo entrante.

DACL: lista de control de acceso que se envía desde ISE al dispositivo de acceso para restringir el acceso a la red.

Grupo de acceso de seguridad (SGA): construye redes seguras mediante el establecimiento de un dominio de dispositivos de red, además puede utilizar la identidad del dispositivo y la información del usuario adquirida durante la autenticación para clasificar los paquetes mediante etiquetado, para controlar el tráfico que entra a la red.

IOS Sensor: habilita la funcionalidad de perfilar, integrada en los sistemas operativos de switches, WLC, permitiendo hacerlo de forma local, en lugar de hacerlo en forma centralizada en un nodo de ISE. En la tabla 25 se pueden observar si los equipos elegidos cumplen estas funciones.

Tabla 25.
Capacidades de los equipos.

Equipo	Versión IOS	MAB	802.1X	CWA	LWA	CoA	VLAN	DACL	SGA	IOS Sensor
Switch 6506-E	15.1	Si	Si	Si	Si	Si	Si	Si	Si	No
Switch 3750G	12.2(25) SEE2	Si	Si	Si	Si	Si	Si	Si	Si	No
Switch 2960S	12.2(50)SE5	Si	Si	Si	Si	Si	Si	Si	No	No
WLC 5508	7.5	Si	Si	Si	Si	Si	Si	Si	Si	Si
ASA 5515-X	9.1.1	---	---	---	---	Si	Si	Si	Si	No

Nota. Capacidades presentes en los equipos.
Elaborado por: Andrea Díaz y Danilo Lamar.

En la figura 27 se observan los equipos presentes en la red actual y en la propuesta.

Equipos presentes en la red actual y en la propuesta.

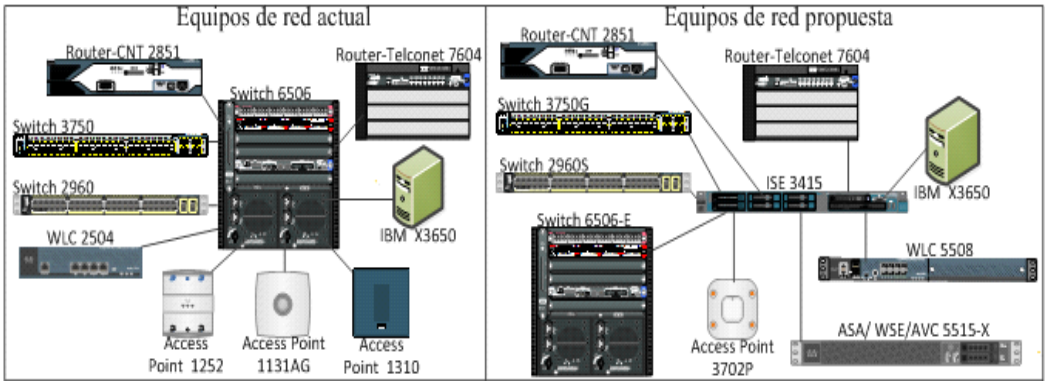


Figura 27. Equipos presentes en la red actual y en la propuesta.
Elaborado por: Andrea Díaz y Danilo Lamar.

En la tabla 26 se observar los equipos y su utilidad para el diseño de la red.

Tabla 26.
Equipos y su interés.

Equipo de red actual	Equipo para el diseño	Interés para el diseño
IBM SYSTEM X3650 M3: Equipo modular, alta disponibilidad, soporta colaboración, virtualización, base datos, etc.		Contiene los servicios de AD, servidor de archivos y el antivirus.
Swicth 6506-E Escalable, alta disponibilidad, modular, simplifica y unifica la red, integra funciones avanzadas, alta densidad de puertos, etc.		Posee características esenciales para poder ser usado en conjunto con el ISE.
Wireless LAN Controller 2504 Versión de software 1.0, estándares inalámbricos IEEE 802.11 a/b/g/n, soporta 25 AP.	Wireless LAN Controller 5508 Escalabilidad, control de RF inteligente, mejora la calidad en voz, video, etc.	WLC 5508 trabaja en conjunto con ISE, tiene soporte de cisco a diferencia del WLC 2504, al cual dejaron de darle soporte.
Swicth 3750G y 2960S Interfaces del tipo 10/100/1000 Ethernet con PoE, soporta enrutamiento y utilizado en la guía de diseño de BYOD de Cisco.		Utiliza un software actual y es compatible con la red para el diseño de BYOD.
AP´s 1131AG, 1310 y 1252 Soportan estándares IEEE 802.11 a/b/g, a/b y a/b/g e incluso n respectivamente.	Access Point 3702P Estándares IEEE 802.11 a/b/g/n/ac, MIMO , alta escalabilidad, etc.	AP de última generación soportan IEEE 802.11 a/b/g/n/ac, compatible con el WLC 5508.
No existen equipos similares en la red actual.	Cisco ISE 3415 Servidor encargado de BYOD	Encargado de generar políticas, gestionar a los diferentes

	sobre la red en conjunto otros equipos de red.	usuarios y dispositivos, equipo principal de BYOD.
	ASA 5515-X Firewall de siguiente generación brinda seguridad a e incluye IPS, AVC y WSE.	Compatible con ISE y junto a este brindar mayor seguridad a la red, y mencionado en la guía de diseño de BYOD de Cisco.

Nota. Equipos y el interés para el diseño.
Elaborado por: Andrea Díaz y Danilo Lamar.

En el servidor IBM se tendrán los servicios descritos en la tabla 27.

Tabla 27.
Requerimientos del servidor IBM.

Servicio	Versión de software	Rol
Microsoft Active Directory (AD), Microsoft Certificate Authority (CA), Servidor de archivos y F-Secure.	Windows 2008 Server R2	Servidor

Nota. Requerimientos para el servidor.
Elaborado por: Andrea Díaz y Danilo Lamar.

Durante el uso de un servidor de CA con ISE, se debe tener en cuenta que se cumpla con los requisitos mostrados en la tabla 28.

Tabla 28.
Requisitos de CA para la interoperabilidad con ISE.

- El tamaño de la calve debe ser de 1024, 2048 o superior. En el servidor de CA, el tamaño de la clave se define utilizando la plantilla de certificado. Se puede definir el tamaño de la clave de Cisco ISE utilizando el perfil suplicante.
- El uso de claves debe permitir firmas y el cifrado en extensión.
- Se recomienda utilizar RSA + SHA1.
- Se admite el protocolo de estado de certificados en línea (Online Certificate Status Protocol, OCSP). Esto no es utilizado directamente en BYOD, pero un CA puede actuar como OCSP se puede utilizar para la revocación de certificados.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Todas estas capacidades están basadas sobre un equipo ISE con versión 1.2 para mantener la compatibilidad entre los equipos. Se debe tomar en cuenta que si algún

equipo no cumple con los requerimientos básicos debe ser actualizado o cambiado dependiendo de la función que cumpla en la red.

4.4 Infraestructura de cableado.

La infraestructura del cableado, que se la revisó en el capítulo anterior puede ser utilizada para esta propuesta de red por las siguientes razones: en la parte del cableado vertical se tiene fibra multimodo 62.5/125, además existe redundancia hacia los cuartos de telecomunicaciones, para la parte del cableado horizontal se tiene un cableado estructurado de categoría 6 con lo cual se tiene una velocidad de 1 Gbps. Se mantendrá la misma infraestructura de cableado debido a que aún satisface las necesidades de BYOD. Para nuevos enlaces se utilizara el mismo tipo de cable si es que fuere necesario.

4.5 Diseño lógico.

La topología de la red propuesta para el Campus Sur, se la puede observar en la figura 28 la cual muestra una topología del tipo estrella extendida.

Topología de la solución.

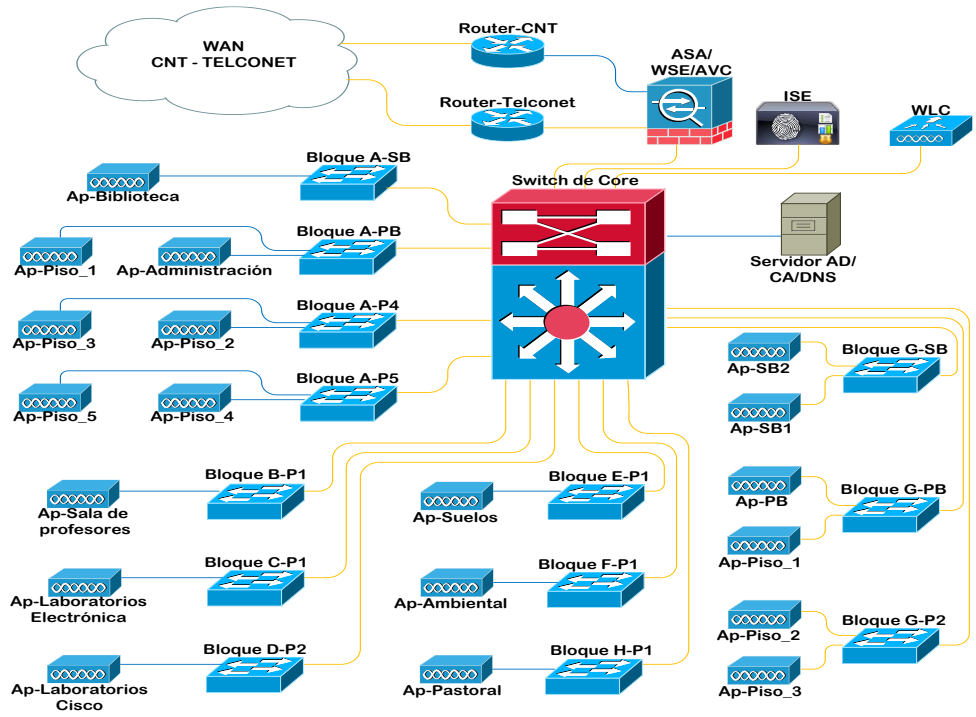


Figura 28. Topología de la solución.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.5.1 Direccionamiento.

Debido a la migración de IPV4 a IPV6 se ha decidido emplear IPV6 para la creación de las redes en este diseño.

Tabla 29.
Direccionamiento de los equipos y las redes inalámbricas.

Equipos o SSID	Direccionamiento
Equipos de red	2001:1234:abc:00::/56
Cima	2001:1234:abc:0010::/60
Eventos	2001:1234:abc:0020::/60
Fisicauios	2001:1234:abc:0030::/60
Gietec	2001:1234:abc:0040::/60
Managment	2001:1234:abc:0050::/60
Wan-docentes	2001:1234:abc:0060::/60
Wlan-estudiantes	2001:1234:abc:0070::/60
Wlan-ups-adm	2001:1234:abc:0080::/60
Wlan-biblioteca	2001:1234:abc:0090::/60

Nota. Direccionamiento a utilizarse en el diseño.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.6 Diseño físico.

El diseño físico de la red muestra cuales equipos se utilizan para BYOD, además las conexiones necesarias para este diseño formando una topología en estrella extendida, este diseño se muestra en la figura 29.

Topología física de la solución.

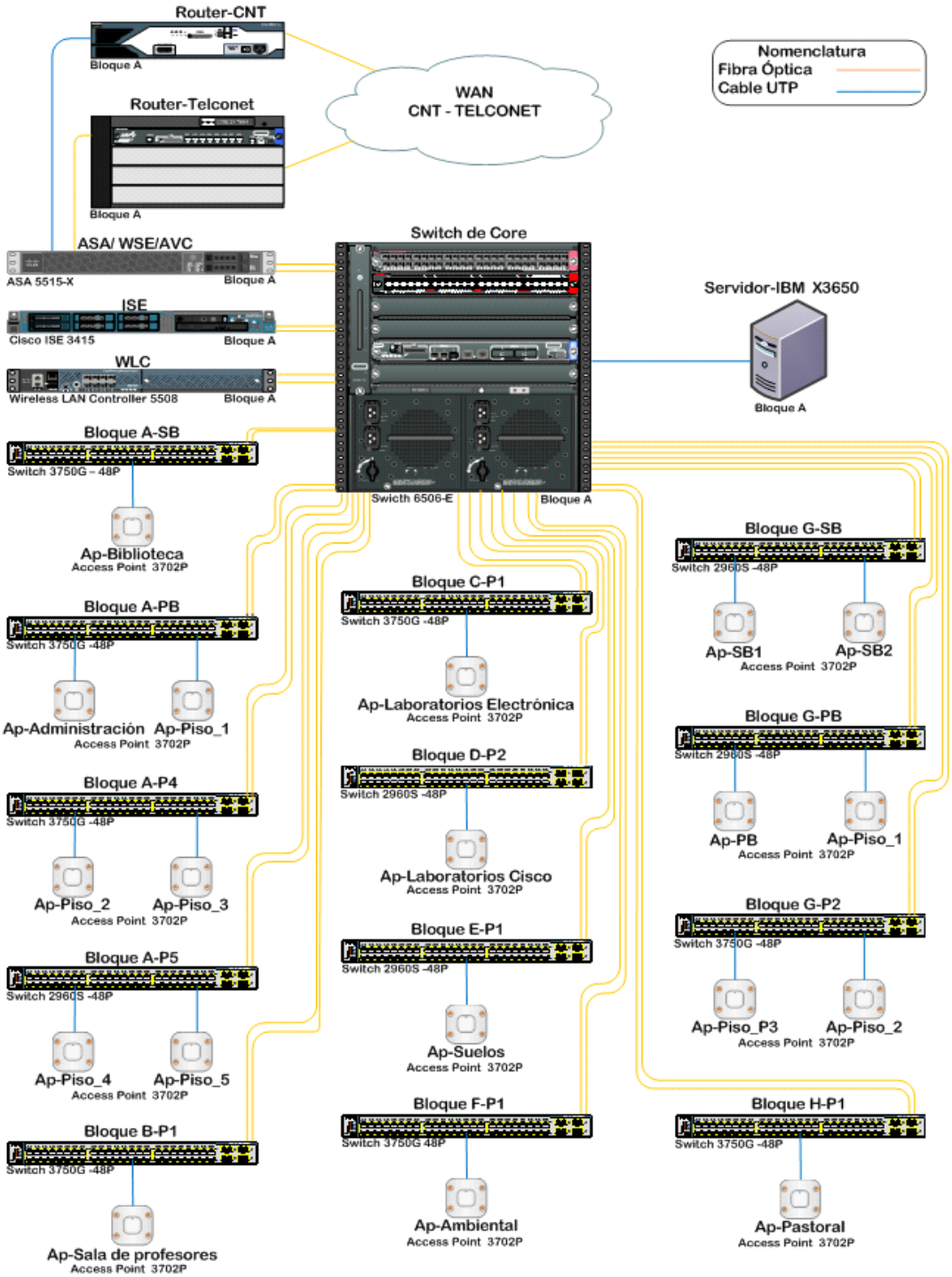


Figura 29. Topología física de la solución.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.7 Integración de los equipos.

En la integración de los equipos con el ISE es necesario tomar en cuenta algunos aspectos para su correcta operatividad.

4.7.1 Integración ISE y Active Directory.

Integración ISE y Active Directory.

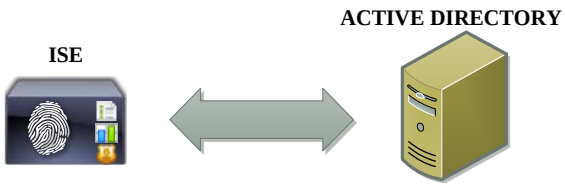


Figura 30. Integración ISE y Active Directory.
Elaborado por: Andrea Díaz y Danilo Lamar.

Antes de conectar ISE con el dominio de Active Directory (AD), se debe comprobar lo siguiente: ISE y Active Directory deben estar sincronizados en tiempo, si hay un firewall entre ISE y AD, algunos puertos deben estar abiertos para permitir la comunicación entre los dos, si la fuente de Active Directory tiene varios dominios, se debe garantizar la existencia de relaciones de confianza entre el dominio de ISE y los otros dominios con recursos a los que necesite tener acceso, el servidor DNS que se configura en el ISE debe ser capaz de resolver los nombres de dominio en el origen de la identidad de AD, el servidor DNS que está en el servidor de AD también debe ser configurado en el ISE, el nombre de usuario de AD que se preste mientras se unen a un dominio deber ser definido en AD y debe tener cualquiera de los siguientes permisos (dominio, creación o eliminación de objetos, permisos de usuarios y grupos) y comprobar que el servidor de AD no resida detrás de un traductor de direcciones de red y que no tiene una traducción de direcciones de red.

4.7.1.1 Grupos de identidad de Active Directory

El grupo de identidad es una lista lógica utilizada para criterios de valoración de grupos en función de sus perfiles. Los dispositivos que pasan por el proceso de aprovisionamiento y el registro se agregan al grupo de identidad de registro de ISE. El grupo de identidad se utiliza en las políticas de autorización para asignar privilegios de acceso a la red en los puntos finales o para aplicar otras reglas. También se pueden mover a otros grupos de identidad, como la identidad de grupo Lista Negra, que se utiliza cuando un dispositivo se pierde o ha sido robado. Se pueden crear varios grupos en el AD. La tabla 38 destaca un ejemplo.

Tabla 30.
Ejemplo de políticas en AD.

Política	**Identidad**	**Grupo de ad**	**Perfil**	**Permiso**
Personal_AccesoCompleto	Registrados	BYOD_Admin	Cualquier S.O.	Completo
Personal_AccesoParcial_1	Registrados	BYOD_Docentes	Android	Parcial
Personal_AccesoParcial_2	Registrados	BYOD_Estudiantes	Android	Parcial
Personal_SoloInternet	No registrados	Invitados	Cualquier S.O.	Internet

Nota. Ejemplo de política con Active Directory.
Elaborado por: Andrea Díaz y Danilo Lamar.

ISE permite al administrador de red seleccionar grupos específicos y los atributos de AD. Esto permite que los tiempos de búsqueda sean más rápidos al autenticar un usuario. También ayuda a asegurar que, cuando el administrador crea una política relacionada con grupos de AD, el administrador tiene que mirar a través de solo una pequeña lista en lugar de cada grupo en Active Directory.

4.7.1.2 Pasos para la configuración de Active Directory.

A continuación se describen los pasos a seguir para la configuración del AD:

1. Iniciar Windows Active Directory en Windows Server.
2. Definir el nombre de dominio completo (Fully Qualified Domain Name, FQDN) del AD durante la instalación por ejemplo servidor.ups.com.
3. Crear un grupo "Admin" y asociar un usuario perteneciente a este grupo y crear otro grupo "Docentes" y asignar un usuario a este grupo. Una cuenta de administrador (creado por defecto en AD) será usada por ISE para unirse al dominio, donde se podrá editar, modificar, importar usuarios y grupos en AD.
4. Realizar un ping al servidor de AD ya que ISE debería ser accesible para este servidor con el fin de que ISE pueda unirse al dominio de AD.

4.7.1.3 Pasos para la configuración de ISE.

A continuación se listan los pasos a seguir en la configuración del ISE:

1. ISE debe unirse al dominio definido en el servidor de AD.
2. En ISE el servidor DNS debe estar configurado para que apunte a la dirección IP de AD, ya que el resolverá el nombre de dominio de AD a través de esta

dirección IP. Después de esto se reiniciarán todos los procesos en el ISE en aproximadamente 10 minutos de tiempo de inactividad de la red. Luego de esto se confirmará el reinicio exitoso de todos los procesos de ejecución.

3. Una vez guardada la configuración se debe realizar una prueba de conexión. En esta prueba se confirmará la accesibilidad al controlador de dominio y la sincronización.
4. Una vez conectado el ISE al AD se deben importar los grupos del AD al ISE.
5. Definir una política de autenticación en el ISE de tal manera que cada usuario que inicie de forma remota un dispositivo se autentique con el ISE-AD.

4.7.2 Integración ISE y Wireless LAN Controller (WLC)

Integración ISE y Wireless LAN Controller.

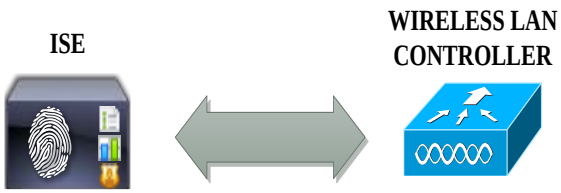


Figura 31. Integración ISE y Wireless LAN Controller.
Elaborado por: Andrea Díaz y Danilo Lamar.

En la integración de estos dos equipos se deben tener en cuenta algunos aspectos los cuales serán descritos a continuación en cada tema.

4.7.2.1 Pasos para integrar WLC a ISE.

A continuación se describe los pasos para integrar WLC a ISE:

1. Desde ISE ingresar en Administración>Recursos de red>Dispositivos de red y llenar los siguientes parámetros del WLC:
    a. Nombre: ingresar el nombre del WLC.
    b. Dirección IP: asignada al WLC.
    c. Habilitar las herramientas de autenticación.
    d. Habilitar protocolo: radius.
    e. Contraseña: contraseña compartida cisco.
2. Una vez guardada la entrada del WLC se debe confirmar que el controlador este en la lista de dispositivos agregados.

4.7.2.2 Pasos para integrar ISE a WLC.

ISE junto con el WLC deben estar configurados para permitir 802.1X y la característica CoA para los puntos finales.

1. Ingresar en el WLC, Seguridad>Autenticación>Nuevo.
2. Ingresar los parámetros:
    a. Dirección IP del servidor ISE.
    b. Clave secreta compartida: cisco.
    c. Soporta RFC 3576 (CoA): habilitar (por defecto).
    d. Todo lo demás: por defecto.
3. Seleccionar RADIUS Accounting>añadir nuevo.

4.7.2.3 Pasos para configurar ISE para autenticación inalámbrica.

1. Desde ISE ingresar a Política > Autenticación
2. Escoger la opción Dot1X > Wired_802.1X
3. Agregar condición de adicionales ingresando a Condición Compuesto> Wireless_802.1X.
4. Establecer la condición expresa de que OR, esta permitirá escoger una autenticación tanto alámbrica como inalámbrica.
5. Aceptar los usuarios internos por defecto Wireless_802.1X.

4.7.2.4 Creación de interfaz dinámica en el WLC.

Se crean interfaces dinámicas para distinguir entre los tráficos de invitados y usuarios registrados.

1. Controlador>Interfaces
    a. Nombre de interfaz: empleados.
    b. Vlan id: número de la vlan asignada.

4.7.2.5 Añadir IEEE 802.1X en el WLC.

Aquí se requieren los siguientes pasos:

1. Desde WLC ir a WLAN> crear nuevo.

2. Ingresar nombre de perfil, SSID, ID.
3. Para la configuración de WLAN>ficha general, utilizar lo siguiente:
    a. Política radio: All.
    b. Grupo/ Interfaz: administración.
    c. Todo lo demás: por defecto.
4. WLAN>pestaña seguridad>Layer 2, utilizar lo siguiente:
    a. Seguridad Capa 2: WPA+WPA2.
    b. Política WPA"/encriptar: Habilitar/AES.
    c. Administración de llave de autenticación: 802.1X.
5. WLAN>seguridad>ServidorAAA> seleccionar:
    a. Servidor de autenticación/Contabilidad: habilitado.
    b. Dirección de servidor: dirección IP del servidor ISE.
6. WLAN>opciones avanzadas elegir:
    a. Permitir AAA anular: habilitado.
    b. Estado NAC: Radius NAC.
7. WLAN>General seleccionar:
    a. Estado: habilitado.

4.7.2.6 Estado de postura.

El cumplimiento de estado (postura) de un punto final puede ser:

- UNKNOWN (desconocido): No hay datos que fueron recogidos con el fin de determinar la postura, nuevo cliente.
- NONCOMPLIANT (no cumple): se realizó una evaluación de la postura y uno o más requisitos fallo, todo trafico bloqueado.
- COMPLIANT (cumple): la estación cumple con todos los requisitos obligatorios, se permite todo el tráfico.

4.7.2.7 Configuración global en el WLC.

Aquí se deben tomar en cuenta dos aspectos:

1. Asegúrese de que el servidor RADIUS tiene RFC3576 (CoA) activado, que este activado por defecto.

2. Desplácese hasta Listas de Control de Seguridad>Access, cree ACL en el WLC dependiendo de los tres diferentes estados de postura del dispositivo.

4.7.3 Integración ISE y Adaptive Security Appliance (ASA).

Integración ISE y Adaptive Security Appliance.

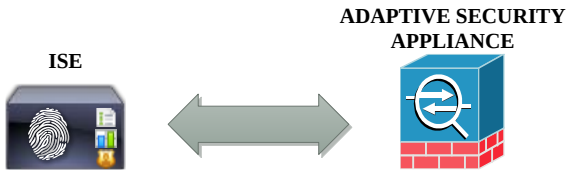


Figura 32. Integración ISE y Adaptive Security Appliance.
Elaborado por: Andrea Díaz y Danilo Lamar.

Es fundamental esta integración ya que se propone tener un equipo destinado hacia la seguridad de la red.

4.7.3.1 Registro de ASA con ISE

Para registrar ASA con ISE, se realizan los siguientes pasos:

1. Inicie sesión en el ISE.
2. Seleccione Administración>Dispositivos de red.
3. Haga clic en agregar.
4. Introduzca la dirección IP de Cisco ASA.
5. Cuando ISE se utiliza para la autenticación de usuarios, introduzca una calve secreta compartida en el área de Configuración de autenticación. Al configurar el servidor AAA en el ASA, proporcione la clave secreta compartida que se crea en el ISE. El servidor AAA en el ASA utiliza esta clave secreta compartida para comunicarse con el ISE.
6. Especifique un nombre de dispositivo, ID de dispositivo, una contraseña y un intervalo de descarga de ASA.

4.7.3.2 Creación de un grupo de seguridad en ISE.

Al configurar el servidor de AAA en el ASA, se debe especificar un grupo, este grupo debe estar configurado para utilizar el protocolo RADIUS. Para crear un grupo de seguridad en el ISE, se realiza los siguientes pasos:

1. Inicie sesión en el ISE.
2. Elija Política > Política Elementos > Resultados > Seguridad Grupo de Acceso > Grupo de seguridad.
3. Añadir un grupo de seguridad para ASA. Con esto ISE crea una entrada en grupos de seguridad con una etiqueta.
4. En la sección Seguridad de Acceso a grupo, configurar las credenciales de identificación de dispositivos y una contraseña para el ASA.

4.7.4 Integración ISE y Cisco Catalyst 6506-E/3750G/2960S Series Switch

Integración ISE y Cisco Catalyst 6506-E/3750G/2960S Series Switch.

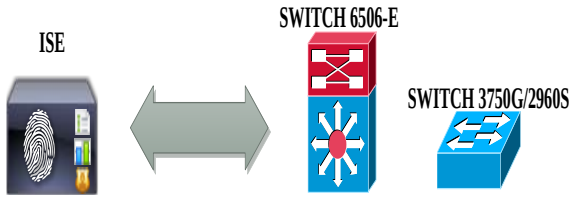


Figura 33. Integración ISE y Cisco Catalyst 6506-E/3750G/2960S Series Switch.
Elaborado por: Andrea Díaz y Danilo Lamar.

Los swicthes permiten la autenticación 802.1X para los dispositivos del cliente e interactúan con ISE utilizando el protocolo RADIUS. Con base en los resultados del proceso de autenticación, un usuario puede tener acceso restringido o completo a la red mediante la asignación de VLAN y una lista de control de acceso descargable (DACL). La configuración flexible de autenticación permite utilizar tanto 802.1X y MAC de omisión de autenticación (MAB) como un mecanismo de reserva.

Se requieren los siguientes pasos para configurar acceso al switch para AAA:

1. Habilitar la autenticación, autorización y contabilidad (AAA).
2. Crear un método de autenticación para 802.1X (uso por defecto todos los servidores RADIUS para la autenticación).
3. Crear un método de autorización para 802.1X (habilita RADIUS para la aplicación de políticas).
4. Crear un método de contabilidad para 802.1X (proporciona información adicional acerca de las sesiones con ISE).

Se requieren los siguientes pasos para configurar acceso al switch para RADIUS:

1. Agregar servidor ISE al grupo RADIUS.
2. Configurar en el servidor ISE un tiempo muerto (15 segundos en total, 3 reintentos de 5 segundos de tiempo de espera).
3. Configurar el switch para enviar atributos específicos del proveedor de Cisco.
4. Configurar los atributos específicos del proveedor de Cisco.
5. Configurar la dirección IP para el uso de mensajes RADIUS.

Se requieren los siguientes pasos para configurar acceso al switch para 802.1X:

1. Activar 802.1X global.
2. Habilitar el seguimiento de dispositivos IP.

Los siguientes pasos para permitir a 802.1X ser flexible en la autenticación:

1. Configure la autenticación prioritaria Dot1X sobre MAB.
2. Configure la orden de autenticación prioritaria Dot1X sobre MAB.
3. Habilitar autenticación flexible.
4. Habilitar la relación con más de una dirección MAC en el puerto físico.
5. Configure la acción de violación (en caso de fallar la autenticación).
6. Habilitar el puerto para 802.1X.
7. Habilitar el puerto para MAB.
8. Configure temporizadores para MAB.
9. Encienda la autenticación.
10. Habilitar la ACL por defecto al puerto.
11. Habilitar el servidor http y https.

4.8 Políticas.

Es necesario definir políticas de seguridad y calidad de servicio que permita que el acceso a la red sea confiable. En la tabla 31 se puede observar un ejemplo de política que se puede implantar en la red debido al BYOD.

Tabla 31.
Ejemplo de políticas en ISE.

Usuario	**Dispositivo**	**Método de Acceso**	**Lugar**	**Tiempo**	**Política**
Invitados	Personal	Inalámbrico	Bloques Campus Sur	Lunes a Viernes 8:00–16:00	Vlan Invitados
Estudiantes	Personal	Inalámbrico	Bloques Campus Sur	Lunes a Viernes 7:00–19:00	Vlan Estudiantes Acl Estudiantes
Docentes	Personal o institucional	Inalámbrico	Bloques Campus Sur	Cualquier momento	Vlan Docentes Acl Docentes
Administrativos	Personal o institucional	Inalámbrico y cableado	Bloques Campus Sur	Cualquier momento	Vlan Administrativos Acl Administrativos

Nota. Ejemplo de los aspectos que se involucran en una política de ISE.
Elaborado por: Andrea Díaz y Danilo Lamar.

BYOD hace posible que la comunidad salesiana del Campus Sur pueda utilizar distintos dispositivos para acceder a la red.

Etapas de BYOD.

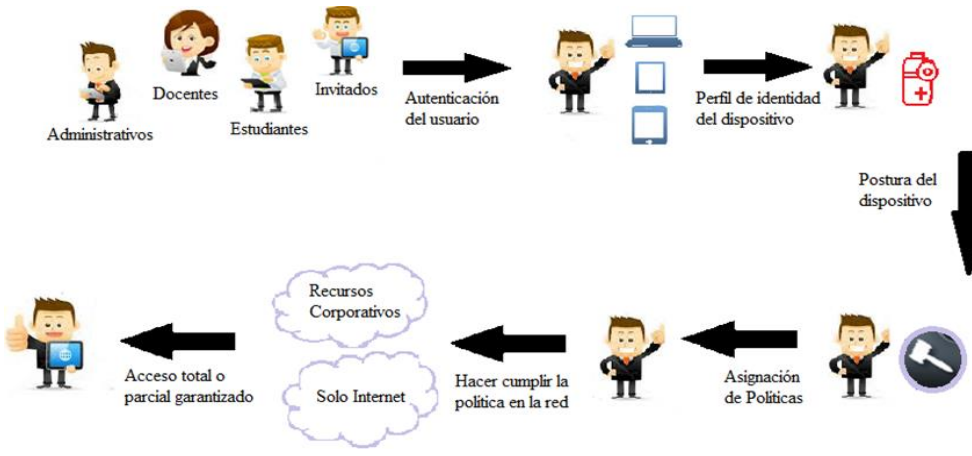


Figura 34. Etapas de BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.9 Enrolamiento y aprovisionamiento.

Los usuarios de la institución deben estar previamente enrolados y pertenecer a un grupo en el AD.

1. El usuario debe conectarse al SSID: BYOD_Aprovisonamiento, que lo redirige a un portal de registro, donde se realizará la autenticación.
2. Cuando se ha autenticado correctamente, empieza la inscripción de certificados y el perfil de aprovisionamiento, el cual adquiere información sobre el dispositivo, entonces el servidor de políticas asigna una política al usuario además, lo puede cambiar a un segundo SSID seguro.
3. Para conexiones posteriores, el dispositivo utilizara el SSID seguro.
4. Los dispositivos de invitados que no pasen el proceso de aprovisionamiento, se conectarán a un SSID de invitados el cual podrá estar configurado solo para brindar acceso a internet a este grupo de usuarios.

Ejemplo de aprovisionamiento.

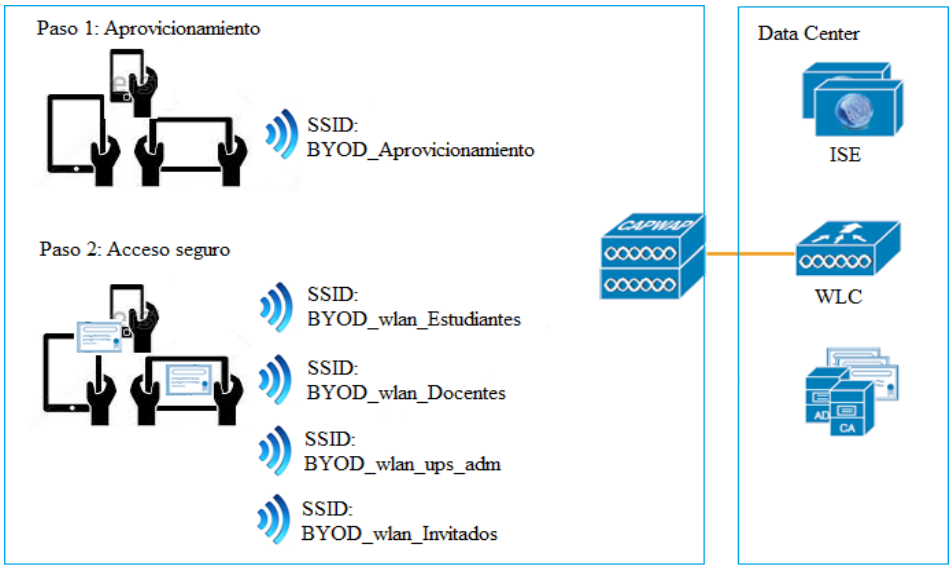


Figura 35. Ejemplo de aprovisionamiento.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.10 Flujo de conectividad.

ISE evalúa certificados digitales, la pertenencia a grupos de Active Directory, tipo de dispositivo, utilizando herramientas, de esta manera el acceso se basa en credenciales y otras condiciones. ISE puede tener diferentes niveles de acceso a la red configurados, los cuales se pueden hacen cumplir con ACLs, SGT o Vlan.

Flujo de conectividad.

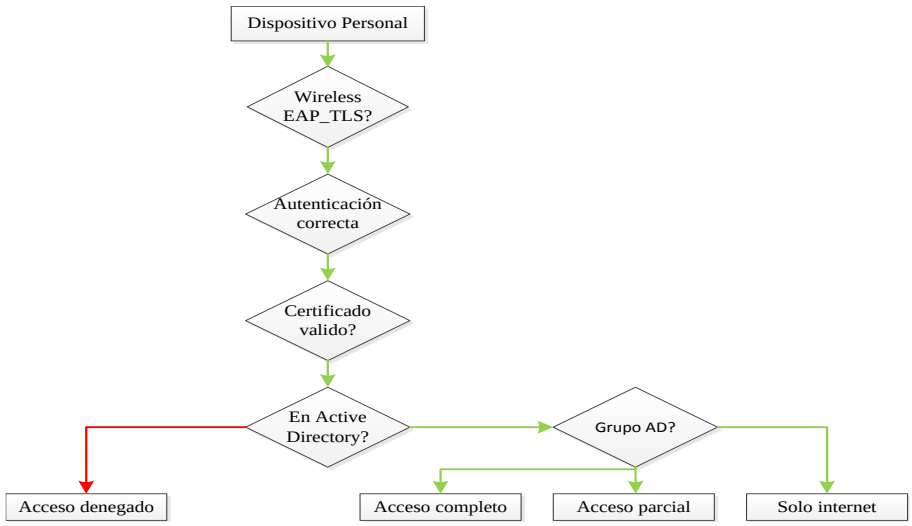


Figura 36. Flujo de conectividad.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.10.1 Acceso a la red.

La capacidad de Cisco ISE para hacer cumplir la política de acceso a la red hace que sea fácil para los administradores de TI proporcionar a los usuarios una experiencia de acceso de red confiable. Cisco ISE permite realizar la autenticación de usuarios, perfiles de dispositivo, y la evaluación de la postura en una red inalámbrica configurada para la autenticación IEEE 802.1X. La autenticación y la autorización para los usuarios inalámbricos se explican en la figura 37.

Autenticación y autorización.

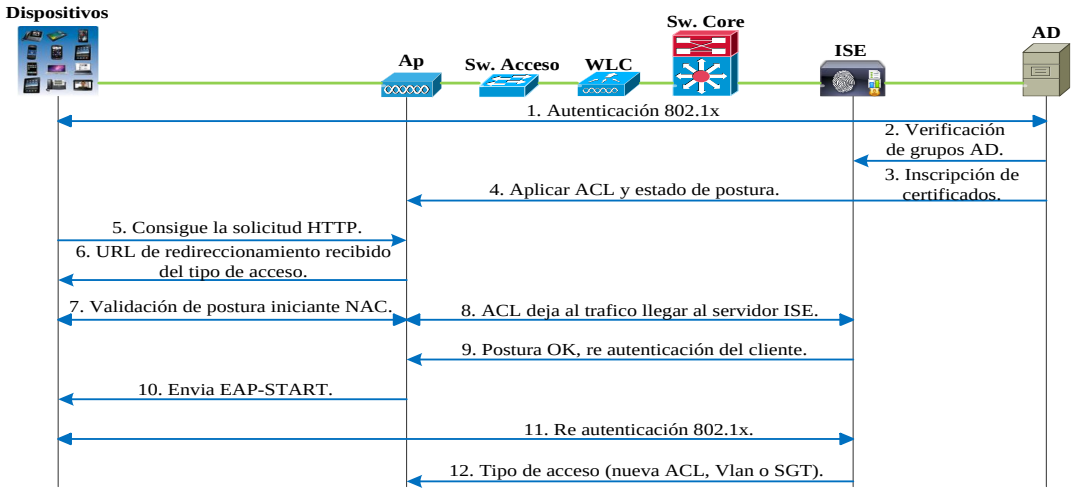


Figura 37. Autenticación y autorización.
Elaborado por: Andrea Díaz y Danilo Lamar.

1. El usuario se autentica correctamente mediante 802.1X.
2. ISE valida al usuario en la base de datos de AD.
3. Una vez autenticado correctamente inicia la inscripción de certificados.
4. Acepta el acceso RADIUS que redirige a una URL con ACLs de pre-autenticación, que provee direcciones y puertos IP o VLAN de cuarentena.
5. Cliente será redirigido a la URL dependiendo el tipo de acceso que tenga y se pondrá en un modo de solicitud de estado postura, hasta que la validación de postura sea completa.
6. El agente NAC en el cliente inicia la validación de la postura: el agente envía una solicitud de descubrimiento HTTP por el puerto 80, que el controlador redirige a una URL proporcionada por el tipo de acceso. ISE conoce que el cliente está tratando de llegar a él y responde directamente al cliente. De esta manera el cliente se entera de la IP de ISE y, a partir de ahora, el cliente se comunica directamente con ISE.
7. El WLC permite este tráfico debido a la ACL configurada para permitirlo. En el caso de anulación de VLAN, se crea un puente para que el tráfico llegue al ISE.
8. Cuando el cliente de ISE completa la evaluación, un RADIUS CoA con servicio de re autenticación es enviado al WLC, que inicia la re autenticación del cliente (mediante el envío de EAP- START). Cuando la re autenticación tiene éxito, ISE envía el tipo de acceso por ejemplo (Acceso Aceptado) con una nueva ACL (si existe) y no redirige a ninguna URL o acceso VLAN.
9. En lugar de ACL descargables, tenemos que utilizar ACL pre configuradas en el WLC. ISE envía el nombre de ACL, que ya está configurado en el WLC.

4.11 Funciones de ISE.

ISE provee de varios servicios a la red, a continuación se menciona algunos de ellos: RADIUS con autenticación, autorización, contabilidad, incluye 802.1X y MAC autenticación bypass (MAB), autenticación Web (local, central y registro de dispositivos), servicios de portal de visitantes y patrocinadores, representación de estado de transferencia (monitoreo), registro de dispositivos y aprovisionamiento, acceso a grupo de seguridad SGT (TrusSec), Postura (cumplimiento de punto final y remediación) y administración de dispositivos móviles (MDM de terceros).

4.12 Funciones de ASA.

ASA es un firewall de siguiente generación en el cual tiene algunos servicios: Coincidencia de aplicaciones, cortafuego basado en identidad, filtrado URL, prevención de intrusos, solución de gestión intuitiva, control y visibilidad de aplicaciones (AVC), servicios para restringir el uso de aplicaciones Web (WSE), y sistema de prevención de intrusos (IPS).

4.13 Red piloto con BYOD.

La red piloto con BYOD de la Universidad Politécnica Salesiana da a conocer cómo se lleva a cabo una administración de los dispositivos móviles en el cual se puede observar la gestión de políticas por dispositivo o usuario, seguridad, calidad de servicio y otros servicios adicionales que se pueden tener en un ambiente con BYOD. Para la simulación se eligió productos de la marca Cisco Meraki en comparación a otros proveedores como HP, Citrix y Aruba debido a varios factores como son: costo de equipos, manejabilidad de las configuraciones, la infraestructura de Cisco Meraki provee de servicios similares a los de la infraestructura de Cisco propuesto en el diseño de red, exponer que BYOD se puede llevar a cabo en otras infraestructuras de red. En la tabla 32 se puede ver los factores por lo cual se eligió Cisco Meraki.

Tabla 32.
Factores para la elección de equipos para la red piloto.

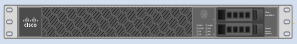
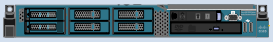
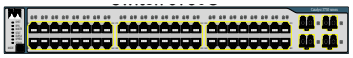
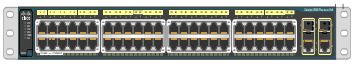
Factores	Cisco	HP	Citrix	Aruba	Meraki
Intervención de hardware y software.	O	O	O	O	X
Costo de hardware o software.	O	O	O	O	X
Costo de licenciamiento.	+	+	+	+	X
Costo de garantías.	+	+	+	+	X
Manejabilidad Configuraciones.	X	X	X	+	+
Similitudes con el diseño de red propuesto.	O	O	+	+	O
Adaptabilidad a los dispositivos de usuarios.	O	O	O	O	O
Accesibilidad a los recursos o equipos por parte de proveedores.	+	+	+	+	X

Nota: X= bajo, O = alto y + = medio.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.13.1 Diseño de la red piloto.

El diseño de la red piloto está enmarcado en la utilización de equipos, los cuales puedan ser similares a los propuestos en el diseño de red. En la tabla 33 se muestra la comparativa entre los equipos de la propuesta y los equipos de la red piloto.

Tabla 33.
Representación de equipos.

Equipos de red propuesta	Equipos de red piloto
ASA/WSE/AVC 5515  ISE 3415  WLC 5508  IBM X3650 	MDM en Cloud y System Manager 
Switch de Core 6506  Switch 3750  Switch 2960  Access Point 3702P 	 Meraki Z1 

Nota. Representación entre los equipos en el diseño de red y la red piloto.
Elaborado por: Andrea Díaz y Danilo Lamar.

La figura 38 se muestra la topología de la red piloto.

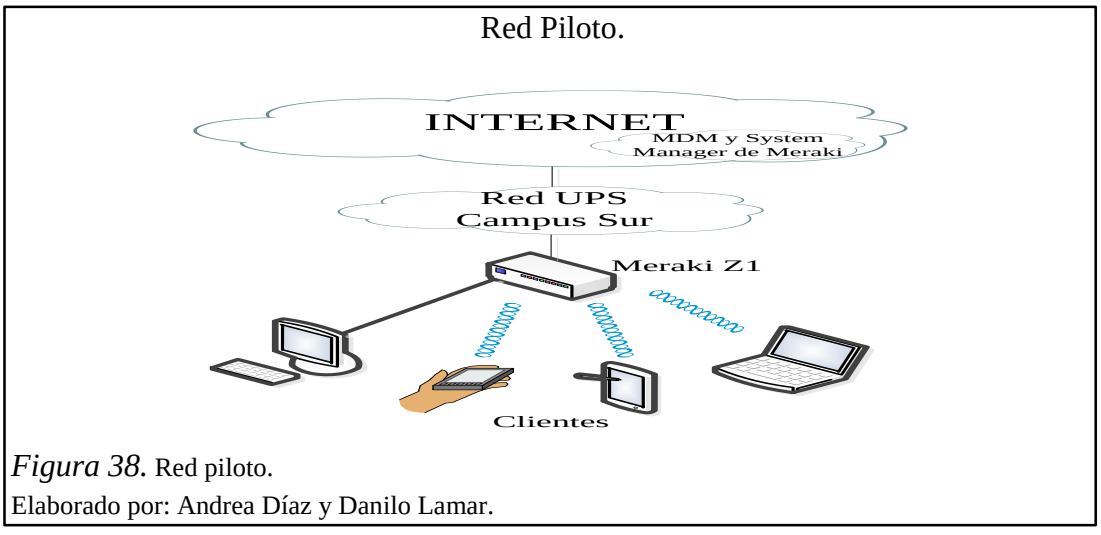


Figura 38. Red piloto.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.13.2 Proveedores.

Cisco Meraki es una plataforma de gestión en la nube para infraestructuras de red, los servicios están organizados en centros de datos que tienen certificados tipo TIER 1, SAS70 Tipo II / SASE16, un acuerdo de nivel de servicio (LSA) del 99,99% (Cisco Meraki, 2015). Algunas características de Cisco Meraki son: replicación de configuraciones en tiempo real entre los centros de datos dentro de 60 segundos, la configuración de red y las estadísticas son almacenadas en la nube, todos los datos sensibles son encriptados y almacenados, se ocupa 1 Kb/s para los datos de administración entre el equipo y la nube de Cisco Meraki, el espacio de almacenamiento es ilimitado en la nube de Cisco Meraki para las configuraciones (Dynacom, 2015).

Telconet es la empresa que presta servicios de internet y datos a las Universidad Politécnica Salesiana, se tiene un ancho de banda de 120 Mbps, los cuales son repartidos para todo el campus por parte del departamento de TI (Departamento TI UPS, 2013). La prueba piloto se realizó en los laboratorios de Cisco donde se tiene 6 Mbps de velocidad tanto en subida como en bajada, esta velocidad fue utilizada en la realización de la red piloto y administrada para cada una de las redes inalámbricas creadas en el equipo Cisco Meraki. Para la parte de WAN la red trabaja con una interfaz de 1 GbE, la cual tiene 6 Mbps de velocidad, en la LAN se tienen varias velocidades según las políticas aplicadas a las VLAN creadas en la configuración.

4.13.3 Equipos para la red piloto.

En las siguientes tablas se muestran los componentes usados para la red piloto.

Tabla 34.
Equipos de red.

Componente	Función
Meraki Dashboard	Configuración del equipo de red vía web.
MDM de Meraki en Cloud	Gestión de los equipos móviles de clientes.
Meraki Z1	Accesibilidad a configuraciones de equipo y al MDM.

Nota. Equipos utilizados para la red piloto.
Elaborado por: Andrea Díaz y Danilo Lamar.

Tabla 35.
Equipos para pruebas.

Dispositivos	Función	Versión de software
Samsung Galaxy S3 mini.	Dispositivo móvil.	Android 4.1.2
Samsung Galaxy Tab 3	Dispositivo móvil.	Android 4.2.2
Laptop Hp.	Dispositivo inalámbrico/alámbrico.	Microsoft Windows 7, 64 bits.
Laptop Toshiba.	Dispositivo inalámbrico/alámbrico.	Microsoft Windows 7, 64 bits.
Laptop Toshiba.	Dispositivo inalámbrico/alámbrico.	Microsoft Windows 8, 64 bits.

Nota. Equipos para las pruebas en la red piloto.
Elaborado por: Andrea Díaz y Danilo Lamar.

Para la red piloto los equipos e infraestructura que se ocupó presentan algunas características. En la tabla 36 se menciona al MDM de Meraki.

Tabla 36.
MDM de Meraki.

- Gestión centralizada en la nube.
- Gestión unificada de dispositivos multiplataforma.
- Gestión de software y aplicaciones.
- Control de acceso a la red.
- Aplicación de restricciones y políticas de seguridad.
- Seguimiento de inventario y estados de dispositivos.
- Geolocalización.
- Calidad de servicio (QoS).
- Visibilidad de la red en tiempo real.
- Seguimiento de seguridad para clientes.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

En la tabla 37 se presentan las características del equipo Cisco Meraki Z1.

Tabla 37.
Cisco Meraki Z1.

Rendimiento	**Control y Seguimiento**
• Firewall: 50 Mbps • VPN: 10 Mbps	• Rendimiento, conectividad, monitoreo y alertas por correo electrónico.

Interfaces • Interfaz WAN: 1x GbE • Interfaz LAN: 4x GbE • 1x USB 2.0 puerto para 3G / conectividad 4G.	• Historial de detalles por puerto y estadísticas de uso por cliente. • Estadísticas de uso de aplicaciones. • Registros de cambios de nivel de organización para el cumplimiento y gestión del cambio. • Túnel VPN y monitoreo de la latencia. • Descubrimiento de activos de la red e identificación de usuarios. • Correos electrónicos periódicamente con métricas de clave de utilización. • Integración Syslog.
Servicio de red y seguridad • Estado Firewall, 1:1 NAT, DMZ • Auto (site-to-site IPsec) VPN • Cliente VPN (IPsec L2TP), • Límite de 2 usuarios autorizados (sólo con la autenticación alojada en Meraki) • Nivel de aplicación (Capa 7) Análisis de tráfico y conformación. • Múltiple WAN IP, PPPoE, NAT. • Soporte VLAN y servicios DHCP. • Enrutamiento estático. • Cuarentena de usuario y dispositivo.	**Diagnostico Remoto** • Captura de paquetes remotos. • Diagnóstico en tiempo real y herramientas de solución de problemas. • Registro de eventos agregados con búsqueda instantánea.
Integración Inalámbrica • 4 SSID. • 2 x 802.11a/b/g/n (2.4Ghz o 5Ghz). • Velocidad de datos máxima 600 Mbit/s. • 2x2 MIMO • 4x Antenas dipolo internas (ganancia: 3dBi – 2.4 Ghz, 4 dBi – 5Ghz) • Autenticación WPA2-PSK	**Administración** • Gestión a través de Internet. • Redes cableadas e inalámbricas. • Despliegue remoto. • Actualizaciones de firmware automáticas y parches de seguridad. • Gestión centralizada de políticas. • Org-nivel de autenticación de dos factores y simple sign-on.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

4.13.4 Similitudes y diferencias de la red piloto a implementarse.

Las características implantadas en la red piloto están relacionadas con la red inalámbrica de la UPS, la tabla 38 muestra estas similitudes y las diferencias.

TABLA 38.
Similitudes y diferencias de la red inalámbrica UPS con la red piloto.

Características	**Red inalámbrica UPS y Red piloto**	
	Similares	Diferentes
Redes inalámbricas	x	
Direccionamiento	x	
Creación de usuarios		x
Porta cautivo	x	
Firewall	x	
Control de ancho de banda		x
Calidad de servicio	x	
Vlans	x	
MDM		x
Asignación de tráfico		x
Grupo de políticas		x
Control de acceso		x
Alertas		x
Administración		x

Nota. Similitudes y diferencias entre la red inalámbrica de la UPS y la red piloto.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.13.5 Conexiones del equipo Cisco Meraki Z1.

El equipo Cisco Meraki Z1 consta de 4 puertos LAN y 1 puerto para Internet, en la siguiente figura 39 se muestra las conexiones.

Conexiones del equipo.

Figura 39. Conexiones del equipo.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.13.6 Creación de la cuenta en Cisco Meraki.

Para poder administrar al Cisco Meraki Z1 se debe crear una cuenta en la nube de Meraki. La figura 40 muestra la creación de la cuenta.

Creación de la cuenta para la administración del equipo.

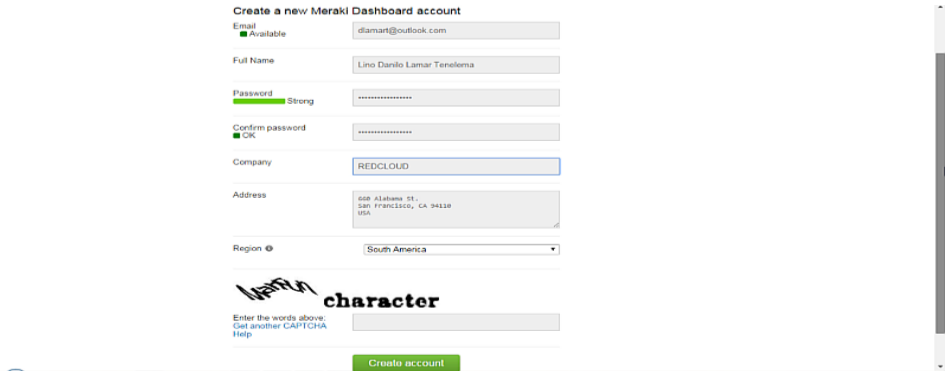


Figura 40. Creación de la cuenta para la administración del equipo.
Elaborado por: Andrea Díaz y Danilo Lamar.

En la figura 41 se tiene la bienvenida a la cuenta en Meraki.

Bienvenida de la cuenta de Meraki.

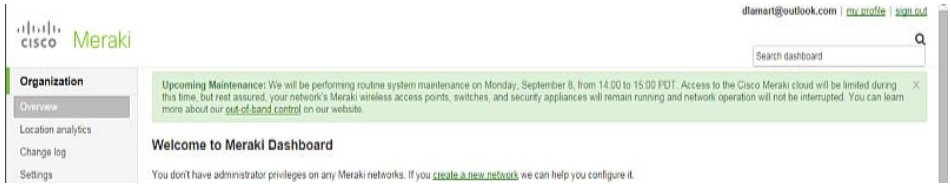


Figura 41. Bienvenida de la cuenta de Meraki.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.13.7 Registro de Cisco Meraki Z1.

Luego de crear la cuenta en Meraki se necesita registrar el equipo, verificar el estatus de la licencia y crear una red en la cual se va a reclamar al equipo registrado para empezar a realizar las configuraciones. En las siguientes figuras puede observar este proceso.

Registro del equipo.

Figura 42. Registro del equipo.
Elaborado por: Andrea Díaz y Danilo Lamar.

Verificación de la licencia.

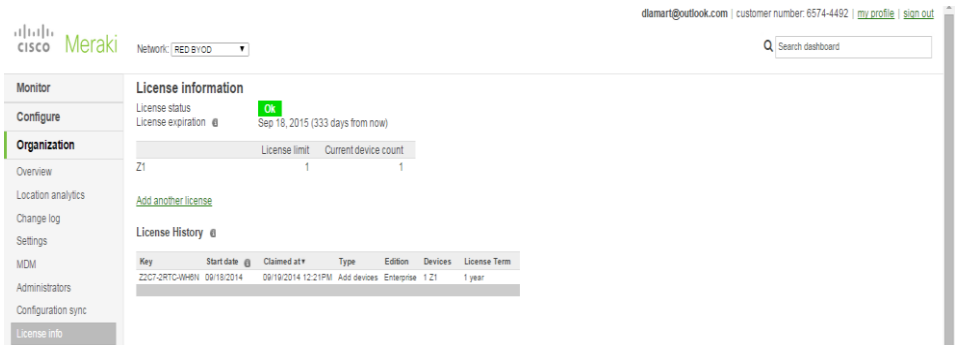


Figura 43. Verificación de la licencia.
Elaborado por: Andrea Díaz y Danilo Lamar.

Creación de la RED BYOD.

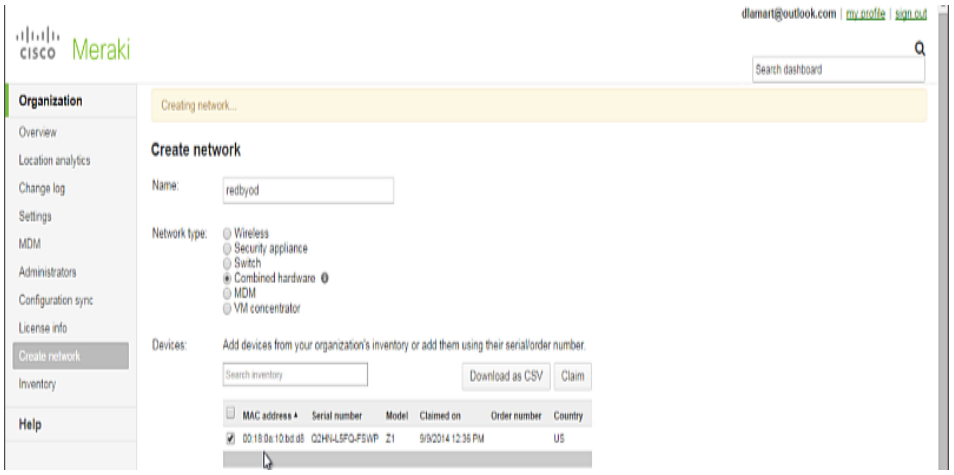


Figura 44. Creación de la RED BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

Creación de la red MDM BYOD.

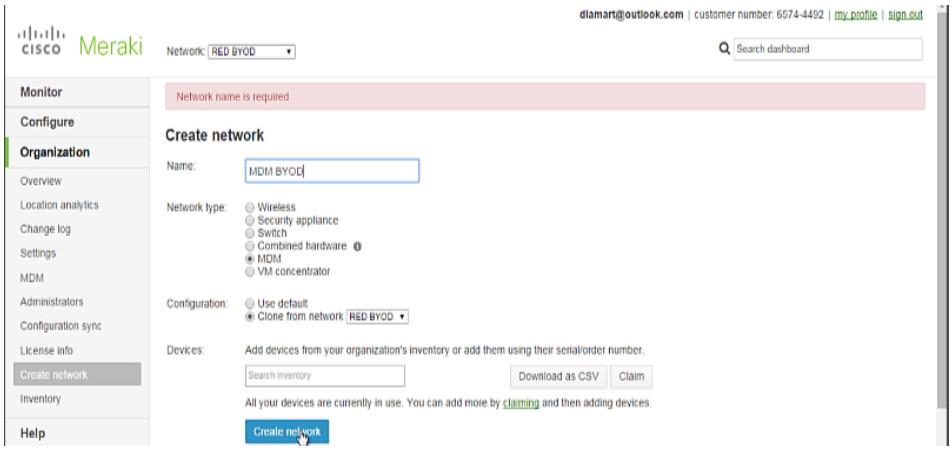


Figura 45. Creación de la red MDM BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

4.13.8 Direccionamiento de la red piloto.

El direccionamiento para la red piloto se basa en la utilización del direccionamiento IP del tipo clase B 172.17.X.X, el cual también utiliza la universidad. Además se especificaron otros parámetros que se presentan a continuación:

- Nombre: Administrativos, IP de red 172.17.20.0/24, ID de VLAN 20.
- Nombre: Docentes, IP de red 172.17.30.0/24, ID de VLAN 20.
- Nombre: Estudiantes, IP de red 172.17.40.0/24, ID de VLAN 20.
- Nombre: Invitados, IP de red 172.17.50.0/24, ID de VLAN 20.

4.13.9 Seguridades en la red piloto.

Las seguridades configuradas en la red piloto son las siguientes: uso del estándar IEEE 802.1X, página de autorización para el ingreso a internet, control de acceso a la red mediante NAC, configuración para el uso de uno o varios dispositivos en la red, políticas de seguridad por parte del MDM (requerimiento de ingreso, chequeo de antivirus y antispyware, contraseña de dispositivo, verificado de cortafuegos, etc).

4.13.10 Ventajas y desventajas de Cisco Meraki.

Cisco Meraki tiene un sistema de gestión intuitivo que permite al personal de TI realizar configuraciones de manera rápida y sencilla con una administración en tiempo real de la infraestructura de red con fácil escalabilidad y reducción de costos en la implementación, también se pueden crear políticas de seguridad para la red inalámbrica y la red Ethernet que permitan proteger a los dispositivos (multiplataforma) y los datos.

Algunos inconvenientes que presenta una arquitectura de red con Meraki es la incompatibilidad con sistemas operativos de poca demanda, además cuando no se tenga accesos a la nube de Meraki los servicios dejaran de estar disponibles temporalmente como también las herramientas de configuración y diagnóstico.

Las configuraciones realizadas sobre la RED BYOD y el MDM BYOD, se presentan desde el anexo diez hasta el anexo diecisiete.

CAPÍTULO 5
ANÁLISIS DE PRUEBAS Y OBTENCIÓN DE RESULTADOS

5.1 Pruebas y resultados.

Las pruebas se las obtuvo tanto del usuario como del administrador de red.

- Administrador

En la figura 46 se observa un resumen general de toda la red.

Visión general de la red.

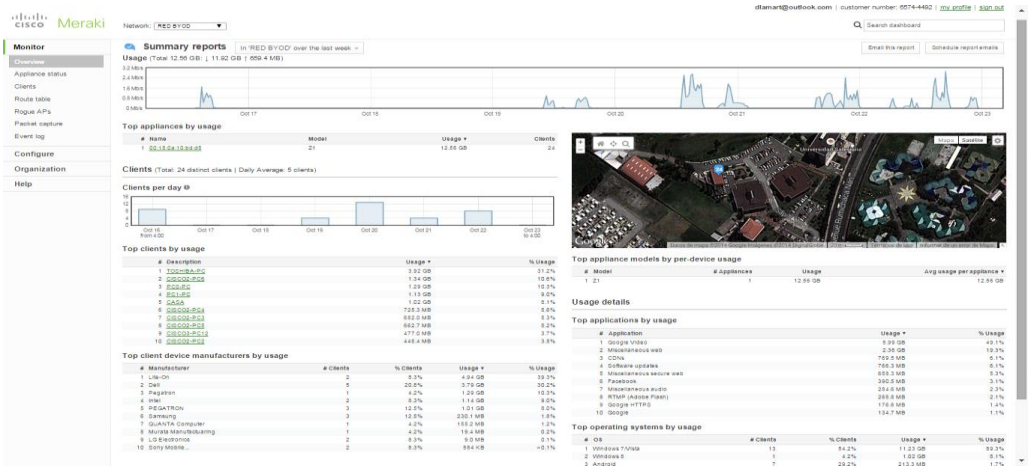


Figura 46. Visión general de la red.
Elaborado por: Andrea Díaz y Danilo Lamar.

La figura 47 muestra los parámetros del equipo y además otras herramientas útiles para administrar la red.

Estado del equipo.

Figura 47. Estado del equipo.
Elaborado por: Andrea Díaz y Danilo Lamar.

La figura 48 muestra los dispositivos conectados a la red.

Clientes RED BYOD.

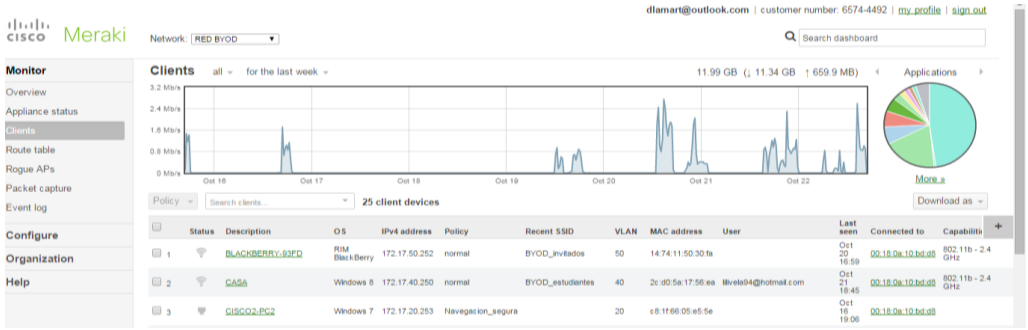


Figura 48. Clientes RED BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

En la figura 49, con la captura de paquetes se observa el tráfico que pasa por ese dispositivo.

Captura de paquetes.

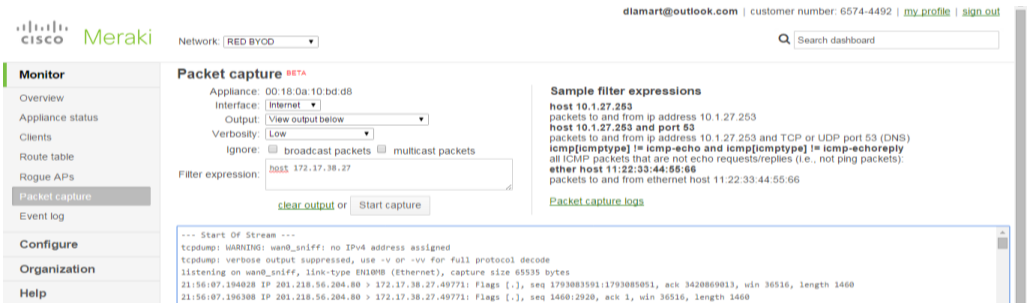


Figura 49. Captura de paquetes.
Elaborado por: Andrea Díaz y Danilo Lamar.

La figura 50 muestra el log de eventos en el cual se observa que hechos han sucedido en la red, además que nos entregan detalles de los mismos.

Log de eventos.

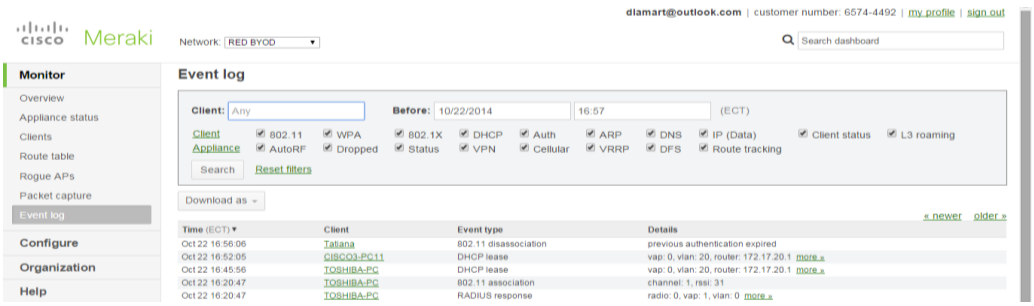


Figura 50. Log de eventos
Elaborado por: Andrea Díaz y Danilo Lamar.

En la figura 51 muestra los clientes que están en el MDM BYOD y algunos detalles de los dispositivos conectados.

Lista de clientes en el MDM BYOD.

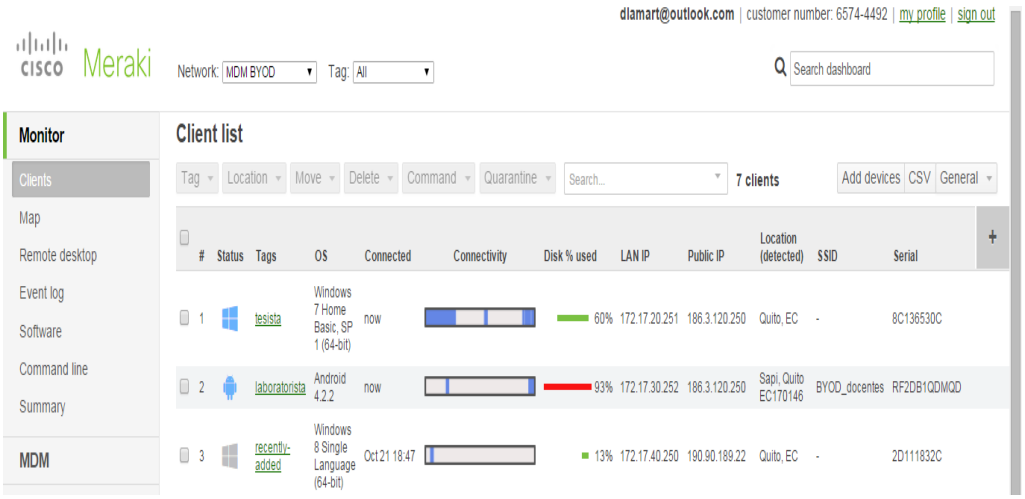


Figura 51. Lista de clientes en el MDM BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

En la figura 52 muestra los clientes en un mapa y su estado.

Ubicación geográfica de los clientes.

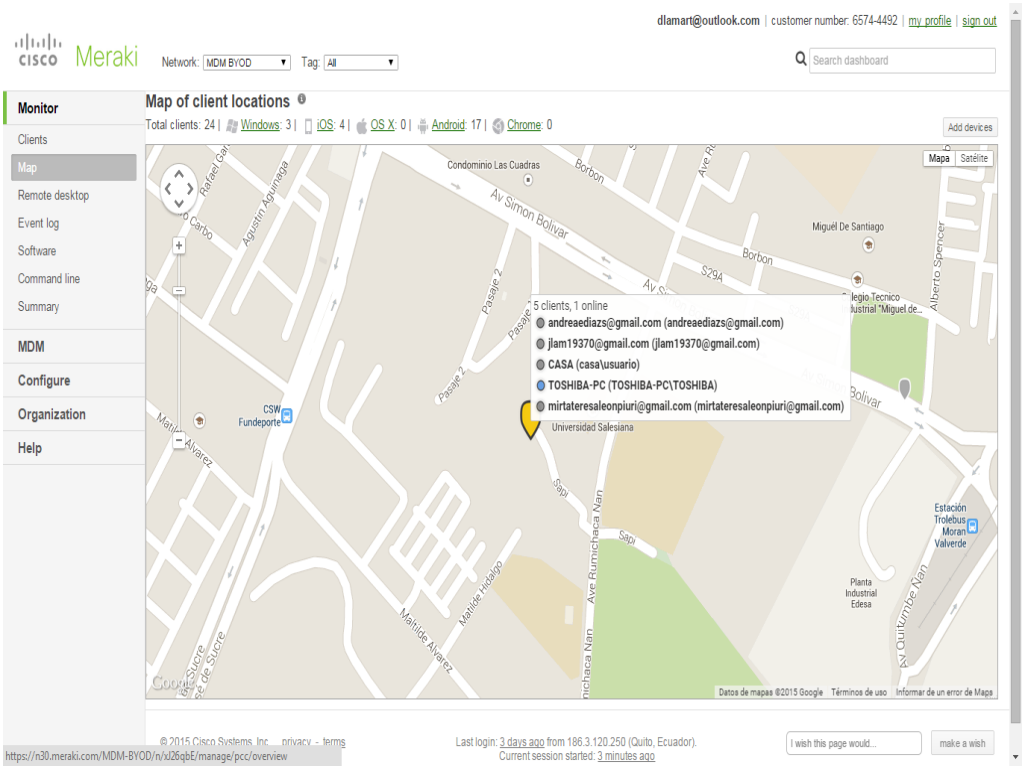


Figura 52. Ubicación geográfica de los clientes.
Elaborado por: Andrea Díaz y Danilo Lamar.

La figura 53 muestra el log de eventos en el MDM y algunos detalles de estos eventos.

Log de eventos en MDM BYOD.

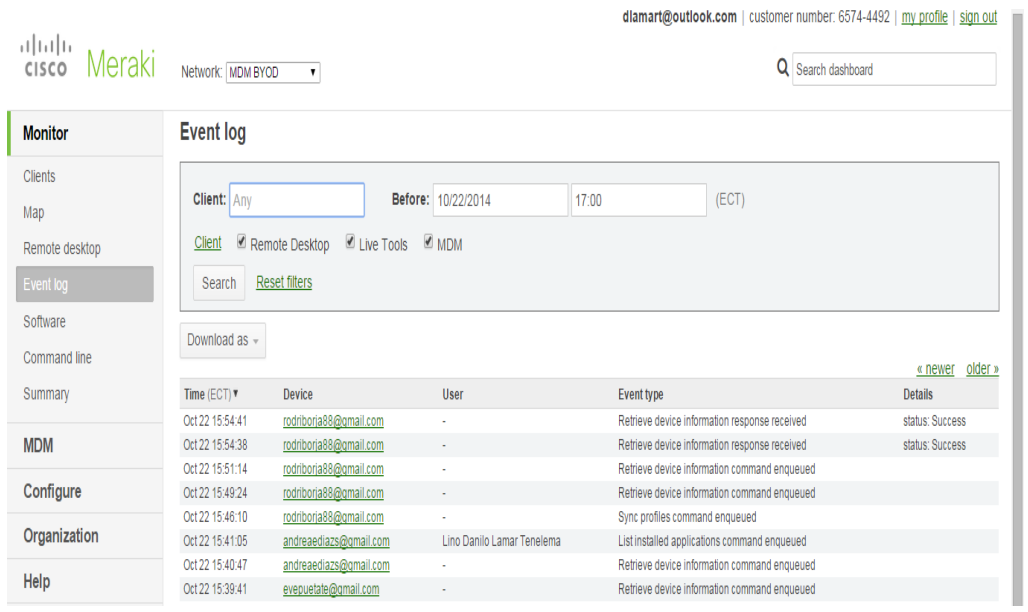


Figura 53. Log de eventos en MDM BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

La figura 54 muestra un inventario de todo el software que contiene los distintos dispositivos conectados al MDM BYOD.

Inventario de software.

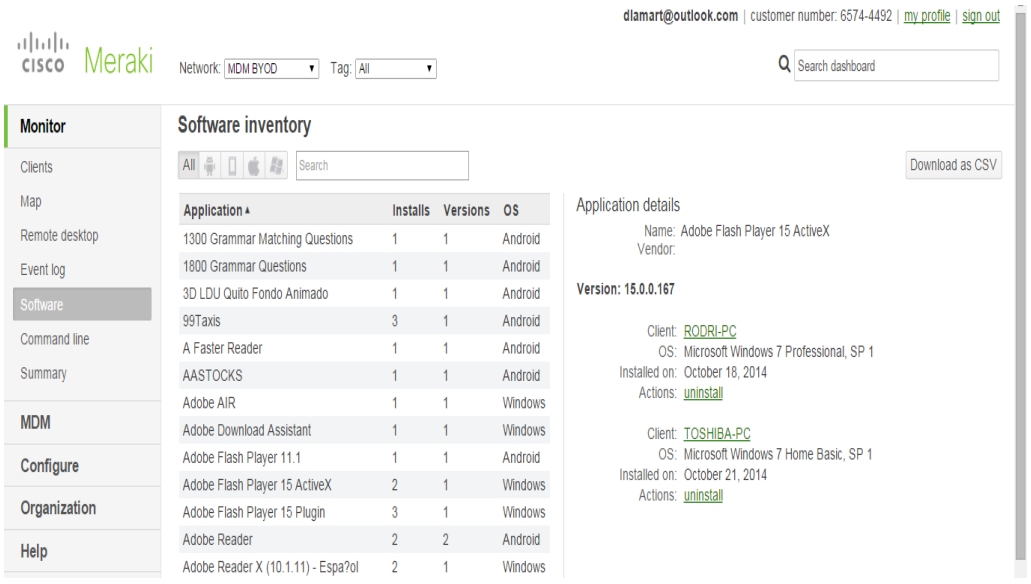


Figura 54. Inventario de software.
Elaborado por: Andrea Díaz y Danilo Lamar.

La figura 55 muestra una opción para ingresar comandos en un cliente.

Línea de comandos.

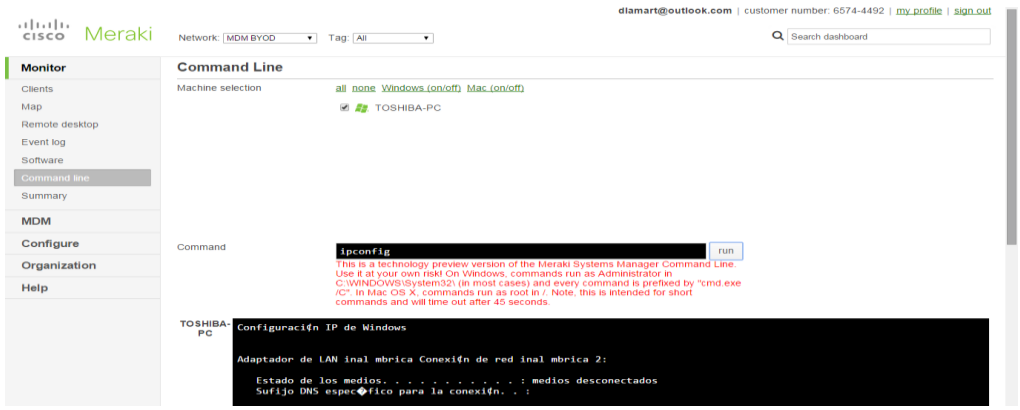


Figura 55. Línea de comandos.
Elaborado por: Andrea Díaz y Danilo Lamar.

En la figura 56 muestra un resumen general de la red MDM BYOD.

Resumen de la red MDM BYOD.

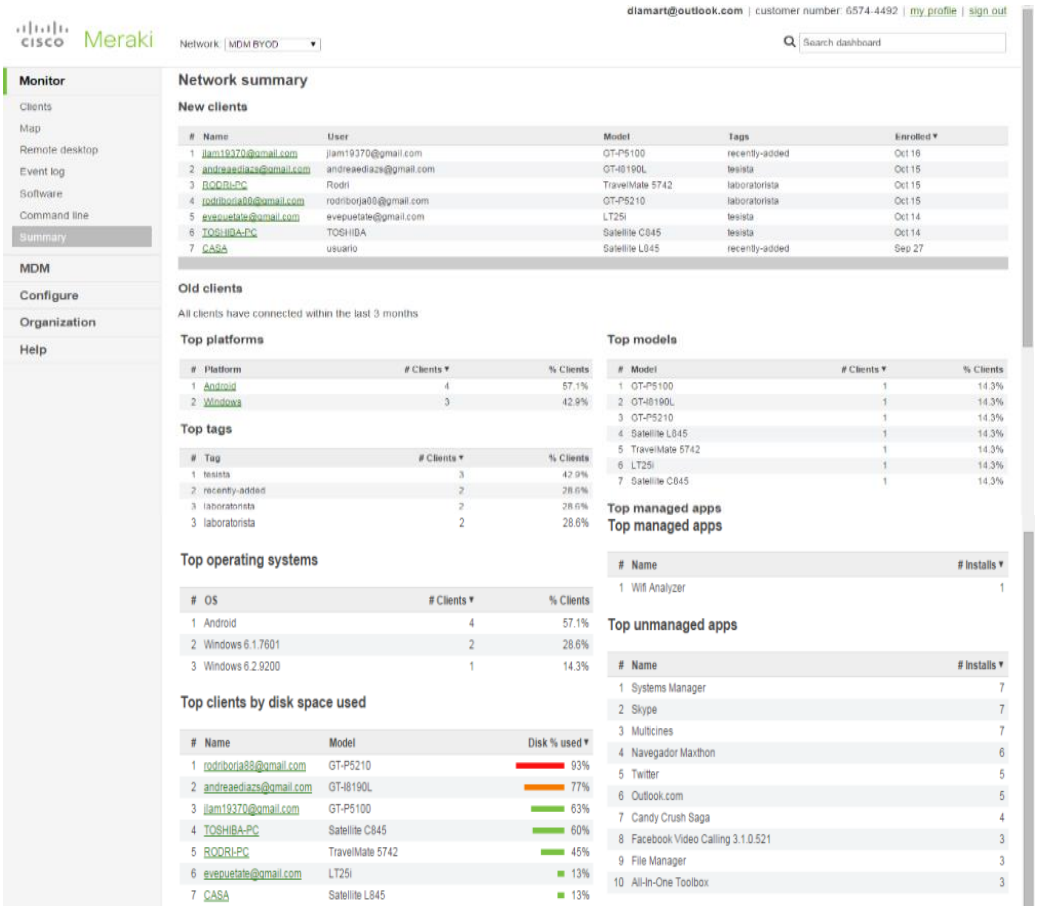


Figura 56. Resumen de la red MDM BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

Revisión de un cliente específico en Windows.

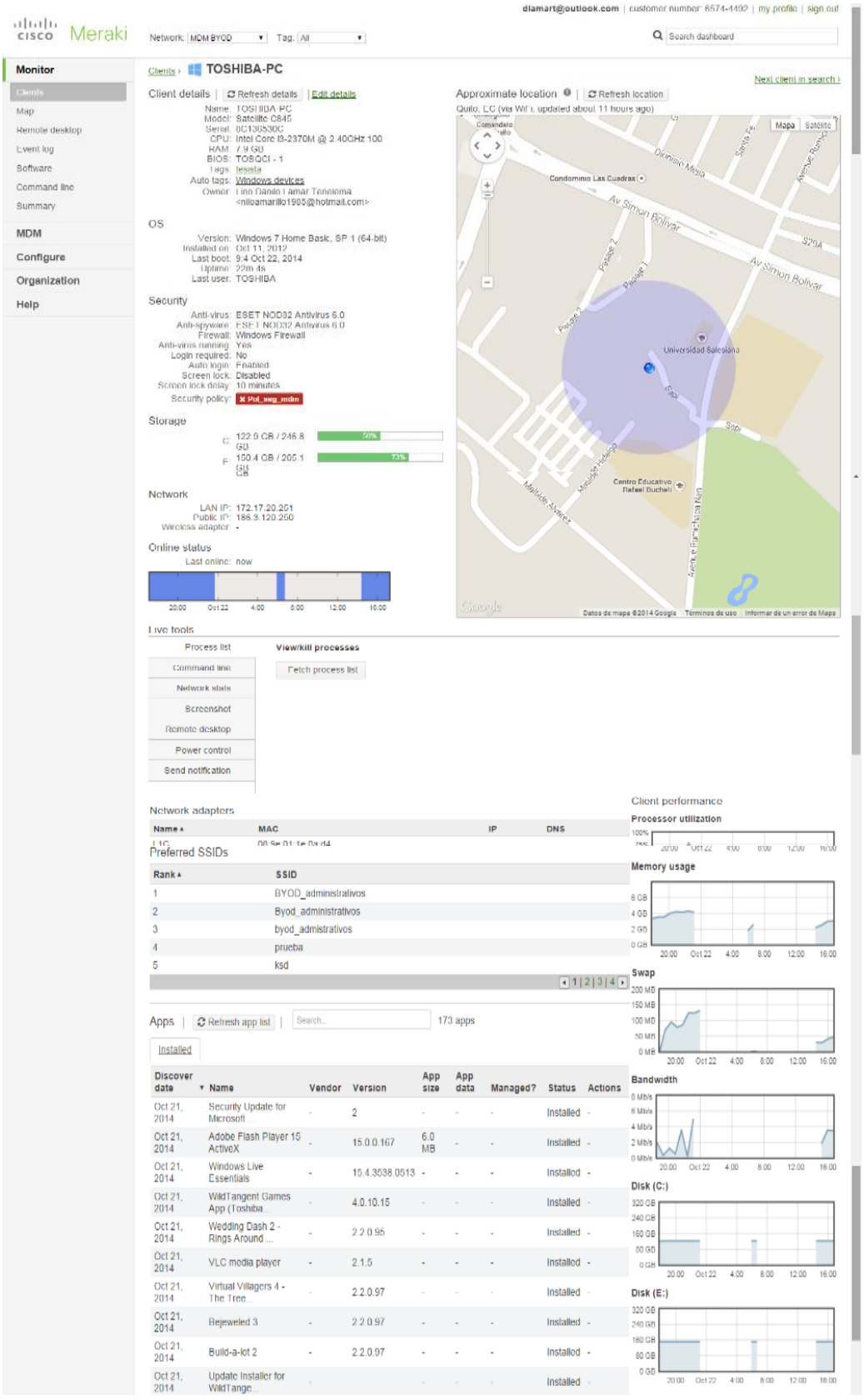


Figura 57. Revisión de un cliente específico en Windows.
Elaborado por: Andrea Díaz y Danilo Lamar

Revisión de un cliente específico en Android.

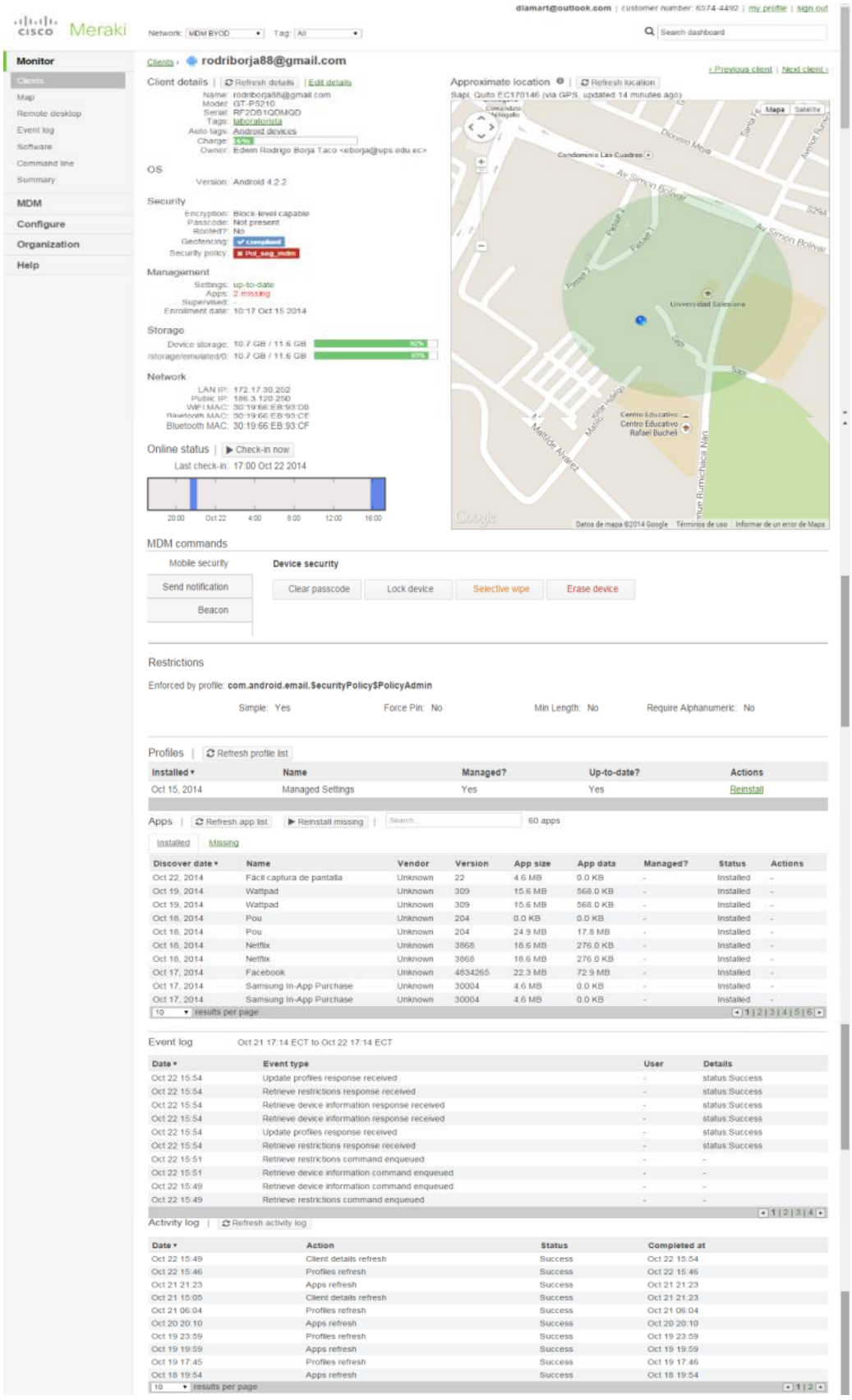
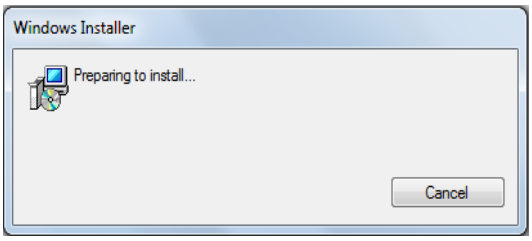


Figura 58. Revisión de un cliente específico en android.
Elaborado por: Andrea Díaz y Danilo Lamar.

- Usuario

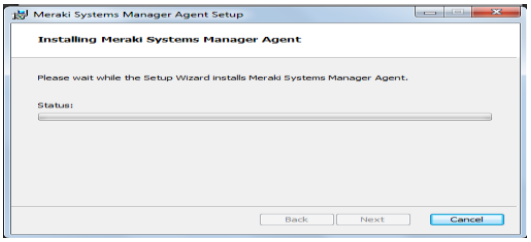
A continuación se muestran las pruebas de conexión en los clientes, las cuales, dependiendo del dispositivo, instalarán un agente o un app.

Instalación de agente en computador o laptop para MDM BYOD.

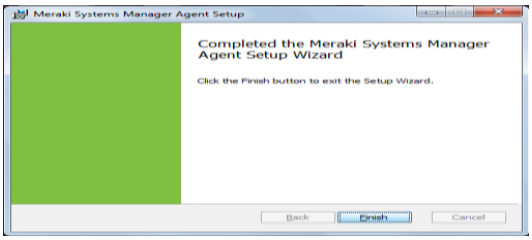


a) Inicio de instalación.

b) Acepto terminos de licencia



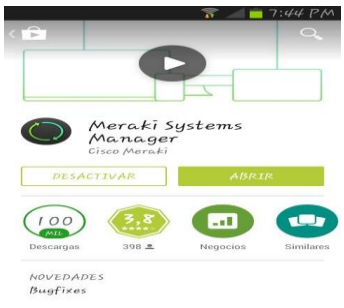
c) Instalacion en proceso.



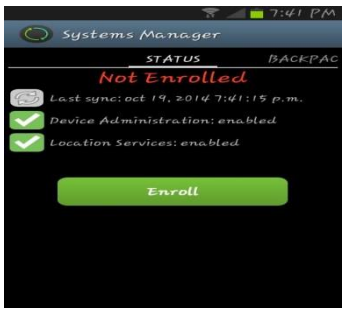
d) Fin de instalación.

Figura 59. Instalación de agente en computador o laptop para MDM BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

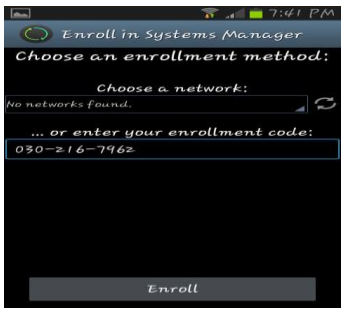
Instalación de app en teléfono móvil para MDM BYOD.



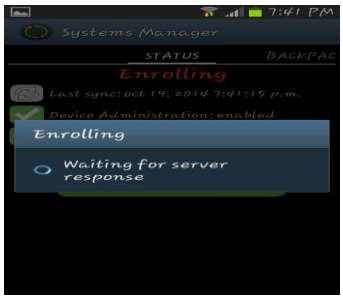
a) Inicio de instalación.



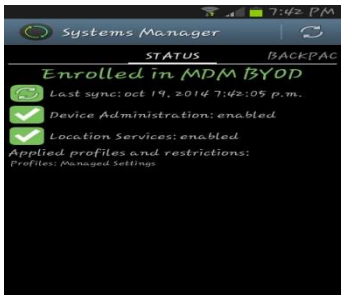
b) Dispositivo no enrolado.



c) Ingreso de clave para enrolar.



d) Enrolando dispositivo.

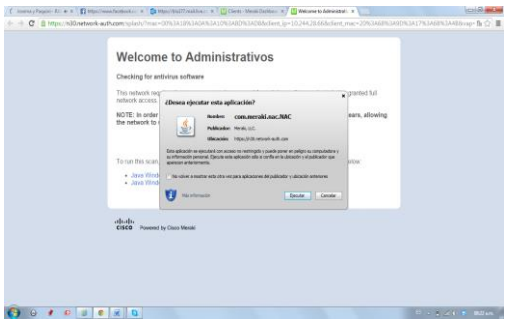


e) Enrolameinto satisfactorio.

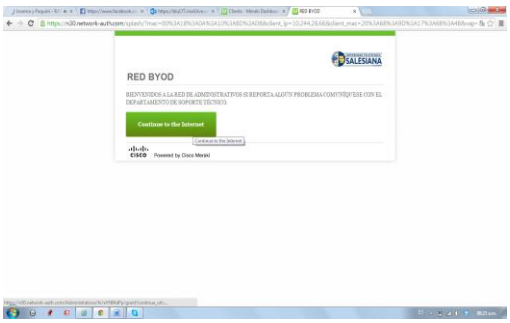
f) Administrador de app.

Figura 60. Instalación de app en teléfono móvil para MDM BYOD.
Elaborado por: Andrea Díaz y Danilo Lamar.

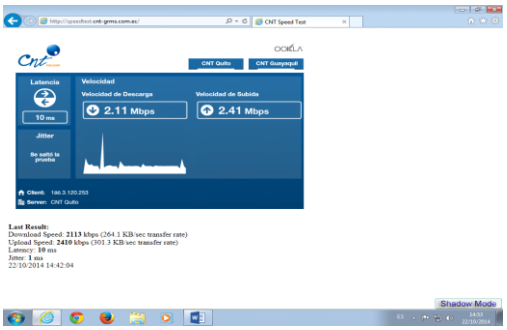
Pruebas en la red administrativa.



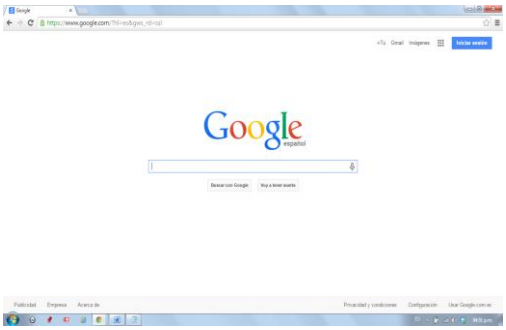
a) Software para chequeo de equipo.



b) Página de bienvenida a la red.



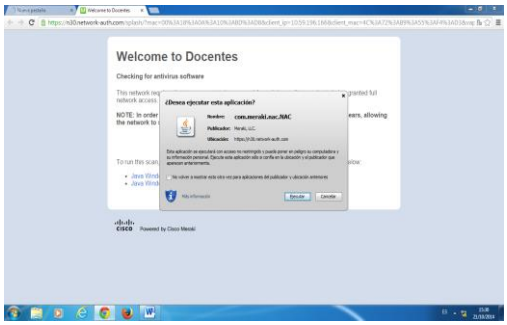
c) Prueba de velocidad.



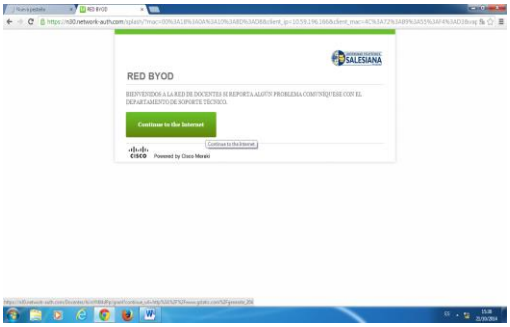
d) Navegación exitosa.

Figura 61. Pruebas en la red administrativa.
Elaborado por: Andrea Díaz y Danilo Lamar.

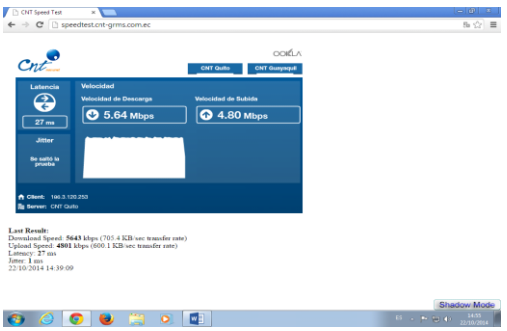
Pruebas en la red docentes.



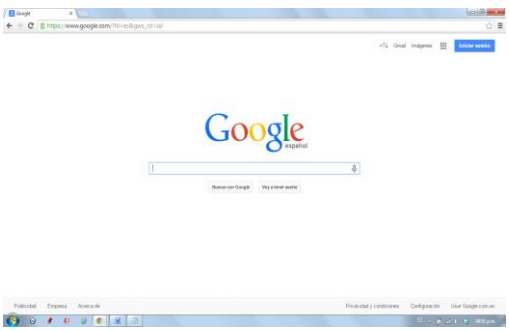
a) Software para chequeo de equipo.



b) Página de bienvenida.



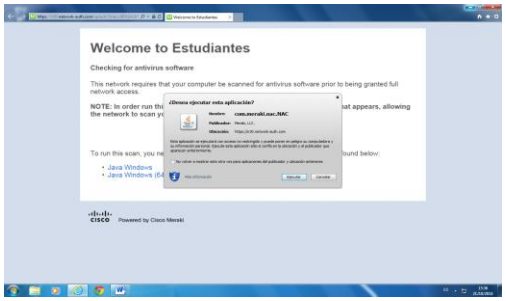
c) Prueba de velocidad.



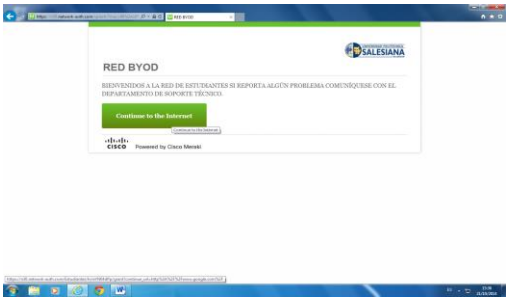
d) Navegación exitosa

Figura 62. Pruebas en la red docentes.
Elaborado por: Andrea Díaz y Danilo Lamar.

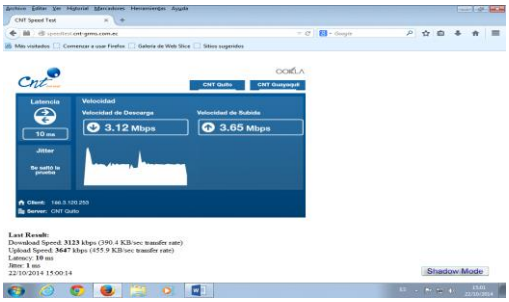
Pruebas en la red estudiantes.



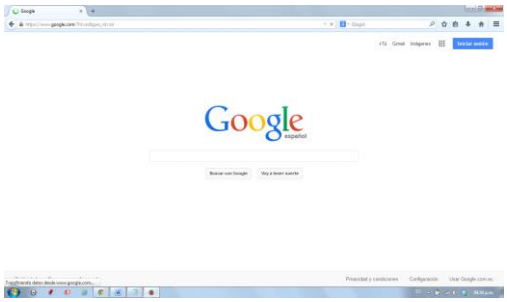
a) Software de chequeo de equipo.



b) Página de bienvenida.



c) Prueba de velocidad.



d) Navegación exitosa.

Figura 63. Pruebas en la red estudiantes.
Elaborado por: Andrea Díaz y Danilo Lamar.

El acceso a la red inalámbrica por parte de los usuarios tiene una concurrencia promedio de 245 usuarios, para tener una certeza en la encuesta del 90% se necesita una muestra mayor o igual a 54 usuarios conectados a la red inalámbrica piloto.

$$n = \frac{Z^2 pqN}{Ne^2 + Z^2 pq}$$

Se realizó una encuestó a 76 estudiantes de la UPS Campus Sur, los cuales fueron subdivididos para los cuatro tipos de usuarios que la red piloto (Administrativos, Docentes, Estudiantes e Invitados) y conectados con sus dispositivos de manera concurrente a la red dependiendo de su tipo de usuario. En las pruebas realizadas a los dispositivos de los usuarios midieron algunas características de BYOD, a saber:

- Políticas de red.
- Seguridad en la red.
- Administración de dispositivos móviles.
- Administración de la red.

La guía de encuesta que se aplicó consta en el anexo dieciocho y en el anexo diecinueve se encuentran el resumen de los resultados.

En la figura 64 se pueden observar gráficamente como están los resultados.

Gráfica de los resultados.

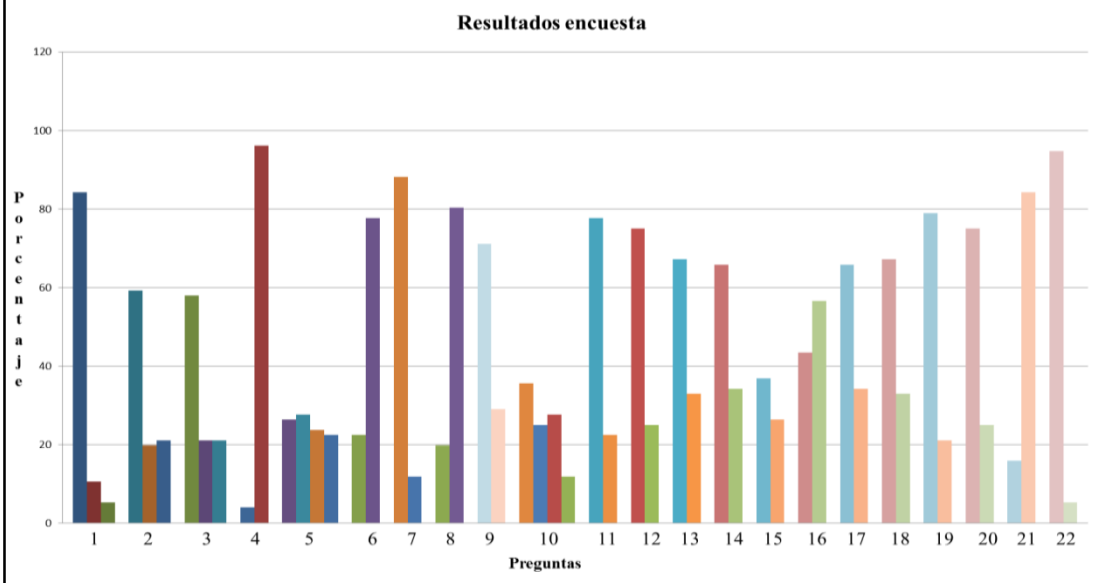


Figura 64. Gráfica de los resultados.
Elaborado por: Andrea Díaz y Danilo Lamar.

- Las preguntas 1, 2, 3 hacen referencia al tipo de dispositivo y características del equipo que tiene los usuarios en la UPS Campus Sur. De la pregunta 1 con 84.21% de los estudiantes tiene por lo menos un dispositivo móvil, el 10.52% posee dos dispositivos móviles y que un 5.26% ostenta tres dispositivos móviles. Además el 59.21% tiene un Smartphone y que el 57.89% prefieren el sistema operativo es Android.
- Las preguntas 2, 7, 9, 14 y 16 tratan acerca de las políticas implantadas en la red de aquí se tiene que, con. La pregunta 2 implica la variedad de dispositivos móviles que pudieron acceder a la red, esto implica que no se tenía restricción alguna en relación a los dispositivos y se tuvo que con un 59.21% lo realizo con un Smartphone, con un 19.73% con una tablet y con un 21.05% con una laptop. La pregunta 7 con un 88.15% refleja cuan fácil fue acceder a la red esto debido a las políticas impuestas en cada red inalámbrica de la red piloto, tanto solo el 11.84% tuvo algún tipo de complicaciones. La pregunta 9 con un 71.05% indica que el enrolamiento a la red fue rápido para los usuarios y con un 28.94% fue lento. la pregunta 14 trata acerca de la descarga de archivos donde se pudo observar que el 65.78% pudo realizar descargar, mientras el 32.89% no pudo realizar la descarga, debido a las políticas implantadas en las configuraciones de ancho. Y finalmente la

pregunta 16 evidencia que el 56.57% de usuarios no notaron los cambios realizados en las políticas mientras que un 43.43% si las noto.

- Las preguntas 4, 5, 6, 8 y 21 están relacionadas acerca de la seguridad que se tenía en la red. La pregunta 4 que decía si tenía problemas con acceder por primera vez a la red tuvo 96.05% de que no hubo problemas. La pregunta 5 refleja el número de usuarios que pudieron acceder a cada una de las redes inalámbricas, siguiendo el debido proceso para su acceso el cual era tener su usuario y contraseña individual, cumpliendo de esta manera con la seguridad implantada en la red piloto y se pudo observar que todos ingresaron a cada una de sus redes respectivas. La pregunta 6 refleja que tan solo el 22.36% tuvo algún tipo problema al cambiarse de red. La pregunta 8 muestra si el dispositivo fue enviado a un sitio de remediación de antivirus esto para proteger a la red y se tiene que tan solo el 19.73% fue enviado al sitio de remediación. Y finalmente en la pregunta 21 se realizó la prueba de apagar el dispositivo y volverlo a encender para ver si tenían algún tipo de problema al conectarse a cada una de las redes inalámbricas creadas en la red piloto y se encontró que el 84.21% de los usuarios no tuvieron ningún tipo de problema, esto implica que una vez ya tenido su usuario y contraseña se vuelve más fácil y seguro el acceso a la red.
- Las preguntas 17, 18 y 19 están relacionadas con la administración de los dispositivos móviles. La pregunta 17 trata cerca del envió de notificaciones a los distintos dispositivos móviles y se tiene que para un 65.78% fue satisfactorio. La pregunta 18 implica cuan satisfactorio fue la localización de dispositivos y se tiene un nivel del de satisfacción del 67.10%. Y finalmente la pregunta 19 preguntó si él envió de app a los distintos dispositivos fue exitoso, hallando que un 78.94% lo lograron.
- Las preguntas 10, 11, 12, 13 15 y 20 están relacionadas con la administración de la red, teniendo en la pregunta 10 los distintos anchos de banda para cada una de las redes inalámbricas creadas. En la pregunta 11 se preguntó si se tenía una percepción de la velocidad de navegación con el 77.63% los usuarios respondieron que fue rápida. La pregunta 12 muestra cuán rápido se cargaba una página solo de texto, el 75% de los usuarios respondieron que lo percibieron rápido. La pregunta 13 se relacionó con la reproducción de video

hallando que 67.10% logro reproducirlo. La pregunta 15 averiguó sobre una muestra de 48 usuarios sobre las descargas donde el 58.33% de los usuarios tenían una descarga rápida y el 41.66% su descarga fue lenta. Cabe destacar que los 28 usuarios restantes no tenían permisos para realizar descargas. Y finalmente la pregunta 20 que indaga el funcionamiento de las aplicaciones en tiempo real expone que un 75% fue bueno.

- La pregunta 22 inquiere si se recomendaría la implementación de BYOD en la Universidad evidenciando un 84.21% de aceptación para llevar a cabo esta implementación.
- Finalmente la pregunta 23 recoge algunas recomendaciones que hacen los usuarios a la red, lo cual no es cuantificado, pero si se lo resumido de manera general en la tabla 46.

5.2 Análisis de factibilidad técnica

En la factibilidad técnica estuvo destinado a recolectar información sobre los equipos tecnológicos que posee la organización y la posibilidad de hacer uso de los mismos en el desarrollo y la dable implementación de BYOD y de ser necesario, los requerimientos tecnológicos que deben ser adquiridos. La tabla 39 muestra toda esa información.

Tabla 39.
Hardware y software.

Hardware	Software	Observaciones
IBM X3650M3	----------	Satisface los requerimientos de la propuesta, en la parte de hardware y en la parte de software puede ser actualizado a un sistema operativo más actual o trabajar con el mismo.
ISE 3415	1.2	Cumple con las características mostradas en el capítulo 4.
WLC 5508	7.5	Cumple con las características mostradas en el capítulo 4.
ASA 5515-X	9.1.1	Cumple con las características mostradas en el capítulo 4.
Switch 6506-E	15.1	Cumple con las características mostradas en el capítulo 4.
Switch 3750G	12.2(25)SEE2	Algunos equipos poseen la UPS y otros hay que adquirirlos.
Switch 2960S	12.2(50)SE5	Cumple con las características mostradas en el capítulo 4.
AP 3702P	7.6	Cumple con las características mostradas en el capítulo 4.

Nota. Hardware y software para el diseño de la red.
Elaborado por: Andrea Díaz y Danilo Lamar.

La tabla 40 muestra el cableado de red que tiene la universidad y si esta cumple con los lineamientos del diseño.

Tabla 40.
Cableado de red.

Cableado	Par trenzado / Fibra óptica	Observaciones
Vertical	Multimodo 62.5 / 125 um	Se conservaría el actual sistema de cableado, este cumple con las características del diseño.
Horizontal	Categoría 6 A / 7A	Se conservaría el actual sistema de cableado, ya que cumple con las características del diseño.

Nota. Cableado de red y sus observaciones.
Elaborado por: Andrea Díaz y Danilo Lamar.

La tabla 41 muestra la experiencia técnica que tiene el personal de TI de la institución en manejar la infraestructura de red.

Tabla 41.
Experiencia técnica.

Personal de TI	Observaciones
Director de TI Sede Quito	Ing. Juan Carlo Domínguez, trabaja en la universidad desde 2005, posee certificaciones en Cisco CCNA, CCNP, CCDA, SWSA, SASAA y administración de equipos Blue Coat.
Responsable de infraestructura	Ing. Diego Soria, trabaja en la universidad desde 2010, posee certificaciones en virtualización de servidores en Windows y Linux, certificados de CCNA.
Asistente de redes de sede	Ing. Milton Ruiz, trabaja en la universidad desde 2011, posee certificaciones relacionadas con infraestructura de tecnología como cableado estructurado, fibra óptica, certificados Cisco.
Técnico de soporte de campus	Alejandro Moreno Encargado de la parte técnica de TI de la institución, trabaja en la universidad desde 2013, posee certificados de CCNA.

Nota. Experiencia por parte del personal de TI de la universidad.
Elaborado por: Andrea Díaz y Danilo Lamar.

Es viable implementar una infraestructura de red para BYOD sobre la red inalámbrica de la UPS, ya que la misma actualmente consta con una infraestructura funcional, en la cual se pueden agregar equipos nuevos, los cuales estarían involucrados en el desarrollo y puesta en funcionamiento del proyecto, además que el personal de TI tiene las capacidades para operar y mantener el sistema propuesto.

5.3 Análisis de costos.

Este análisis de costos se basa en dar un valor aproximado de cuanto le va a costar la posible implementación para BYOD a la institución, cabe mencionar que este estudio no tiene fines de lucro, sino el mejoramiento del servicio a toda la comunidad salesiana. A continuación se muestra los costos de la propuesta.

- **Costos de equipos.**

En la tabla 42 se muestran los costos referenciales del equipamiento cuyos valores fueron obtenidos de cotizaciones de proveedores de equipamiento Cisco.

Tabla 42.
Detalle del costo de equipos de la propuesta de diseño.

Ítem	Descripción	Cantidad	Valor unitario	Valor total
1	Switch Catalyst 3750G 48 Puertos 4 Puertos SFP WS-C3750G-48TS-E.	6	$ 8,512.45	$ 51,074.70
2	Wireless LAN Controller 5508 AIR-CT5508-50-K9.	1	$ 19,039.21	$ 19,039.21
3	Access Point 3700 AIR-CAP3702I-A-K9.	19	$ 1,265.33	$ 24,041.28
4	ASA 5515-X 6 puertos SFP ASA5515-2SSD120-K9, ASA-IC-6GE-SFP-C.	1	$ 10,355.53	$ 10,355.53
5	Cisco ISE SNS-3415-K9 CON-SNT-SNS3415.	1	$ 10,148.04	$ 10,148.04
			Total	$ 114,658.76

Nota. Detalle del costo de los equipos.
Elaborado por: Andrea Díaz y Danilo Lamar.

- **Costo de licenciamiento y garantía.**

En la tabla 43 se muestran los costos referenciales de licenciamiento, está dado para cinco años y las garantías están para doce meses.

Tabla 43.
Costo de licencias y garantías.

Ítem	Descripción	Cantidad	Valor
1	Switch: WS-C3750G-48TS-E, garantía SMARTNET 8X5XNBD.	6	$ 5,336.70
2	WLC: AIR-CT5508-50-K9, garantía SMARTNET 8X5XNBD.	1	$ 3,769.23

3	AP: AIR-CAP3702I-A-K9, garantía SMARTNET 8X5XNBD.	19	$ 1,469.54
4	ASA: ASA5515-2SSD120-K9, garantía SMARTNET 8X5XNBD, licencia ASA 5515-X AVCWSE IPS 5 Year.	1	$ 12,778.02
5	ISE: licencias L-ISE-BSE-1k, L-ISE-ADV-S-1k, ISE-ADV-5YR-1k y garantía SMARTNET 8X5XNBD.	1	$ 38,030.52
		Total	$ 61,384.01

Nota. Costos de licencias y garantías.
Elaborado por: Andrea Díaz y Danilo Lamar.

- **Costo de instalación y configuración.**

La tabla 44 muestra los costos de configuraciones e instalación de los equipos.

Tabla 44.
Detalle del costo de instalación y configuración.

Descripción	Valor
25% del valor total de equipos, licenciamiento y garantías.	$ 45,933.35

Nota. Costo de instalación y configuración de los equipos.
Elaborado por: Andrea Díaz y Danilo Lamar.

- **Costo total.**

El costo final del proyecto que representaría para la universidad implementar una infraestructura de red para BYOD, se muestra a continuación.

Tabla 45.
Detalle del costo total del proyecto.

Descripción	Valor
Costos de equipos	$ 114,658.76
Costos de licenciamiento y garantías.	$ 61,384.01
Costo de instalación y configuraciones.	$ 45,933.35
Costos por insumos extras	$ 7,690.67
Subtotal	$ 229,666.76
IVA (12%)	$ 27,560.01
TOTAL	$ 257,226,77

Nota. Costo total del diseño de red.
Elaborado por: Andrea Díaz y Danilo Lamar.

Este análisis de costo se basó solo en los equipos que le hacen falta a la universidad para poder tener BYOD, a continuación se muestra en la tabla 46 los valores totales si se tuviera que invertir en la compra si no existieran equipos de red.

Tabla 46.
Costo total de equipos de red nuevos.

Descripción	Valor
Equipos y licencias.	$ 539,857.75
Instalación y configuración.	$ 134.964.44
Subtotal	$ 674.822.19
IVA (12%)	$ 80,978.66
Total	$ 755,800.85

Nota. La siguiente tabla muestra el costo de equipos nuevos si la universidad no tuviera equipamiento. Elaborado por: Andrea Díaz y Danilo Lamar.

Como se puede observar si se tuviera que cambiar toda la infraestructura de red y poner nueva se tendría que invertir una suma superior, en comparación a solo comprar el equipamiento faltante con el cual solo se invertiría un 34.03% para cumplir con la propuesta de red y reutilizando los equipos que tiene en la actualidad la universidad. El anexo treinta y treinta uno muestran los costos de la cotización.

5.4 Aspectos esenciales del impacto de la propuesta.

Para los aspectos esenciales de la propuesta se tomaron en cuenta los beneficios que pueden traer la posible implementación de BYOD en la institución. Por tal motivo se clasificaron en:

Beneficios Tangibles: los benéficos tangibles aportados por el proyecto propuesto son:

- Facilidad de escalabilidad y administración para la red inalámbrica.
- Mayor confidencialidad y autenticación para la red inalámbrica debido al uso del protocolo IEEE 802.11X.
- Los datos que recolecten el ISE y el RADIUS sobre los clientes y la carga que generen, permitirán tomar de decisiones a nivel administrativo para mantener o mejorar el servicio de red inalámbrica en la Universidad.

- Con BYOD aumenta la capacidad de control y seguimiento de todos los actores (dispositivos y equipos) que usan la red inalámbrica.
- La disminución en los costos y en el tiempo se puede dar con BYOD al escalarlo de la red inalámbrica a la red alámbrica.

Beneficios Intangibles: entre los beneficios intangibles del proyecto propuesto se pueden incluir:

- Mejor servicio en la parte de la red inalámbrica para los docentes, administrativos y estudiantes debido a la creación de perfiles, por lo que se consigue identificación de los dispositivos y un mejor uso de los recursos provistos por la red.
- Realzar la imagen de la Universidad Politécnica Salesiana Campus Sur al ser pionera fomentando los cambios tecnológicos al implementar una tendencia global como lo es BYOD.

CONCLUSIONES

- Se levantó la información de la red inalámbrica de la UPS encontrándose que: los switch 6506-E, switch 3750G, switch 2960S y el servidor X3650M3 pueden ser utilizados para la implantación de BYOD.
- Para mejorar el servicio de la red al implementar la red piloto con BYOD se generaron políticas sobre cada uno de los dispositivos entre las cuales estaba: calidad de servicio, restricciones al acceso a páginas web, limitar el ancho de banda, seguridad sobre los dispositivos.
- Para cumplir BYOD en la red inalámbrica de la UPS es necesario incrementar políticas sobre cada grupo de usuarios que tienen acceso a la red además de adquirir infraestructura como switch, acces point, ISE, ASA y WLC de forma que los administradores del departamento de Tecnologías de la información puedan administrar la red.
- La propuesta de BYOD con Cisco requiere que toda la infraestructura de red este basada en esta marca, además hubo otros factores para determinar la utilización de estos equipos como son: la reutilización de equipo actual para la reducción de costos, la mejor integración de los equipos y el manejo de estos equipos por parte del departamento de TI de la Universidad. Si se requiere crecer a nivel de licenciamiento estas se las puede obtener a través de Cisco.
- La red piloto se diseñó con equipos de Cisco Meraki debido a que los costos ofrece una solución viable para la red piloto. La solución de Cisco Meraki brinda la facilidad de gestionar diferentes tipos de políticas basados en seguridad, control del acceso, QoS, perfiles y revisión de posturas de los dispositivos, etc.
- Mediante el análisis de costos se pudo determinar que el proyecto es viable puesto que la universidad cuenta con equipos que pueden ser utilizados para BYOD por lo que la inversión que la universidad debería realizar para implementar BYOD seria de un 34.03%, en vez de una inversión del 100% si no tuviera equipos de red.
- Se determinó una aceptación de la red piloto en orden del 95% por parte de los usuarios que la utilizaron.

- La granularidad que se presentó con la red piloto al saber cómo estaban los distintos dispositivos de los usuarios, es un beneficio que presenta BYOD para el departamento de TI ya que con esto se pueden determinar afinar las políticas implantadas sobre la red.
- Con la red piloto en el browser se observó en un 100% cómo estaban todos los dispositivos de los usuarios, conociendo así la postura de los dispositivo, para enviarlo o no, al sitio de remediación.
- Del análisis de los resultados obtenidos de las pruebas realizadas a la red piloto de BYOD a una población de 76 estudiantes de la UPS campus SUR el 84,21% de los estudiantes se conectó a la red desde un dispositivo que en su mayoría eran Smartphone y el 15,79% lo hace con dos o tres dispositivos, en un 71,05% el enrolamiento a la red fue rápido, la aplicación de políticas se cumplieron en un 59.21% para Smartphone, 19,73% para tablet y 21,05% para laptops. En relación a políticas el 56,57% de los usuarios no notaron los cambios de las políticas aplicadas mientras que el 43,43% si notaron los cambios. En la seguridad de la red el 96,05% no tuvo ningún inconveniente, solamente el 19,73% fue enviado a remediación. Se obtuvo un 70,6% de éxito en la administración de los dispositivos con envío de notificaciones, localización de dispositivos y envío de app. También según lo indicado por los usuarios hubo un 84,21% de aceptación del proyecto para ser implementado en la Universidad.
- Con BYOD se puede tener entornos virtuales en los cuales puede existir colaboración a nivel de la comunidad Salesiana, debido a esto se tendría que migrar, o a una infraestructura para virtualización, o algún tipo de solución en nube. Todo esto dependerá del enfoque que la Universidad le dé a la solución de BYOD propuesta.

RECOMENDACIONES

- Se exhorta a usar BYOD por la granularidad que ofrece ya que se puede generar políticas para un mayor control de la red.
- Para tener un mayor control de los dispositivos móviles, se recomienda luego de la implementación de la propuesta y viendo las necesidades de usuarios tener un administrador de dispositivos móviles (MDM), en este caso ISE soporta la adición de terceras compañías para este entorno, se pude utilizar el MDM de Cisco Meraki, ya que como se pudo observar en la red piloto ofrece muchas características y opciones para los distintos dispositivos móviles, además al ser de Cisco se tiene una garantía en el correcto funcionamiento de este entorno ISE-MDM de esta forma se tendrá un entorno BYOD con más seguridad tanto para la red como para los usuarios.
- Se pone a consideración generar una infraestructura de virtualización de escritorios y aplicaciones para tener un mismo ambiente de trabajo en la universidad de esta forma los recursos serán compatibles y seguros con el dispositivo del usuario.
- Para tener un BYOD de acceso unificado, se recomienda aplicar esta infraestructura a nivel alámbrico, para esto se debe acceder a la compra de nuevos equipos de red.
- Se encomienda implementar soluciones de colaboración (mensajería, video, etc.), las cuales podrán mejorar la experiencia de todos los usuarios en la red.
- Se incita a llevar una estadística de acceso a los recursos de red, para poder implantar políticas convenientes sobre los dispositivos de los usuarios.

LISTA DE REFERENCIA

Anderson, N. (29 de Agosto de 2013). *Cisco.* Obtenido de http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html

Arbor networks. (2012). Obtenido de http://www.cioandleader.com/digital_assets/66/DDosmitigationinBYODarchitecture.pdf

Aruba. (s.f.). Obtenido de http://www.arubanetworks.com/pdf/technology/whitepapers/WP_BYOD.pdf

Aruba Networks. (2012). *Aruba Networks, Inc*. Obtenido de http://www.arubanetworks.com/pdf/technology/whitepapers/WP_BYOD_ES.pdf

Avaya. (s.f.). Obtenido de http://www.syndeticom.com/~syndetic/docs/BYOD/BYODReadinessSolutionChecklist.pdf

barners, P. (29 de Enero de 2013). *CircleID*. Obtenido de http://www.circleid.com/posts/20130129_reducing_risks_of_byod_with_dns_based_security_intelligence_part_2/

Cisco. (s.f.). Obtenido de http://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-692412.pdf

Cisco . (15 de Junio de 2014). Obtenido de http://www.cisco.com/web/about/ac79/techtopics/BYOD.html#~us

Cisco. (2010). *Cisco.* Obtenido de http://www.cisco.com/web/strategy/docs/gov/collab_workspace.pdf

Cisco. (Marzo de 2011). *Word Press*. Obtenido de http://albinogoncalves.wordpress.com/:

http://albinogoncalves.files.wordpress.com/2011/03/ciscoc2ae-smart-business-architecture-sba-borderless-networks-para-organizaciones.pdf

Cisco. (28 de Abril de 2014). *Cisco.com*. Obtenido de Cisco.com: http://www.cisco.com/c/en/us/products/switches/catalyst-6500-series-switches/datasheet-listing.html

Cisco Bring Your Own Device (BYOD) CVD. (27 de Septiembre de 2013). *Cisco* . Obtenido de http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.html

Cisco Meraki. (30 de Enero de 2015). *Cisco Meraki*. Obtenido de Cisco Meraki: https://meraki.cisco.com/trust

Cisco System . (2014). *Cisco Meraki*. Obtenido de https://meraki.cisco.com/solutions/byod

Cisco Systems. (10 de Enero de 2014). Obtenido de http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD_Horizons-Global_ES.pdf

Cisco Systems. (3 de Junio de 2014). *Cisco.* Obtenido de Cisco: http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/compatibility/ise_sdt.pdf

Cisco Systems, Inc. (2012). *Cisco Systems, Inc*. Obtenido de http://www.cisco.com/web/ES/pdf/Beyond_BYOD_to_the_Optimal_Experience_for_Any_Workspace_Solution_Overview.pdf

Citrix. (s.f.). Obtenido de https://lac.citrix.com/solutions/bring-your-own-device/features.html

Citrix. (2013). *Citrix.* Obtenido de http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/guidelines-for-deploying-citrix-byod-solutions.pdf

Creative Commons. (2007). *Redes Inalambricas en los Países en Desarrollo.* Suecia: Booksprint.

Departamento TI UPS. (2013). *Análisis de la infraestructura de red de datos de la Universidad Politécnica Salesiana Sede Quito.* Quito.

Diego, M., & Jonathan, J. (2013). *Análisis, diseño y propuesta de implementacion de un portal cautivo para la red inalámbrica de la Universidad Politécnica Salesiana sede Quito Campus Sur.* quito.

Domínguez, J. C. (29 de Abril de 2014). Información sobre la red e la UPS. (A. Díaz, & D. Lamar, Entrevistadores)

Dynacom. (2015). *Dynacom*.

Galeon. (12 de Marzo de 2014). Obtenido de http://ieeestandards.galeon.com/aficiones1573579.html

Geier, J. (2008). *Implementing 802.1X Security Solutions for Wired and Wireless Networks.* Indianapolis: Wiley Publishing, Inc.

HP. (s.f.). Obtenido de http://h17007.www1.hp.com/us/en/networking/solutions/technology/byod/portfolio.aspx#uwwn

HP. (febrero de 2013). *HP*. Obtenido de HP Press Kit: http://www.hp.com/hpinfo/newsroom/press_kits/2013/GPC2013/IMC_BYOD_Appliance_Whitepaper.pdf

HP Networking. (2013). *Hubtechnical.* Obtenido de Hubtechnical: http://www.hubtechnical.com/Collateral/Documents/English-US/CenterForDigitalEduation_Simplifying_BYOD_in_Education_Brief.pdf

IBM. (s.f.). *IBM*. Obtenido de IBM: http://www-03.ibm.com/systems/hardware/browse/amdpro/index.html

Isaacson, N. (2013). Obtenido de http://ilta.ebiz.uapps.net/productfiles/productfiles/1501877/SOSPG2.pdf

Kaminski, K. (2013). *DHSES.* Obtenido de http://www.dhses.ny.gov/ocs/awareness-training-events/conference/2013/documents/presentations/Ken-Kaminski.pdf

Kaspersky. (2013). *Kaspersky Lab*. Obtenido de http://www.kaspersky.com/business-security/securing-mobile-endpoints

Kinnear, K. (18 de Mayo de 2014). *Ciscolive2014*. Obtenido de https://www.ciscolive2014.com/connect/sessionDetail.ww?SESSION_ID=3153

Lehembre, G. (2006). *Hervé Schauer Consultants.* Obtenido de http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

Lewis, B., & Davis, P. T. (2004). *Wireless Networks for Dummies.* Hoboken: Wiley Publishing, Inc.

Luna, J. S., & Martín, J. F. (2013). La gestión segura de la información en movilidad ante el fenómeno BYOD:¿Bring Your Own Device = Bring Your Own Disaster? *Revista SiC*, 65-73.

Martínez, J. (29 de Noviembre de 2012). *Hp Networking*. Obtenido de Hp Networking: http://h30499.www3.hp.com/t5/Infraestructura-Convergente-de/Ventajas-para-las-empresas-al-integrar-sus-redes-WiFi-y/ba-p/5871567#.UymcsfmSzX5

Microsoft. (2008). Obtenido de http://download.microsoft.com/download/6/F/8/6F8EF4EA-26BD-48EA-BF45-BFF00A3B5990/Microsoft%20Client%20Virtualization%20Strategy%20White%20Paper_final.pdf

Microsoft. (2014). *Windows*. Obtenido de http://www.microsoft.com/es-es/windows/enterprise/products-and-technologies/virtualization/operating-system/default.aspx

Stallings, W. (2005). *Wireless Communications and Networks.* New Jersey: Pearson Prentice Hall.

Sullivan, D. (2012). Tabletas y Smartphones en las empresas: riesgos y preocupaciones de gestión. *TechTarget*, 16.

Telcommunity. (12 de Marzo de 2014). Obtenido de http://www.telcommunity.com/wp-content/uploads/pdf/redes_wireless.pdf

Tortosa, C. C. (2005). *Universidad de Valencia* . Obtenido de http://www.uv.es/~montanan/redes/trabajos/SeguridadWLANs.pdf

TRC. (3 de Abril de 2014). *TRC*. Obtenido de http://www.trc.es/documentacion/integracion/TRC_BYOD.pdf

Universidad Iberoamericana. (9 de Marzo de 2014). Obtenido de Universidad Iberoamericana Ciudad de México: http://www.ie.uia.mx/tit/ot03/proy14/vpninal.htm

Virtualización. (24 de Noviembre de 2013). *Virtualización*. Obtenido de Virtualización: http://www.virtualizacion.com/como-se-encuentra-actualmente-la-virtualizacion/

Woland, A. T., & Heary, J. (2013). *Cisco ISE for BYOD and Secure Unified Access.* Indianapolis: Cisco Press.

ANEXOS

Anexo 1. Características del equipo Cisco 3415 (Identity Services Engine ISE).

Cisco Secure Network Server (SNS)	Modelo: SNS-3415-K9
Ranura	1 tarjeta PCIE contiene puertos Ethernet de 1 GB(GigE2 y GigE3).
Puertos Ethernet	1 GB 3 (GigE2), 1 GB 4 (GigE3).
Puertos	1-GB Ethernet 2 (GigE1), USB 2.0.
Procesador	2,4 Ghz, Intel E5-2609 de 4 núcleos.
Memoria RAM	16 GB.
Disco	1 x 600 GB.
Interfaces de red	4 GE.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Anexo 2. Características del equipo Cisco 5508 (Wireless LAN Controller WLC).

Cisco Wireless LAN Controller 5508	Modelo: AIR-CT5508-25-K9
Cantidad de puertos	8 Puertos.
Protocolo de interconexión de datos	Gigabit Ethernet.
Protocolo de conmutación	Ethernet.
Red/Protocolo de transporte	TCP/IP, UDP/IP, ICMP/IP, ARP, FTP, BOOTP, DHCP.
Protocolo de gestión remota	SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH.
Capacidad	25 Puntos de acceso administrables.
Características	Soporta DHCP, BOOTP, ARP, VLAN, Filtro de direcciones MAC.
Algoritmo de cifrado	LEAP, DES, Triple DES, RC4, MD5, AES, 128-bit WEP, 40-bit WEP, IKE, SSL, TLS, SHA-1, TLS 1.0, 104-bit WEP. WPA, WPA2, WPA-PSK, AES-CBC.
Método de Autenticación	RADIUS, TACACS, Extensible Authentication Protocol (EAP).
Cumplimiento de Estándares	IEEE 802.3, IEEE 802.3U, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1X.
Ranuras de expansión	1(1) X Ranura de expansión, 8 (8) x SFP (mini-GNIC).
Interfaces	1 x administración, consola, RJ-45, Ethernet 10 Base-T/100 base-TX/1000 Base-T, RJ-45 1x USB, consola, 4 pin mini-USB Tipo B, 2 x USB, 4 pin USB Tipo A.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Anexo 3. Características del equipo Cisco 5515-X (Adaptive Security Appliance ASA).

Cisco ASA 5515-X	Modelo: ASA5515-SSD120-K9
Capacidad de procesamiento con inspección de paquetes e información de estado	1.2 Gbps.
Capacidad de procesamiento con inspección de paquetes e información de estado (multiprotocolo)	600 Mbps.
ASA rendimiento IPS	400 Mbps.
Capacidad de procesamiento de última generación	350 Mbps.
Triple Data Encryption Standard / Advanced Encryption Standard (3DES/AES) Capacidad de la VPN	250 Mbps.
Usuarios/nodos	Ilimitado.
IPsec VPN	250
Usuarios de Cisco Cloud Web Security	250
Sesiones simultaneas	250,000
Interfaces Virtuales (VLANs)	100
E/S integrada	6 puertos GE.
E/S de ampliación	6 puertos GE o de 6 puertos SFP.
Puertos USB 2.0	2
Puerto serial	1 RJ-45 consola
Memoria	8 GB
Flash mínimo de sistema	8 GB

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Anexo 4. Características del equipo IBM SYSTEM X3650 M3.

IBM SYSTEM X3650 M3	
Procesador	6 Core Xeon
Memoria	8 GB.
Disco duro	8 TB.
Memoria de video	16 MB.
Chipset	Intel 5520.
Puertos	5 USB, 1 serial, y 2 Gigabit Ethernet.

Nota. (IBM).
Elaborado por: Andrea Díaz y Danilo Lamar.

Anexo 5. Características del equipo Cisco Catalyst 6506-E Series Switch.

Cisco Catalyst 6506-E	Modelo: WS-C6506-E
Información de la densidad de puertos, módulos e interfaces WAN	
Numero de Slot	6
10 Gigabit Ethernet (XENPAK)	20
Gigabit Ethernet (SFP)	242
Gigabit Ethernet (Convertidor Interface gigabit[GBIC])	82
10/100/1000 Ethernet	241
10/100 Fast Ethernet	480
100BASE-FX	240
FlexWAN (DS-0 a OC-3)	2 Módulos con 4 puertos adaptables
Puertos OC-3 POS	40
Puertos OC-12 POS	20
Puertos OC-12 ATM	10
OC-48 POS/Puertos de transporte de paquetes dinámico (DPT)	10 POS, 5 DPT
Digital E1/T1 Puertos Troncales	90
Interfaces FXS	360

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Anexo 6. Características del equipo Cisco Catalyst 3750G Series Switch.

Cisco Catalyst 3750G	Modelo: WS-C3750G-48PS-E
10/100/1000 Ethernet	48 puertos con PoE.
Gigabit Ethernet (SFP)	4 puertos.
Velocidad de apilamiento	32 Gbps.
Memoria DRAM	128 MB.
Memoria flash	32 MB.
Tecnología innovadora	Apilamiento (StackWise).
Enrutamiento	IPv6 dinámico.
Características de servicio	IPS, multicapas, QoS.
Soporta	200 Puntos de acceso.
Interfaz de administración	1 Puerto RJ-45.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Anexo 7. Características del equipo Cisco Catalyst 2960S Series Switch.

Cisco Catalyst 2960S	Modelo: WS-C2960S-48PST-L
10/100/1000 Ethernet	48 puertos con PoE.
Gigabit Ethernet (SFP)	4 puertos.
Velocidad de apilamiento	32 Gbps.
Memoria DRAM	64 MB.
Memoria flash	32 MB.
Tecnología innovadora	Apilamiento (StackWise).
Versión del software	12.2 (25).
Tasa de transferencia	0.1 Gbps.
Estándar	IEEE 802.3.
Interfaz de administración	1 Puerto RJ-45.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Anexo 8. Características del equipo Cisco Access Point 3702P.

Cisco Aironet 3702P	Modelo: AIR-CAP3702P-x-K9
Protocolo de interconexión de datos	IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac.
Transferencia de datos	1.3 Gbps
Características	PoE, Auto-sensor por dispositivo, Soporte Wi-Fi multimedia (WMM), tecnología.
Bandas de frecuencia	2.4Ghz, 5Ghz
Algoritmo de cifrado	AES, TLS, PEAP, TTLS, TKIP, WPA, WPA2
Método de autenticación	MS-CHAP v.2, Extensible Authentication Protocol (EAP), EAP-FAST.
Antena	Interna integrada.
Directividad	Omnidireccional.
Interfaces	1 x 1000Base-T - RJ-45; 1 x management - RJ-45; 4 x antenna.

Nota. (Cisco).
Elaborado por: Andrea Díaz y Danilo Lamar.

Anexo 9. Encuesta 1 Conexión a la red inalámbrica de la UPS.

Tema: Conexión a la red inalámbrica de la UPS

Marque con una X la respuesta correcta según su criterio

Preguntas:

1. Con cuantos dispositivos usted se conecta a la red inalámbrica de la Universidad

   1 dispositivo ☐ 2 dispositivos ☐ 3 dispositivos ☐

2. Qué tipo de dispositivo/s utiliza usted para conectarse

   Smartphone ☐ Tablet ☐ Laptop ☐

3. Cuál es el sistema operativo de su/sus dispositivo/s

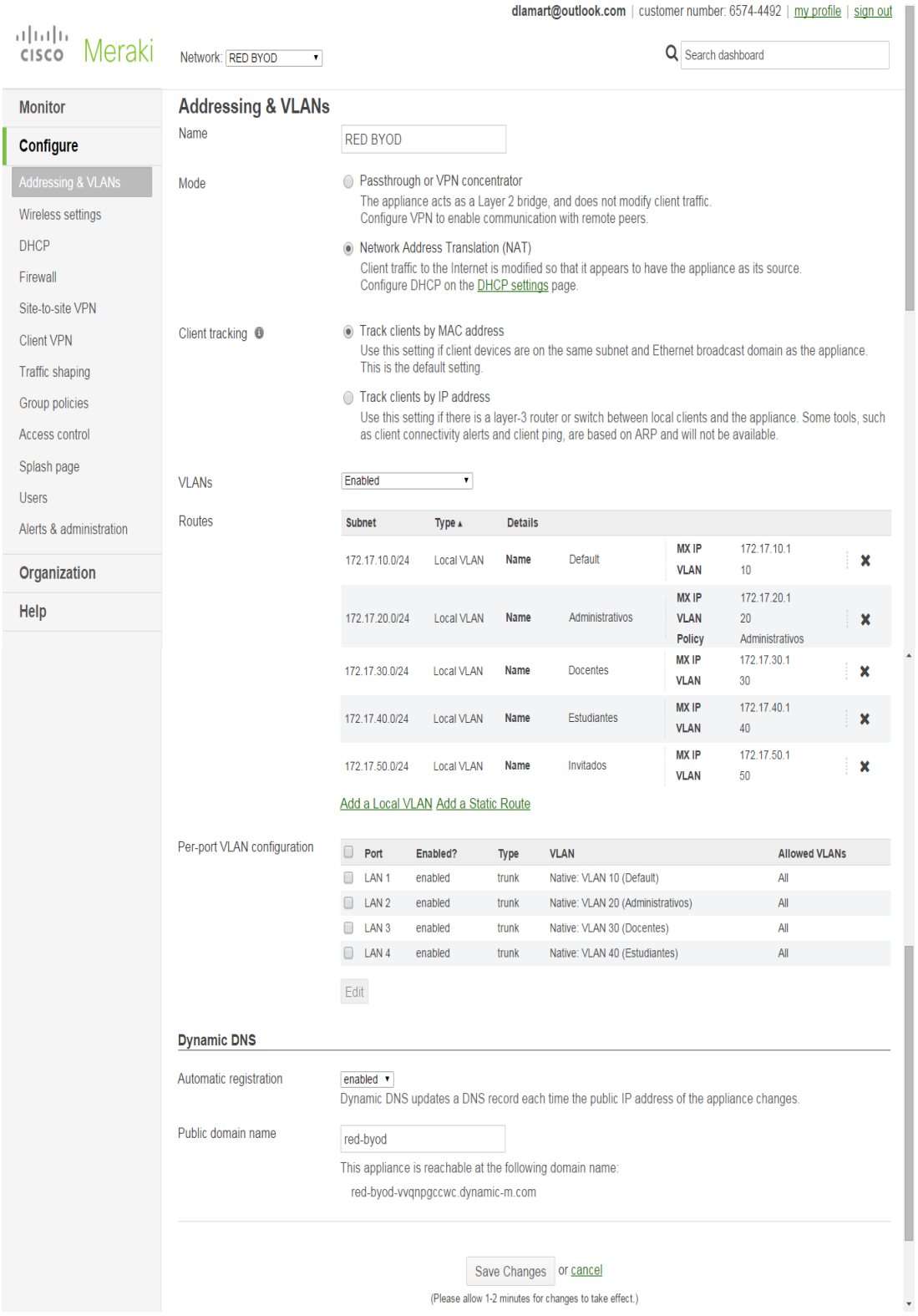
   Android ☐ iOS ☐ Windows ☐

4. Por cuánto tiempo aproximadamente se conecta usted a la red inalámbrica de la Universidad

   1 hora ☐ 2 – 3 horas ☐ 4 o más horas ☐

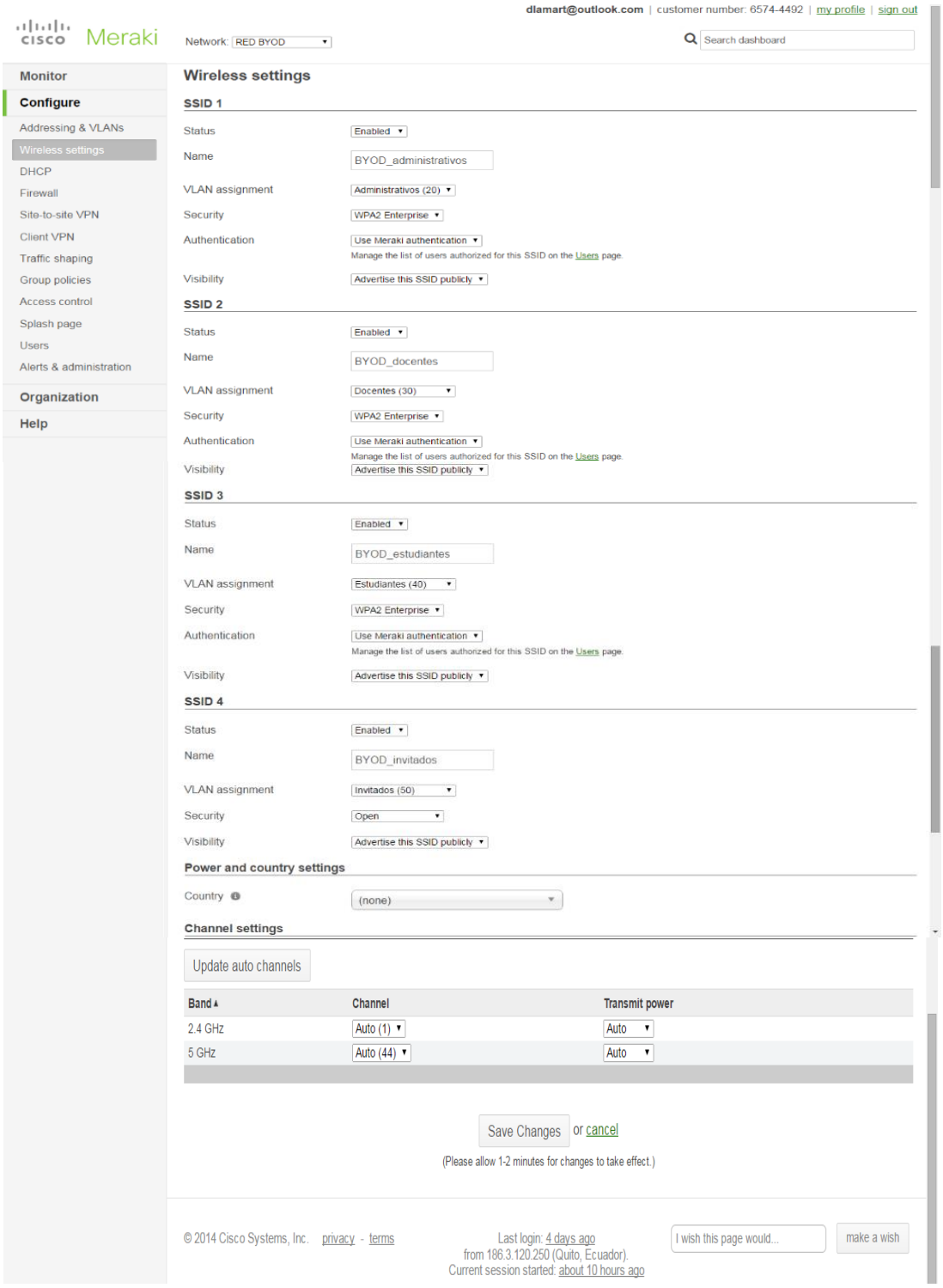
Anexo 10. Direccionamiento y VLAN.

En esta sección se habilitó la creación de las VLAN, con su respectivo nombre, direccionamiento, su identificador de VLAN, la política y la asignación de cada puerto LAN a una VLAN específica cómo se puede observar.



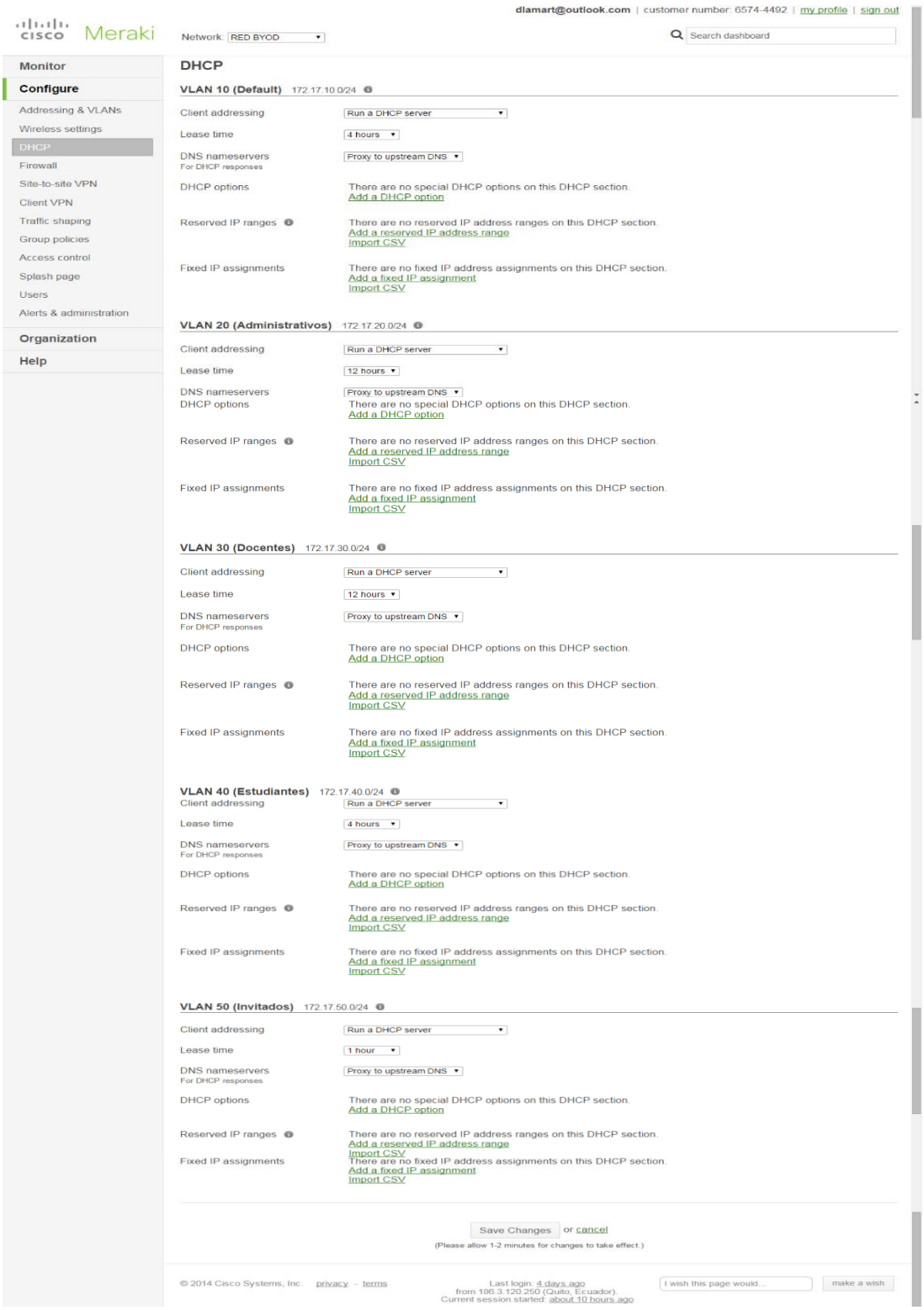
Anexo 11. Opciones Inalámbricas.

Las configuraciones realizadas en esta sección se basan en los siguientes parámetros: nombre, asignamiento de la VLAN, tipo de seguridad en la red inalámbrica, el tipo de autenticación para esta red y la pauta de visibilidad de la red para los usuarios, todo esto se configuró para cada una de la redes inalámbricas y se muestra en la siguiente imagen.



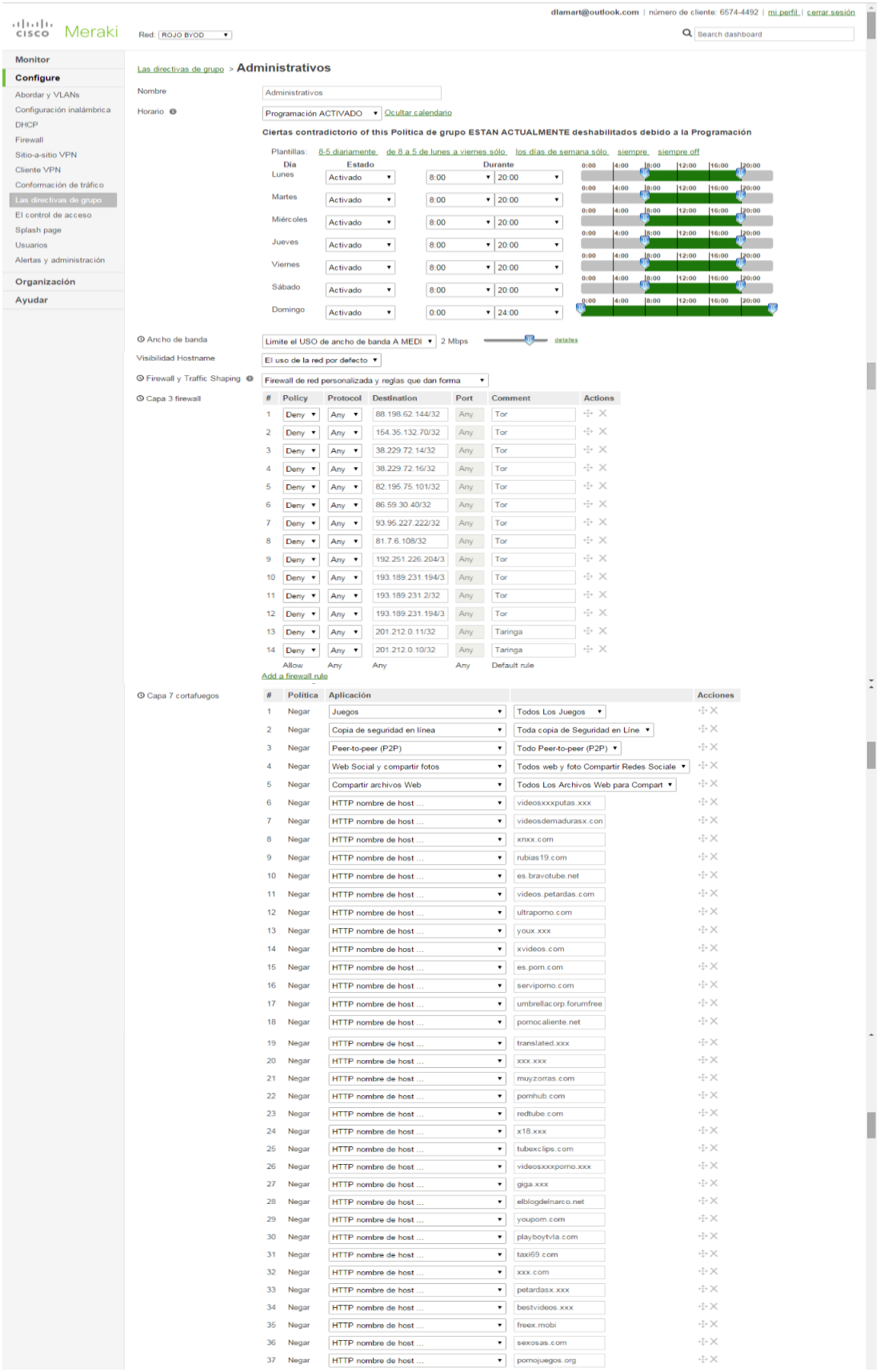
Anexo 12. DHCP.

Para el servicio de DHCP las configuraciones realizadas son las siguientes: se ejecutó el servicio de DHCP y el servicio DNS, se asignó el tiempo de arrendamiento de la IP y además se habilitaron algunas opciones adicionales que puede tener este servicio.

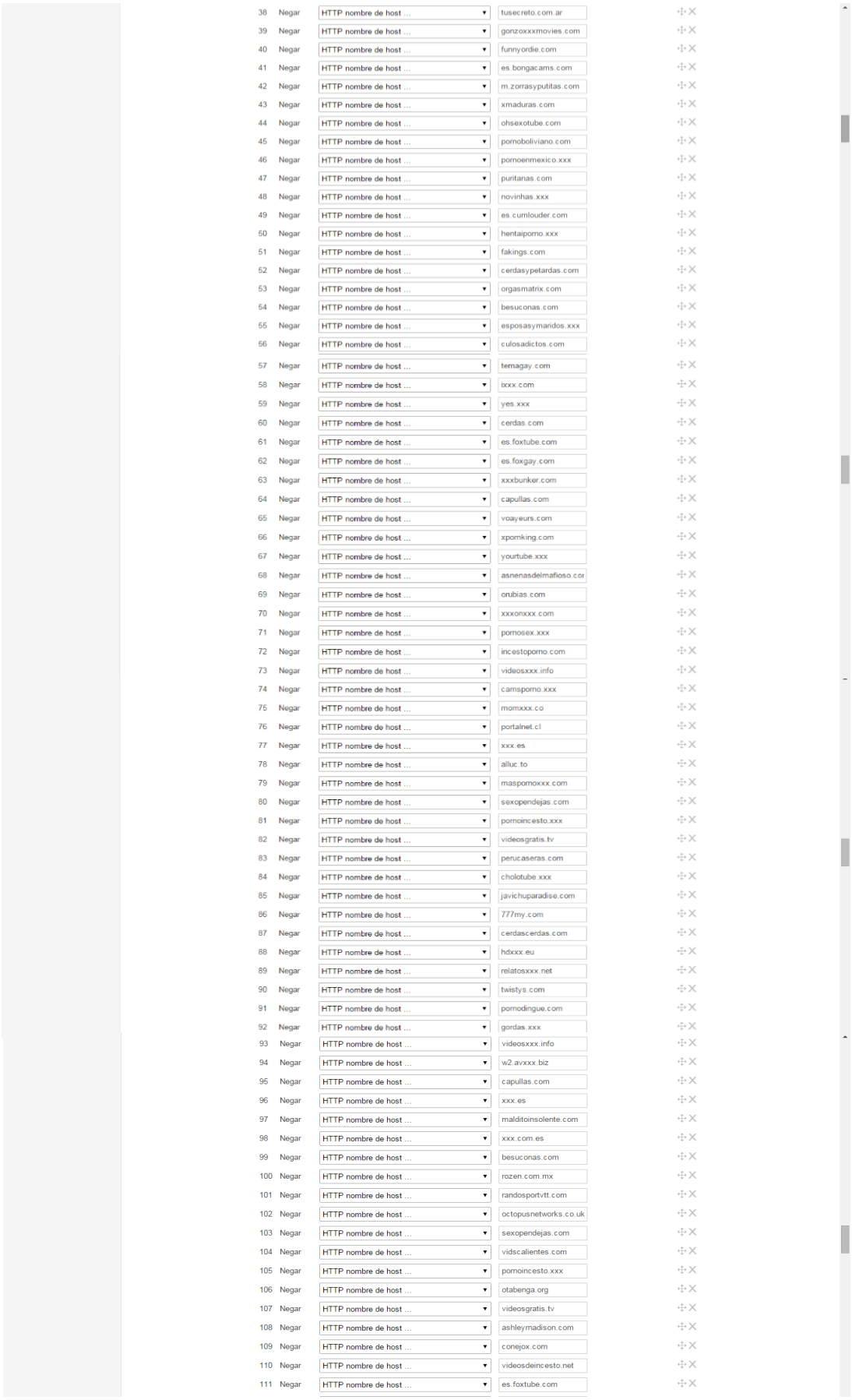


Anexo 13. Política Administrativos.

Parte uno.

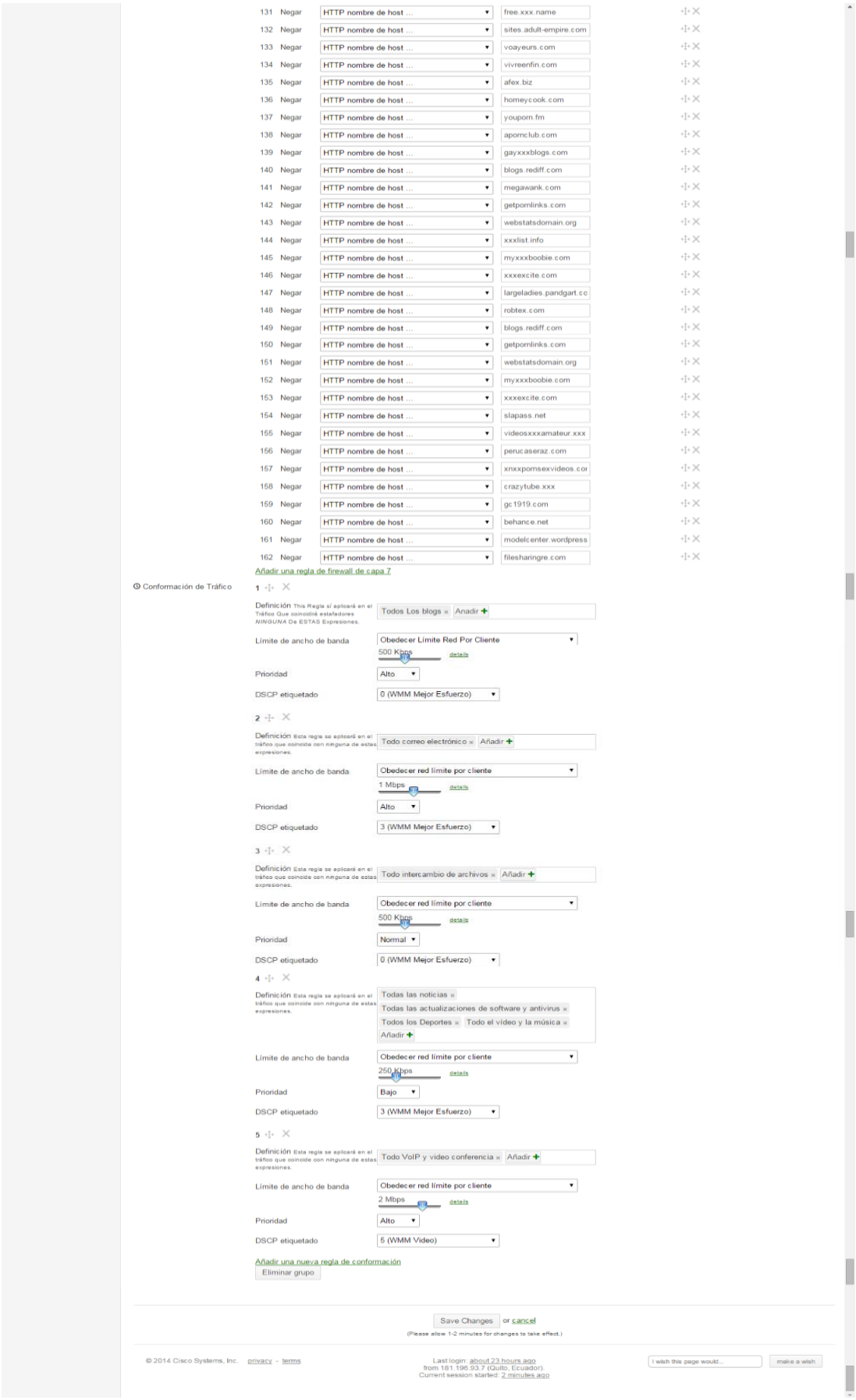


Parte dos.



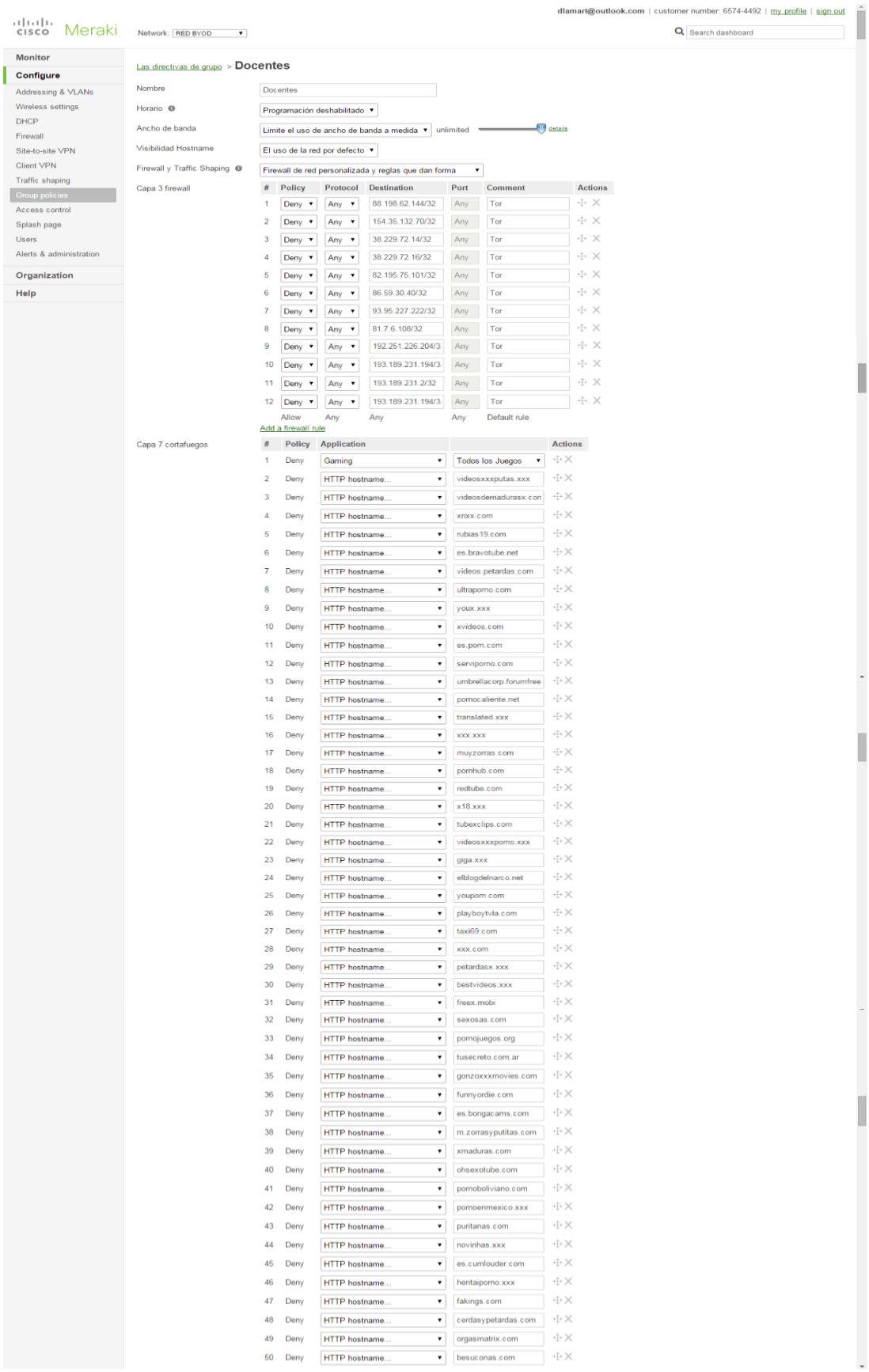
38	Negar	HTTP nombre de host ...	tusecreto.com.ar
39	Negar	HTTP nombre de host ...	gonzoxxxmovies.com
40	Negar	HTTP nombre de host ...	funnyordie.com
41	Negar	HTTP nombre de host ...	es.bongacams.com
42	Negar	HTTP nombre de host ...	m.zorrasyputitas.com
43	Negar	HTTP nombre de host ...	xmaduras.com
44	Negar	HTTP nombre de host ...	ohsexotube.com
45	Negar	HTTP nombre de host ...	pornoboliviano.com
46	Negar	HTTP nombre de host ...	pornoenmexico.xxx
47	Negar	HTTP nombre de host ...	puritanas.com
48	Negar	HTTP nombre de host ...	novinhas.xxx
49	Negar	HTTP nombre de host ...	es.cumlouder.com
50	Negar	HTTP nombre de host ...	hentaiporno.xxx
51	Negar	HTTP nombre de host ...	fakings.com
52	Negar	HTTP nombre de host ...	cerdasypetardas.com
53	Negar	HTTP nombre de host ...	orgasmatrix.com
54	Negar	HTTP nombre de host ...	besuconas.com
55	Negar	HTTP nombre de host ...	esposasymaridos.xxx
56	Negar	HTTP nombre de host ...	culosadictos.com
57	Negar	HTTP nombre de host ...	temagay.com
58	Negar	HTTP nombre de host ...	ixxx.com
59	Negar	HTTP nombre de host ...	yes.xxx
60	Negar	HTTP nombre de host ...	cerdas.com
61	Negar	HTTP nombre de host ...	es.foxtube.com
62	Negar	HTTP nombre de host ...	es.foxgay.com
63	Negar	HTTP nombre de host ...	xxxbunker.com
64	Negar	HTTP nombre de host ...	capullas.com
65	Negar	HTTP nombre de host ...	voayeurs.com
66	Negar	HTTP nombre de host ...	xpornking.com
67	Negar	HTTP nombre de host ...	yourtube.xxx
68	Negar	HTTP nombre de host ...	asnenasdelmafioso.cor
69	Negar	HTTP nombre de host ...	orubias.com
70	Negar	HTTP nombre de host ...	xxxonxxx.com
71	Negar	HTTP nombre de host ...	pornosex.xxx
72	Negar	HTTP nombre de host ...	incestoporno.com
73	Negar	HTTP nombre de host ...	videosxxx.info
74	Negar	HTTP nombre de host ...	camsporno.xxx
75	Negar	HTTP nombre de host ...	momxxx.co
76	Negar	HTTP nombre de host ...	portalnet.cl
77	Negar	HTTP nombre de host ...	xxx.es
78	Negar	HTTP nombre de host ...	alluc.to
79	Negar	HTTP nombre de host ...	maspornoxxx.com
80	Negar	HTTP nombre de host ...	sexopendejas.com
81	Negar	HTTP nombre de host ...	pornoincesto.xxx
82	Negar	HTTP nombre de host ...	videosgratis.tv
83	Negar	HTTP nombre de host ...	perucaseras.com
84	Negar	HTTP nombre de host ...	cholotube.xxx
85	Negar	HTTP nombre de host ...	javichuparadise.com
86	Negar	HTTP nombre de host ...	777my.com
87	Negar	HTTP nombre de host ...	cerdascerdas.com
88	Negar	HTTP nombre de host ...	hdxxx.eu
89	Negar	HTTP nombre de host ...	relatosxxx.net
90	Negar	HTTP nombre de host ...	twistys.com
91	Negar	HTTP nombre de host ...	pornodingue.com
92	Negar	HTTP nombre de host ...	gordas.xxx
93	Negar	HTTP nombre de host ...	videosxxx.info
94	Negar	HTTP nombre de host ...	w2.avxxx.biz
95	Negar	HTTP nombre de host ...	capullas.com
96	Negar	HTTP nombre de host ...	xxx.es
97	Negar	HTTP nombre de host ...	malditoinsolente.com
98	Negar	HTTP nombre de host ...	xxx.com.es
99	Negar	HTTP nombre de host ...	besuconas.com
100	Negar	HTTP nombre de host ...	rozen.com.mx
101	Negar	HTTP nombre de host ...	randosportvtt.com
102	Negar	HTTP nombre de host ...	octopusnetworks.co.uk
103	Negar	HTTP nombre de host ...	sexopendejas.com
104	Negar	HTTP nombre de host ...	vidscalientes.com
105	Negar	HTTP nombre de host ...	pornoincesto.xxx
106	Negar	HTTP nombre de host ...	otabenga.org
107	Negar	HTTP nombre de host ...	videosgratis.tv
108	Negar	HTTP nombre de host ...	ashleymadison.com
109	Negar	HTTP nombre de host ...	conejox.com
110	Negar	HTTP nombre de host ...	videosdeincesto.net
111	Negar	HTTP nombre de host ...	es.foxtube.com

Parte tres.

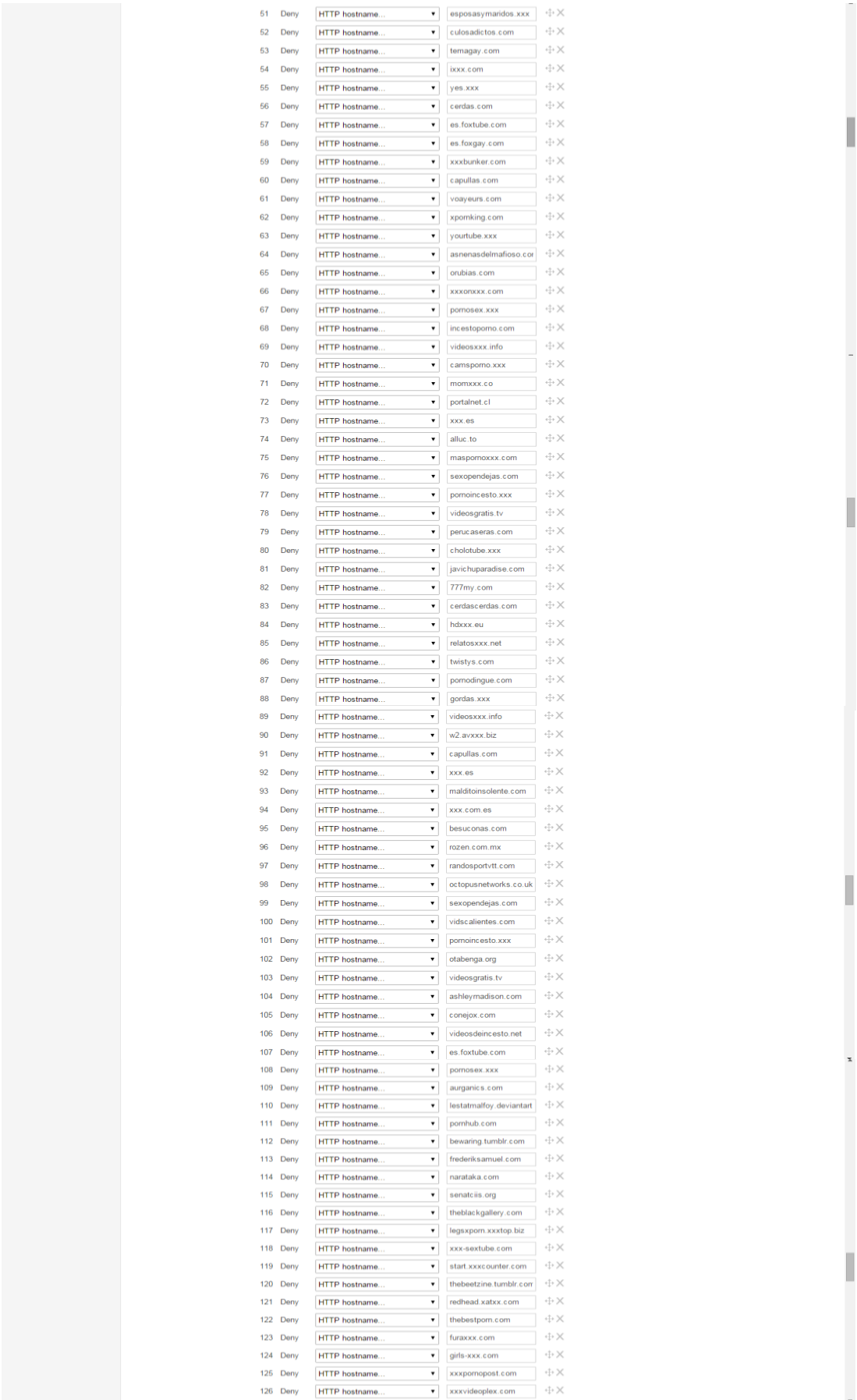

131 Negar HTTP nombre de host ... free.xxx.name
132 Negar HTTP nombre de host ... sites.adult-empire.com
133 Negar HTTP nombre de host ... voayeurs.com
134 Negar HTTP nombre de host ... vivreenfin.com
135 Negar HTTP nombre de host ... afex.biz
136 Negar HTTP nombre de host ... homeycook.com
137 Negar HTTP nombre de host ... youporn.fm
138 Negar HTTP nombre de host ... apornclub.com
139 Negar HTTP nombre de host ... gayxxxblogs.com
140 Negar HTTP nombre de host ... blogs.rediff.com
141 Negar HTTP nombre de host ... megawank.com
142 Negar HTTP nombre de host ... getpornlinks.com
143 Negar HTTP nombre de host ... webstatsdomain.org
144 Negar HTTP nombre de host ... xxxlist.info
145 Negar HTTP nombre de host ... myxxxboobie.com
146 Negar HTTP nombre de host ... xxxexcite.com
147 Negar HTTP nombre de host ... largeladies.pandgart.co
148 Negar HTTP nombre de host ... robtex.com
149 Negar HTTP nombre de host ... blogs.rediff.com
150 Negar HTTP nombre de host ... getpornlinks.com
151 Negar HTTP nombre de host ... webstatsdomain.org
152 Negar HTTP nombre de host ... myxxxboobie.com
153 Negar HTTP nombre de host ... xxxexcite.com
154 Negar HTTP nombre de host ... slapass.net
155 Negar HTTP nombre de host ... videosxxxamateur.xxx
156 Negar HTTP nombre de host ... perucaseraz.com
157 Negar HTTP nombre de host ... xnxxpornsexvideos.cor
158 Negar HTTP nombre de host ... crazytube.xxx
159 Negar HTTP nombre de host ... gc1919.com
160 Negar HTTP nombre de host ... behance.net
161 Negar HTTP nombre de host ... modelcenter.wordpress
162 Negar HTTP nombre de host ... filesharingre.com
Añadir una regla de firewall de capa 7
Conformación de Tráfico
1
Definición This Regla sí aplicará en el Tráfico Que coincidirá estafadores NINGUNA De ESTAS Expresiones.
Todos Los blogs × Anadir +
Límite de ancho de banda
Obedecer Límite Red Por Cliente
500 Kbps details
Prioridad
Alto
DSCP etiquetado
0 (WMM Mejor Esfuerzo)
2
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todo correo electrónico × Añadir +
Límite de ancho de banda
Obedecer red límite por cliente
1 Mbps details
Prioridad
Alto
DSCP etiquetado
3 (WMM Mejor Esfuerzo)
3
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todo intercambio de archivos × Añadir +
Límite de ancho de banda
Obedecer red límite por cliente
500 Kbps details
Prioridad
Normal
DSCP etiquetado
0 (WMM Mejor Esfuerzo)
4
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todas las noticias ×
Todas las actualizaciones de software y antivirus ×
Todos los Deportes × Todo el vídeo y la música ×
Añadir +
Límite de ancho de banda
Obedecer red límite por cliente
250 Kbps details
Prioridad
Bajo
DSCP etiquetado
3 (WMM Mejor Esfuerzo)
5
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todo VoIP y video conferencia × Añadir +
Límite de ancho de banda
Obedecer red límite por cliente
2 Mbps details
Prioridad
Alto
DSCP etiquetado
5 (WMM Video)
Añadir una nueva regla de conformación
Eliminar grupo
Save Changes or cancel
(Please allow 1-2 minutes for changes to take effect.)
© 2014 Cisco Systems, Inc. privacy - terms
Last login: about 23 hours ago
from 181.196.93.7 (Quito, Ecuador).
Current session started: 2 minutes ago
I wish this page would...
make a wish

Anexo 14. Política Docentes.

Parte uno.

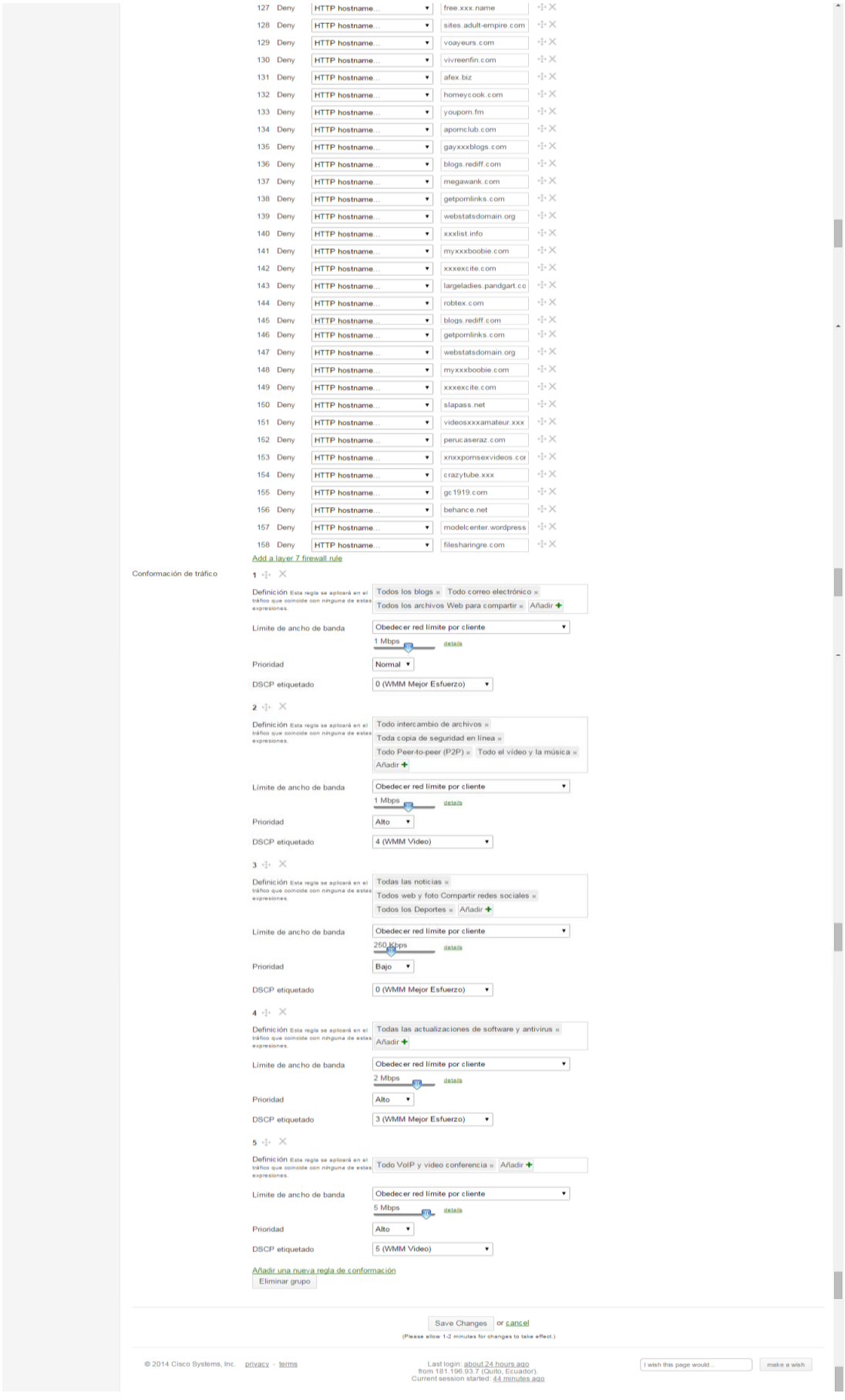


Parte dos.



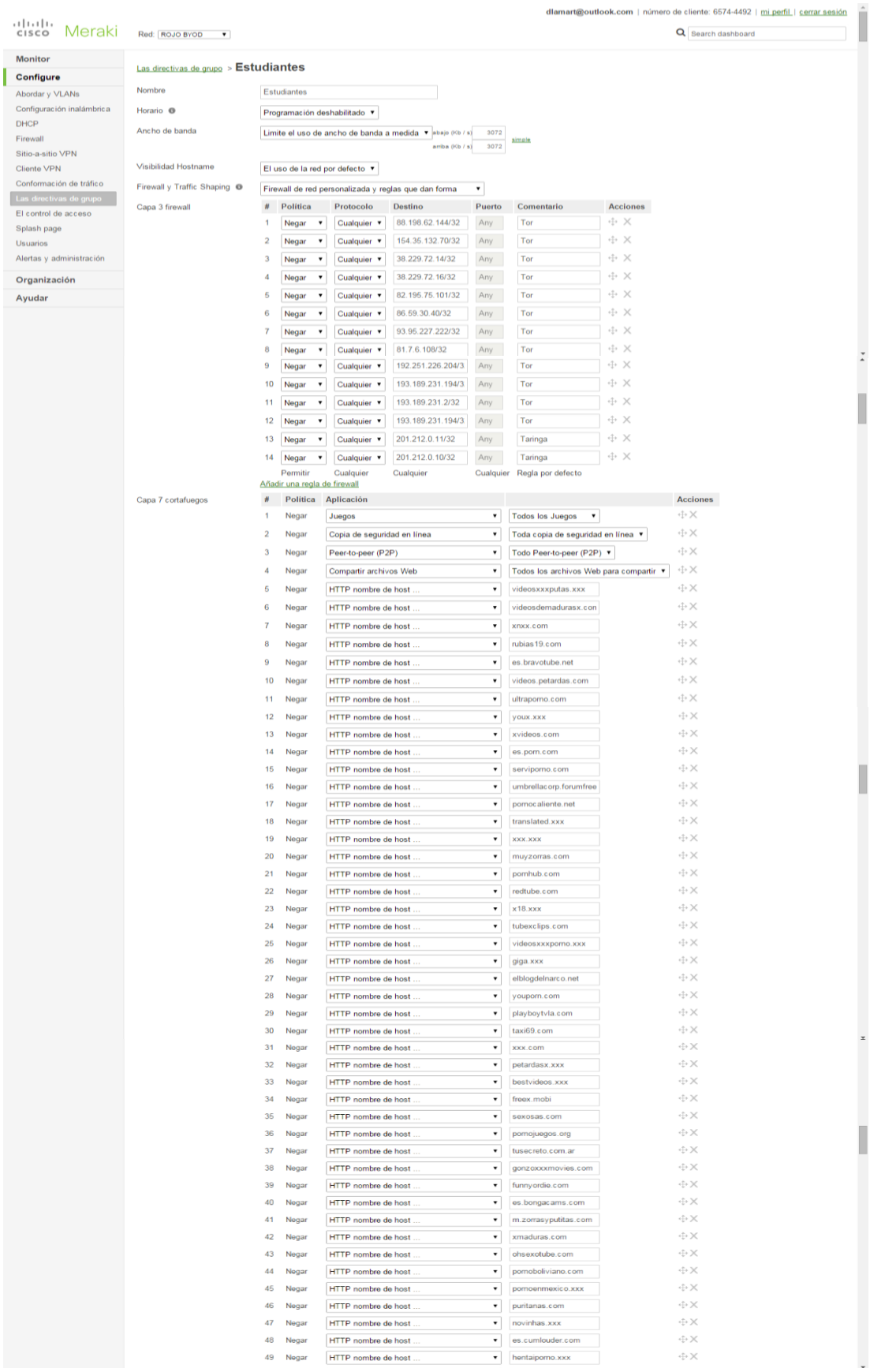
51	Deny	HTTP hostname...	esposasymaridos.xxx
52	Deny	HTTP hostname...	culosadictos.com
53	Deny	HTTP hostname...	temagay.com
54	Deny	HTTP hostname...	ixxx.com
55	Deny	HTTP hostname...	yes.xxx
56	Deny	HTTP hostname...	cerdas.com
57	Deny	HTTP hostname...	es.foxtube.com
58	Deny	HTTP hostname...	es.foxgay.com
59	Deny	HTTP hostname...	xxxbunker.com
60	Deny	HTTP hostname...	capullas.com
61	Deny	HTTP hostname...	voayeurs.com
62	Deny	HTTP hostname...	xpornking.com
63	Deny	HTTP hostname...	yourtube.xxx
64	Deny	HTTP hostname...	asnenasdelmafioso.cor
65	Deny	HTTP hostname...	orubias.com
66	Deny	HTTP hostname...	xxxonxxx.com
67	Deny	HTTP hostname...	pornosex.xxx
68	Deny	HTTP hostname...	incestoporno.com
69	Deny	HTTP hostname...	videosxxx.info
70	Deny	HTTP hostname...	camsporno.xxx
71	Deny	HTTP hostname...	momxxx.co
72	Deny	HTTP hostname...	portalnet.cl
73	Deny	HTTP hostname...	xxx.es
74	Deny	HTTP hostname...	alluc.to
75	Deny	HTTP hostname...	maspornoxxx.com
76	Deny	HTTP hostname...	sexopendejas.com
77	Deny	HTTP hostname...	pornoincesto.xxx
78	Deny	HTTP hostname...	videosgratis.tv
79	Deny	HTTP hostname...	perucaseras.com
80	Deny	HTTP hostname...	cholotube.xxx
81	Deny	HTTP hostname...	javichuparadise.com
82	Deny	HTTP hostname...	777my.com
83	Deny	HTTP hostname...	cerdascerdas.com
84	Deny	HTTP hostname...	hdxxx.eu
85	Deny	HTTP hostname...	relatosxxx.net
86	Deny	HTTP hostname...	twistys.com
87	Deny	HTTP hostname...	pornodingue.com
88	Deny	HTTP hostname...	gordas.xxx
89	Deny	HTTP hostname...	videosxxx.info
90	Deny	HTTP hostname...	w2.avxxx.biz
91	Deny	HTTP hostname...	capullas.com
92	Deny	HTTP hostname...	xxx.es
93	Deny	HTTP hostname...	malditoinsolente.com
94	Deny	HTTP hostname...	xxx.com.es
95	Deny	HTTP hostname...	besuconas.com
96	Deny	HTTP hostname...	rozen.com.mx
97	Deny	HTTP hostname...	randosportvtt.com
98	Deny	HTTP hostname...	octopusnetworks.co.uk
99	Deny	HTTP hostname...	sexopendejas.com
100	Deny	HTTP hostname...	vidscalientes.com
101	Deny	HTTP hostname...	pornoincesto.xxx
102	Deny	HTTP hostname...	otabenga.org
103	Deny	HTTP hostname...	videosgratis.tv
104	Deny	HTTP hostname...	ashleymadison.com
105	Deny	HTTP hostname...	conejox.com
106	Deny	HTTP hostname...	videosdeincesto.net
107	Deny	HTTP hostname...	es.foxtube.com
108	Deny	HTTP hostname...	pornosex.xxx
109	Deny	HTTP hostname...	aurganics.com
110	Deny	HTTP hostname...	lestatmalfoy.deviantart
111	Deny	HTTP hostname...	pornhub.com
112	Deny	HTTP hostname...	bewaring.tumblr.com
113	Deny	HTTP hostname...	frederiksamuel.com
114	Deny	HTTP hostname...	narataka.com
115	Deny	HTTP hostname...	senatciis.org
116	Deny	HTTP hostname...	theblackgallery.com
117	Deny	HTTP hostname...	legsxporn.xxxtop.biz
118	Deny	HTTP hostname...	xxx-sextube.com
119	Deny	HTTP hostname...	start.xxxcounter.com
120	Deny	HTTP hostname...	thebeetzine.tumblr.com
121	Deny	HTTP hostname...	redhead.xatxx.com
122	Deny	HTTP hostname...	thebestporn.com
123	Deny	HTTP hostname...	furaxxx.com
124	Deny	HTTP hostname...	girls-xxx.com
125	Deny	HTTP hostname...	xxxpornopost.com
126	Deny	HTTP hostname...	xxxvideoplex.com

Parte tres.


127 Deny HTTP hostname... free.xxx.name
128 Deny HTTP hostname... sites.adult-empire.com
129 Deny HTTP hostname... voayeurs.com
130 Deny HTTP hostname... vivreenfin.com
131 Deny HTTP hostname... afex.biz
132 Deny HTTP hostname... homeycook.com
133 Deny HTTP hostname... youporn.fm
134 Deny HTTP hostname... apornclub.com
135 Deny HTTP hostname... gayxxxblogs.com
136 Deny HTTP hostname... blogs.rediff.com
137 Deny HTTP hostname... megawank.com
138 Deny HTTP hostname... getpornlinks.com
139 Deny HTTP hostname... webstatsdomain.org
140 Deny HTTP hostname... xxxlist.info
141 Deny HTTP hostname... myxxxboobie.com
142 Deny HTTP hostname... xxxexcite.com
143 Deny HTTP hostname... largeladies.pandgart.co
144 Deny HTTP hostname... robtex.com
145 Deny HTTP hostname... blogs.rediff.com
146 Deny HTTP hostname... getpornlinks.com
147 Deny HTTP hostname... webstatsdomain.org
148 Deny HTTP hostname... myxxxboobie.com
149 Deny HTTP hostname... xxxexcite.com
150 Deny HTTP hostname... slapass.net
151 Deny HTTP hostname... videosxxxamateur.xxx
152 Deny HTTP hostname... perucaseraz.com
153 Deny HTTP hostname... xnxxpornsexvideos.cor
154 Deny HTTP hostname... crazytube.xxx
155 Deny HTTP hostname... gc1919.com
156 Deny HTTP hostname... behance.net
157 Deny HTTP hostname... modelcenter.wordpress
158 Deny HTTP hostname... filesharingre.com
Add a layer 7 firewall rule
Conformación de tráfico
1
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todos los blogs × Todo correo electrónico × Todos los archivos Web para compartir × Añadir
Límite de ancho de banda
Obedecer red límite por cliente
1 Mbps details
Prioridad
Normal
DSCP etiquetado
0 (WMM Mejor Esfuerzo)
2
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todo intercambio de archivos × Toda copia de seguridad en línea × Todo Peer-to-peer (P2P) × Todo el vídeo y la música × Añadir
Límite de ancho de banda
Obedecer red límite por cliente
1 Mbps details
Prioridad
Alto
DSCP etiquetado
4 (WMM Video)
3
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todas las noticias × Todos web y foto Compartir redes sociales × Todos los Deportes × Añadir
Límite de ancho de banda
Obedecer red límite por cliente
250 Kbps details
Prioridad
Bajo
DSCP etiquetado
0 (WMM Mejor Esfuerzo)
4
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todas las actualizaciones de software y antivirus × Añadir
Límite de ancho de banda
Obedecer red límite por cliente
2 Mbps details
Prioridad
Alto
DSCP etiquetado
3 (WMM Mejor Esfuerzo)
5
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todo VoIP y video conferencia × Añadir
Límite de ancho de banda
Obedecer red límite por cliente
5 Mbps details
Prioridad
Alto
DSCP etiquetado
5 (WMM Video)
Añadir una nueva regla de conformación
Eliminar grupo
Save Changes or cancel
(Please allow 1-2 minutes for changes to take effect.)
© 2014 Cisco Systems, Inc. privacy - terms
Last login: about 24 hours ago from 181.196.93.7 (Quito, Ecuador).
Current session started: 44 minutes ago
I wish this page would...
make a wish

Anexo 15. Política Estudiantes.

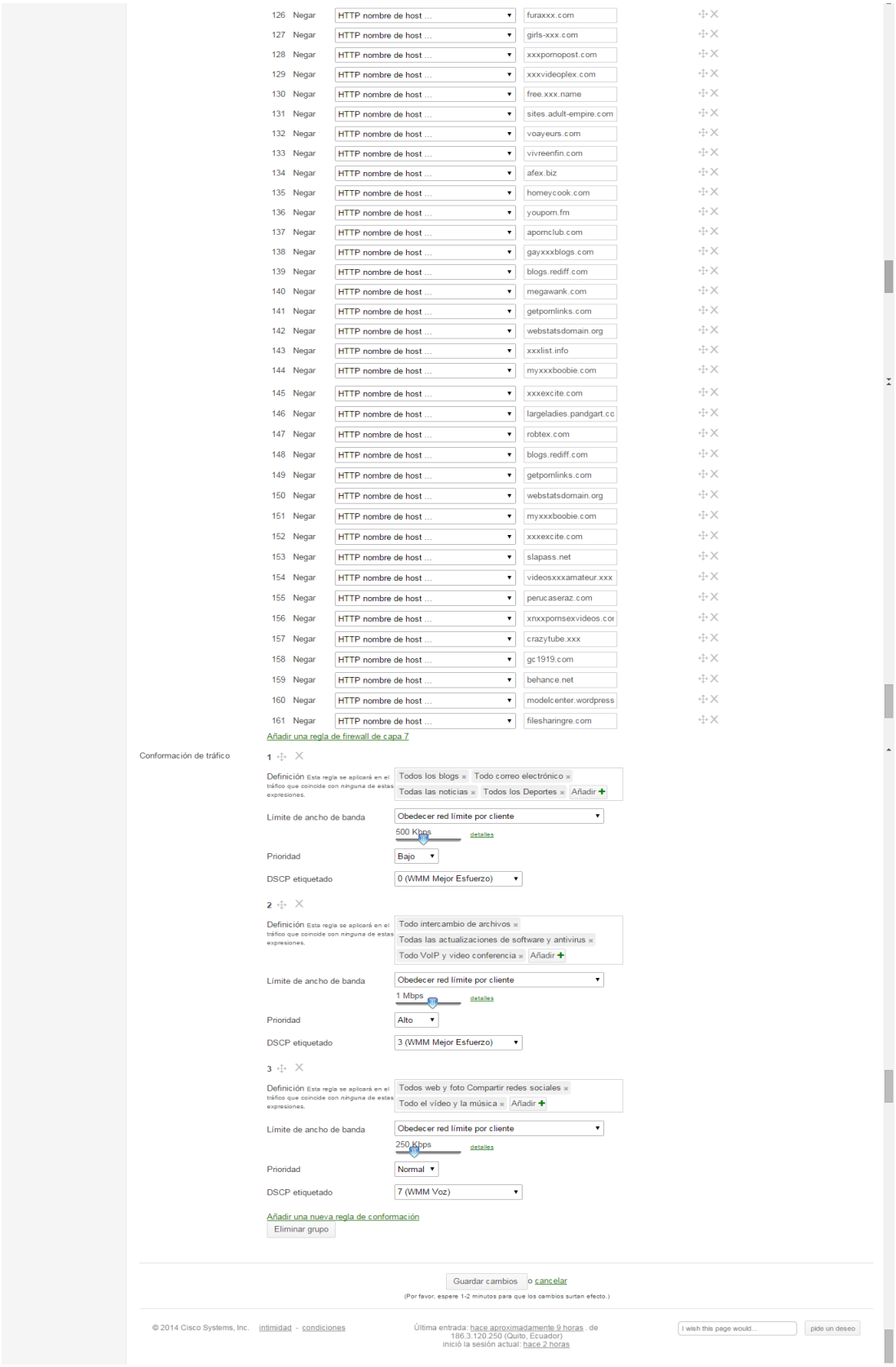
Parte uno.



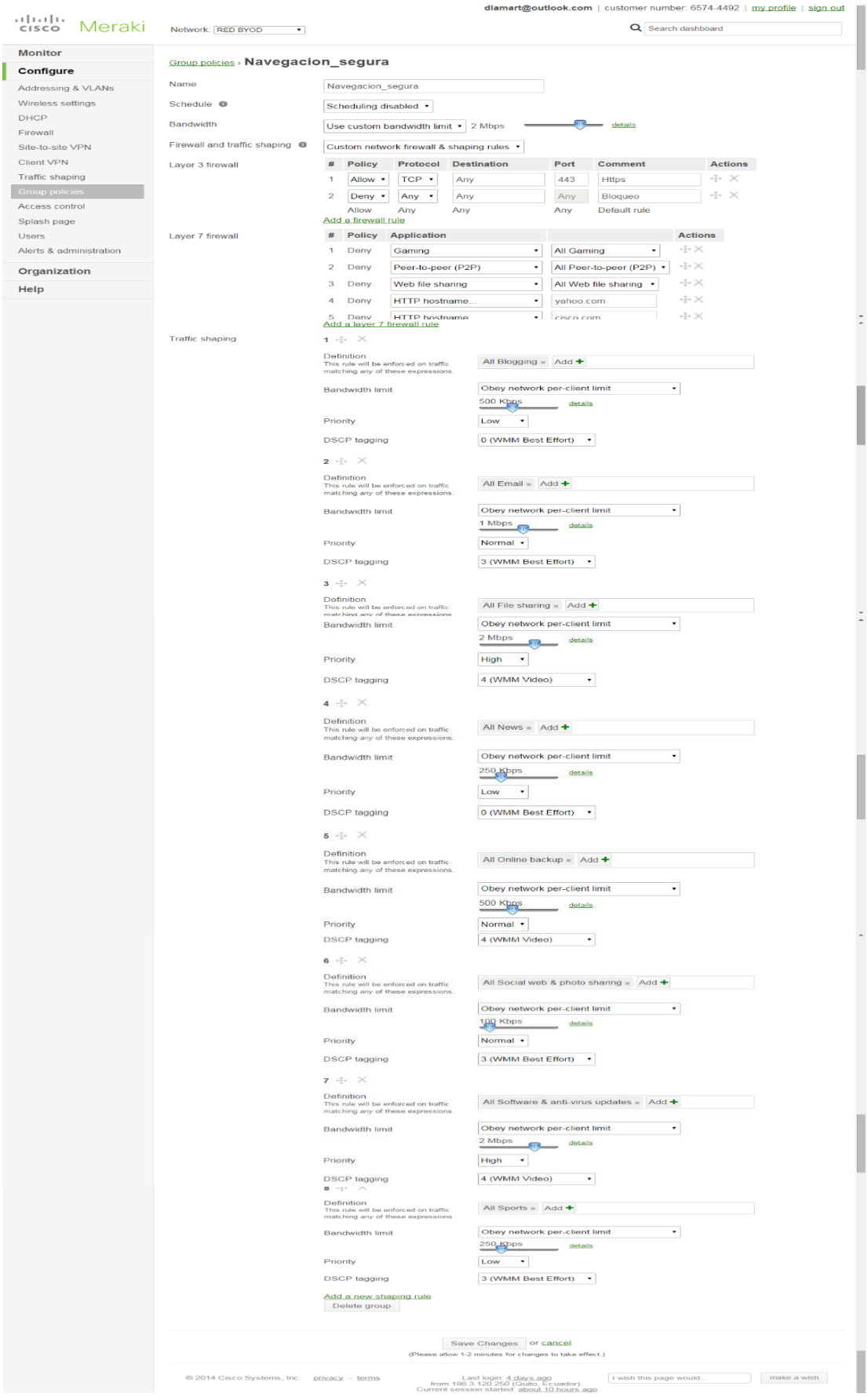
Parte dos.

50	Negar	HTTP nombre de host ...	fakings.com
51	Negar	HTTP nombre de host ...	cerdasypetardas.com
52	Negar	HTTP nombre de host ...	orgasmatrix.com
53	Negar	HTTP nombre de host ...	besuconas.com
54	Negar	HTTP nombre de host ...	esposasymaridos.xxx
55	Negar	HTTP nombre de host ...	culosadictos.com
56	Negar	HTTP nombre de host ...	temagay.com
57	Negar	HTTP nombre de host ...	ixxx.com
58	Negar	HTTP nombre de host ...	yes.xxx
59	Negar	HTTP nombre de host ...	cerdas.com
60	Negar	HTTP nombre de host ...	es.foxtube.com
61	Negar	HTTP nombre de host ...	es.foxgay.com
62	Negar	HTTP nombre de host ...	xxxbunker.com
63	Negar	HTTP nombre de host ...	capullas.com
64	Negar	HTTP nombre de host ...	voayeurs.com
65	Negar	HTTP nombre de host ...	xpornking.com
66	Negar	HTTP nombre de host ...	yourtube.xxx
67	Negar	HTTP nombre de host ...	asnenasdelmafioso.cor
68	Negar	HTTP nombre de host ...	orubias.com
69	Negar	HTTP nombre de host ...	xxxonxxx.com
70	Negar	HTTP nombre de host ...	pornosex.xxx
71	Negar	HTTP nombre de host ...	incestoporno.com
72	Negar	HTTP nombre de host ...	videosxxx.info
73	Negar	HTTP nombre de host ...	camsporno.xxx
74	Negar	HTTP nombre de host ...	mornxxx.co
75	Negar	HTTP nombre de host ...	portalnet.cl
76	Negar	HTTP nombre de host ...	xxx.es
77	Negar	HTTP nombre de host ...	alluc.to
78	Negar	HTTP nombre de host ...	maspornoxxx.com
79	Negar	HTTP nombre de host ...	sexopendejas.com
80	Negar	HTTP nombre de host ...	pornoincesto.xxx
81	Negar	HTTP nombre de host ...	videosgratis.tv
82	Negar	HTTP nombre de host ...	perucaseras.com
83	Negar	HTTP nombre de host ...	cholotube.xxx
84	Negar	HTTP nombre de host ...	javichuparadise.com
85	Negar	HTTP nombre de host ...	777my.com
86	Negar	HTTP nombre de host ...	cerdascerdas.com
87	Negar	HTTP nombre de host ...	hdxxx.eu
88	Negar	HTTP nombre de host ...	relatosxxx.net
89	Negar	HTTP nombre de host ...	twistys.com
90	Negar	HTTP nombre de host ...	pornodingue.com
91	Negar	HTTP nombre de host ...	gordas.xxx
92	Negar	HTTP nombre de host ...	videosxxx.info
93	Negar	HTTP nombre de host ...	w2.avxxx.biz
94	Negar	HTTP nombre de host ...	capullas.com
95	Negar	HTTP nombre de host ...	xxx.es
96	Negar	HTTP nombre de host ...	malditoinsolente.com
97	Negar	HTTP nombre de host ...	xxx.com.es
98	Negar	HTTP nombre de host ...	besuconas.com
99	Negar	HTTP nombre de host ...	rozen.com.mx
100	Negar	HTTP nombre de host ...	randosportvtt.com
101	Negar	HTTP nombre de host ...	octopusnetworks.co.uk
102	Negar	HTTP nombre de host ...	sexopendejas.com
103	Negar	HTTP nombre de host ...	vidscalientes.com
104	Negar	HTTP nombre de host ...	pornoincesto.xxx
105	Negar	HTTP nombre de host ...	otabenga.org
106	Negar	HTTP nombre de host ...	videosgratis.tv
107	Negar	HTTP nombre de host ...	ashleymadison.com
108	Negar	HTTP nombre de host ...	conejox.com
109	Negar	HTTP nombre de host ...	videosdeincesto.net
110	Negar	HTTP nombre de host ...	es.foxtube.com
111	Negar	HTTP nombre de host ...	pornosex.xxx
112	Negar	HTTP nombre de host ...	aurganics.com
113	Negar	HTTP nombre de host ...	lestatmalfoy.deviantart
114	Negar	HTTP nombre de host ...	pornhub.com
115	Negar	HTTP nombre de host ...	bewaring.tumblr.com
116	Negar	HTTP nombre de host ...	frederiksamuel.com
117	Negar	HTTP nombre de host ...	narataka.com
118	Negar	HTTP nombre de host ...	senatciis.org
119	Negar	HTTP nombre de host ...	theblackgallery.com
120	Negar	HTTP nombre de host ...	legsxporn.xxxtop.biz
121	Negar	HTTP nombre de host ...	xxx-sextube.com
122	Negar	HTTP nombre de host ...	start.xxxcounter.com
123	Negar	HTTP nombre de host ...	thebeetzine.tumblr.com
124	Negar	HTTP nombre de host ...	redhead.xatxx.com
125	Negar	HTTP nombre de host ...	thebestporn.com

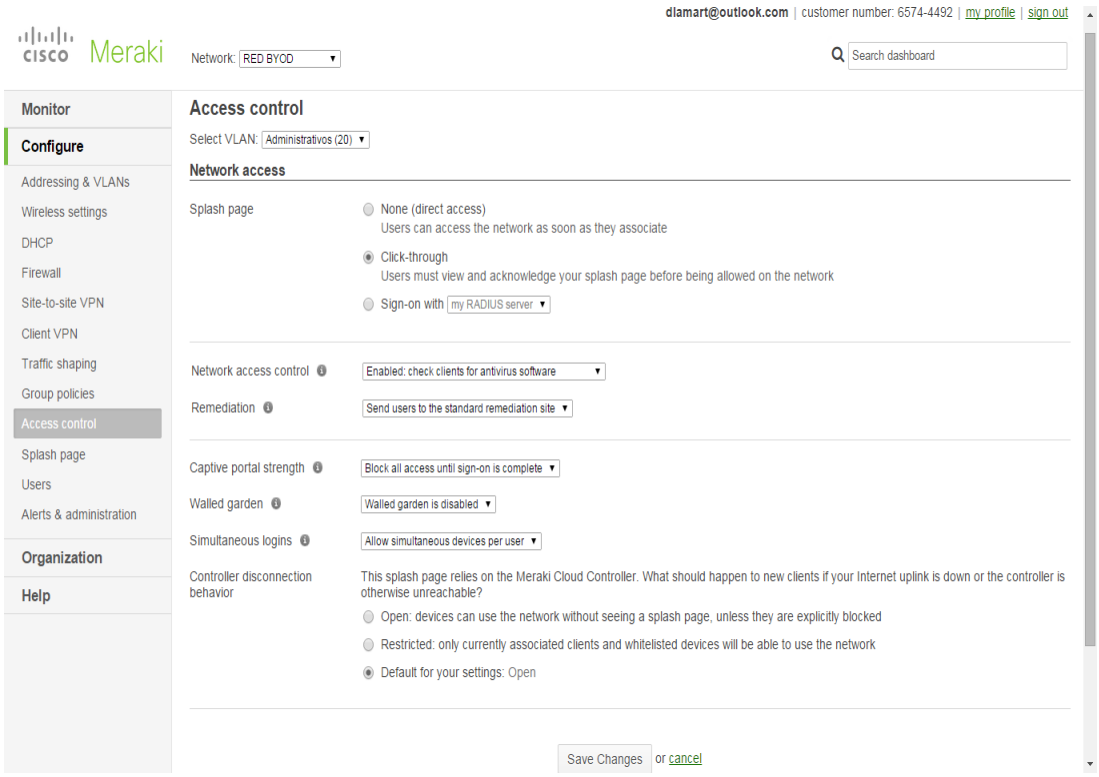
Parte tres.


126 Negar HTTP nombre de host ... furaxxx.com
127 Negar HTTP nombre de host ... girls-xxx.com
128 Negar HTTP nombre de host ... xxxpornopost.com
129 Negar HTTP nombre de host ... xxxvideoplex.com
130 Negar HTTP nombre de host ... free.xxx.name
131 Negar HTTP nombre de host ... sites.adult-empire.com
132 Negar HTTP nombre de host ... voayeurs.com
133 Negar HTTP nombre de host ... vivreenfin.com
134 Negar HTTP nombre de host ... afex.biz
135 Negar HTTP nombre de host ... homeycook.com
136 Negar HTTP nombre de host ... youporn.fm
137 Negar HTTP nombre de host ... apornclub.com
138 Negar HTTP nombre de host ... gayxxxblogs.com
139 Negar HTTP nombre de host ... blogs.rediff.com
140 Negar HTTP nombre de host ... megawank.com
141 Negar HTTP nombre de host ... getpornlinks.com
142 Negar HTTP nombre de host ... webstatsdomain.org
143 Negar HTTP nombre de host ... xxxlist.info
144 Negar HTTP nombre de host ... myxxxboobie.com
145 Negar HTTP nombre de host ... xxxexcite.com
146 Negar HTTP nombre de host ... largeladies.pandgart.co
147 Negar HTTP nombre de host ... robtex.com
148 Negar HTTP nombre de host ... blogs.rediff.com
149 Negar HTTP nombre de host ... getpornlinks.com
150 Negar HTTP nombre de host ... webstatsdomain.org
151 Negar HTTP nombre de host ... myxxxboobie.com
152 Negar HTTP nombre de host ... xxxexcite.com
153 Negar HTTP nombre de host ... slapass.net
154 Negar HTTP nombre de host ... videosxxxamateur.xxx
155 Negar HTTP nombre de host ... perucaseraz.com
156 Negar HTTP nombre de host ... xnxxpornsexvideos.cor
157 Negar HTTP nombre de host ... crazytube.xxx
158 Negar HTTP nombre de host ... gc1919.com
159 Negar HTTP nombre de host ... behance.net
160 Negar HTTP nombre de host ... modelcenter.wordpress
161 Negar HTTP nombre de host ... filesharingre.com
Añadir una regla de firewall de capa 7
Conformación de tráfico
1
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todos los blogs × Todo correo electrónico × Todas las noticias × Todos los Deportes × Añadir +
Límite de ancho de banda
Obedecer red límite por cliente
500 Kbps
detalles
Prioridad
Bajo
DSCP etiquetado
0 (WMM Mejor Esfuerzo)
2
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todo intercambio de archivos × Todas las actualizaciones de software y antivirus × Todo VoIP y video conferencia × Añadir +
Límite de ancho de banda
Obedecer red límite por cliente
1 Mbps
detalles
Prioridad
Alto
DSCP etiquetado
3 (WMM Mejor Esfuerzo)
3
Definición Esta regla se aplicará en el tráfico que coincide con ninguna de estas expresiones.
Todos web y foto Compartir redes sociales × Todo el vídeo y la música × Añadir +
Límite de ancho de banda
Obedecer red límite por cliente
250 Kbps
detalles
Prioridad
Normal
DSCP etiquetado
7 (WMM Voz)
Añadir una nueva regla de conformación
Eliminar grupo
Guardar cambios o cancelar
(Por favor, espere 1-2 minutos para que los cambios surtan efecto.)
© 2014 Cisco Systems, Inc. intimidad - condiciones
Última entrada: hace aproximadamente 9 horas . de 186.3.120.250 (Quito, Ecuador)
inició la sesión actual: hace 2 horas
I wish this page would...
pide un deseo

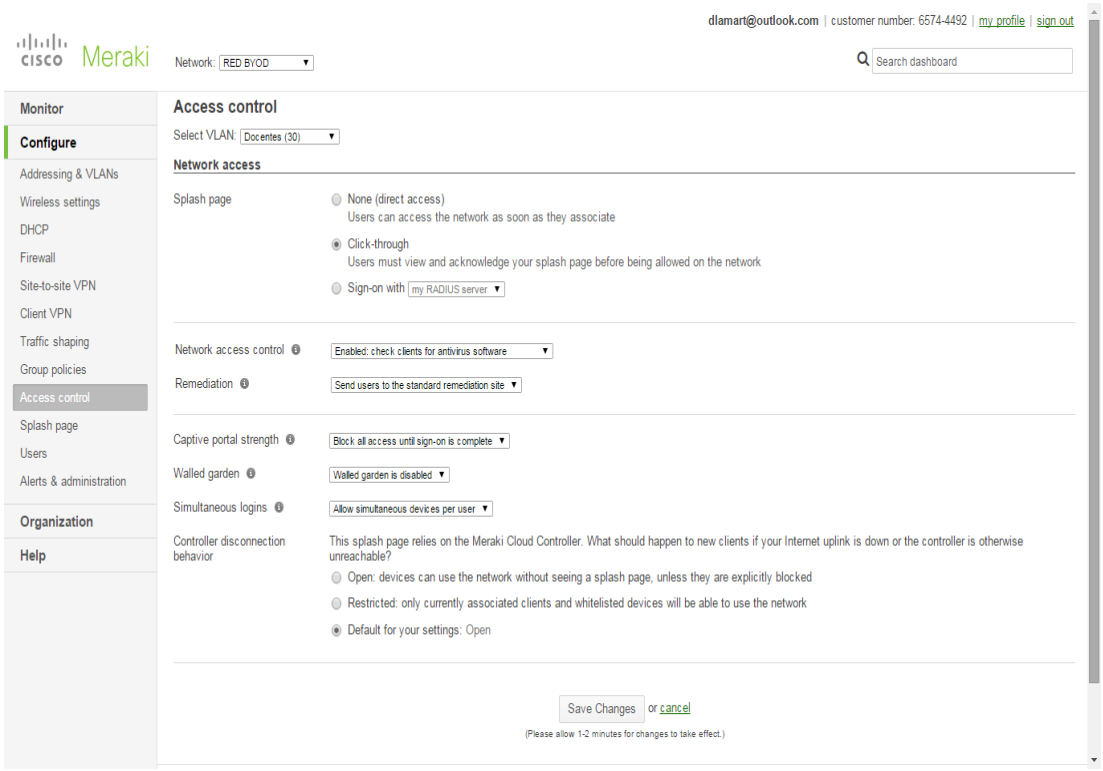
Anexo 16. Política Navegacion_segura.



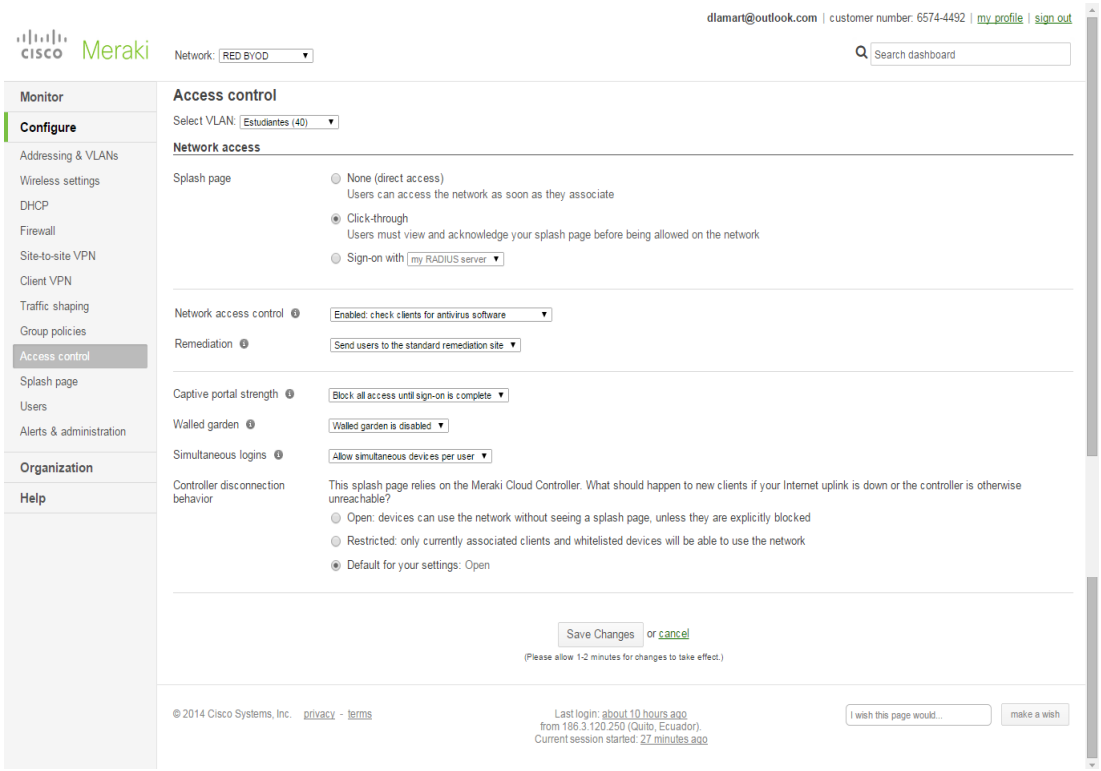
Anexo 17. Control de Acceso VLAN Administrativos.



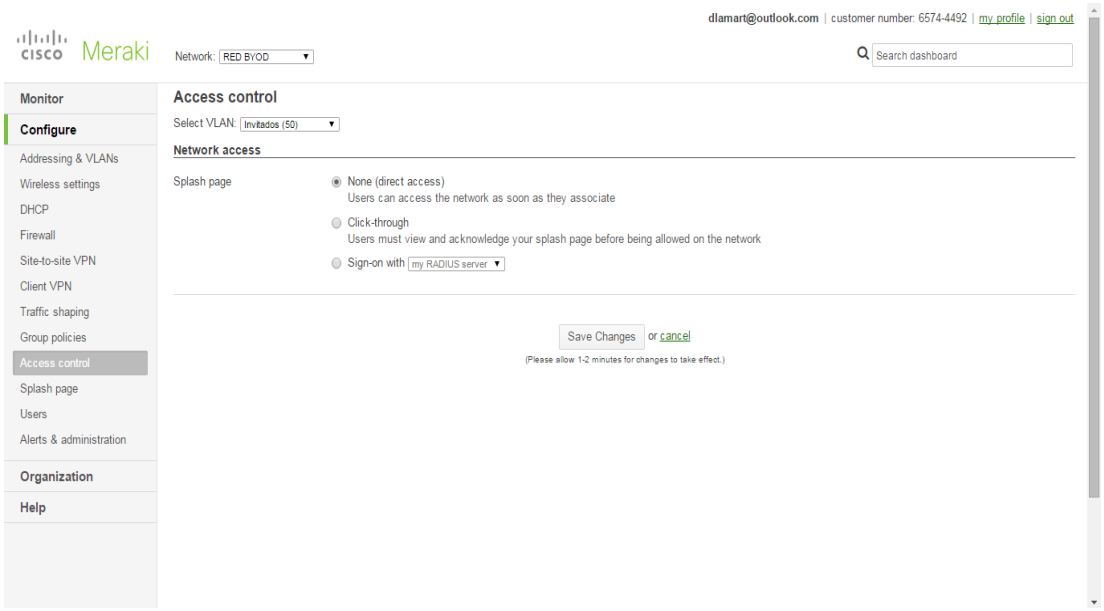
Anexo 18. Control de Acceso VLAN Docentes.



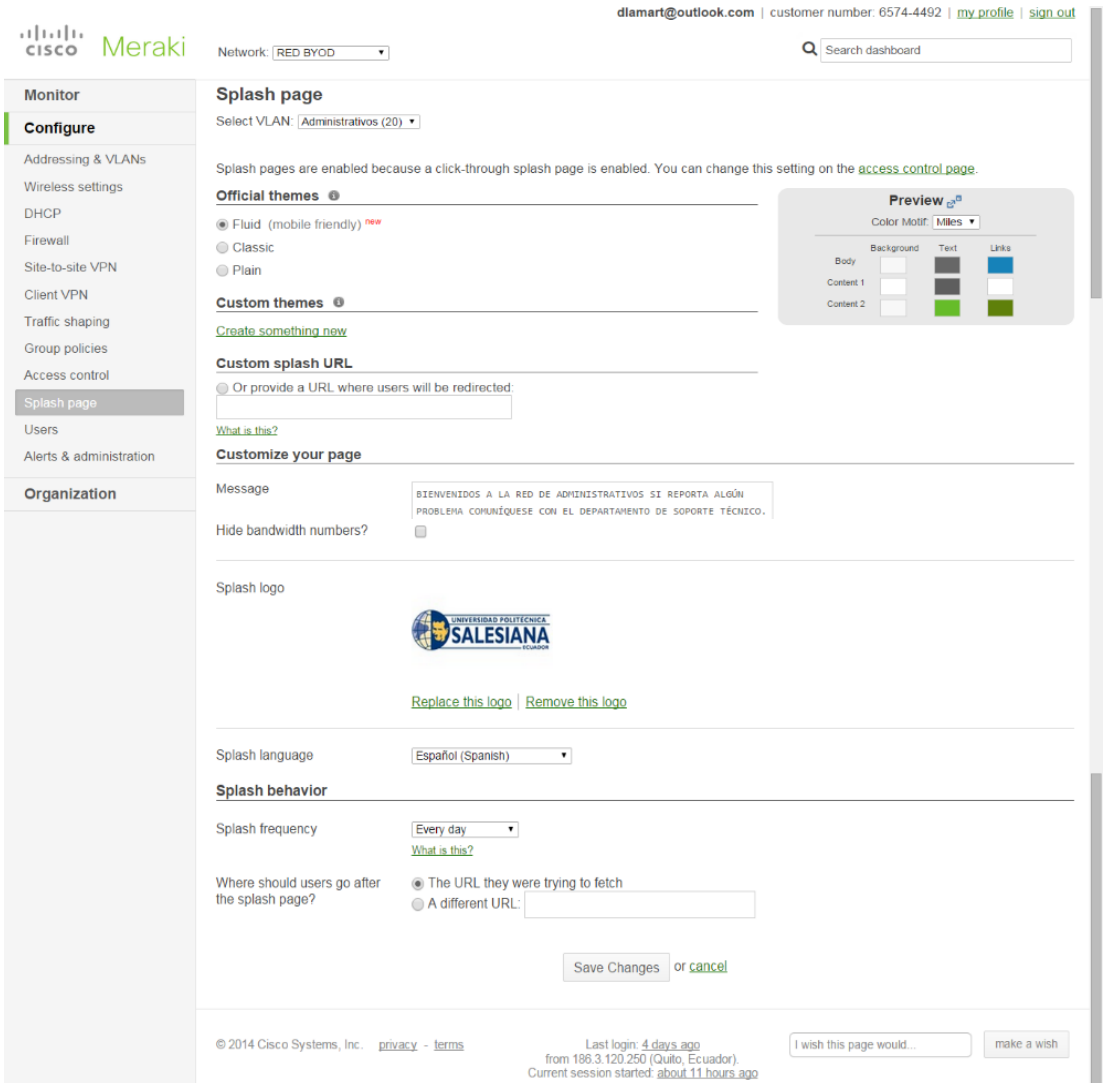
Anexo 19. Control de Acceso VLAN Estudiantes.



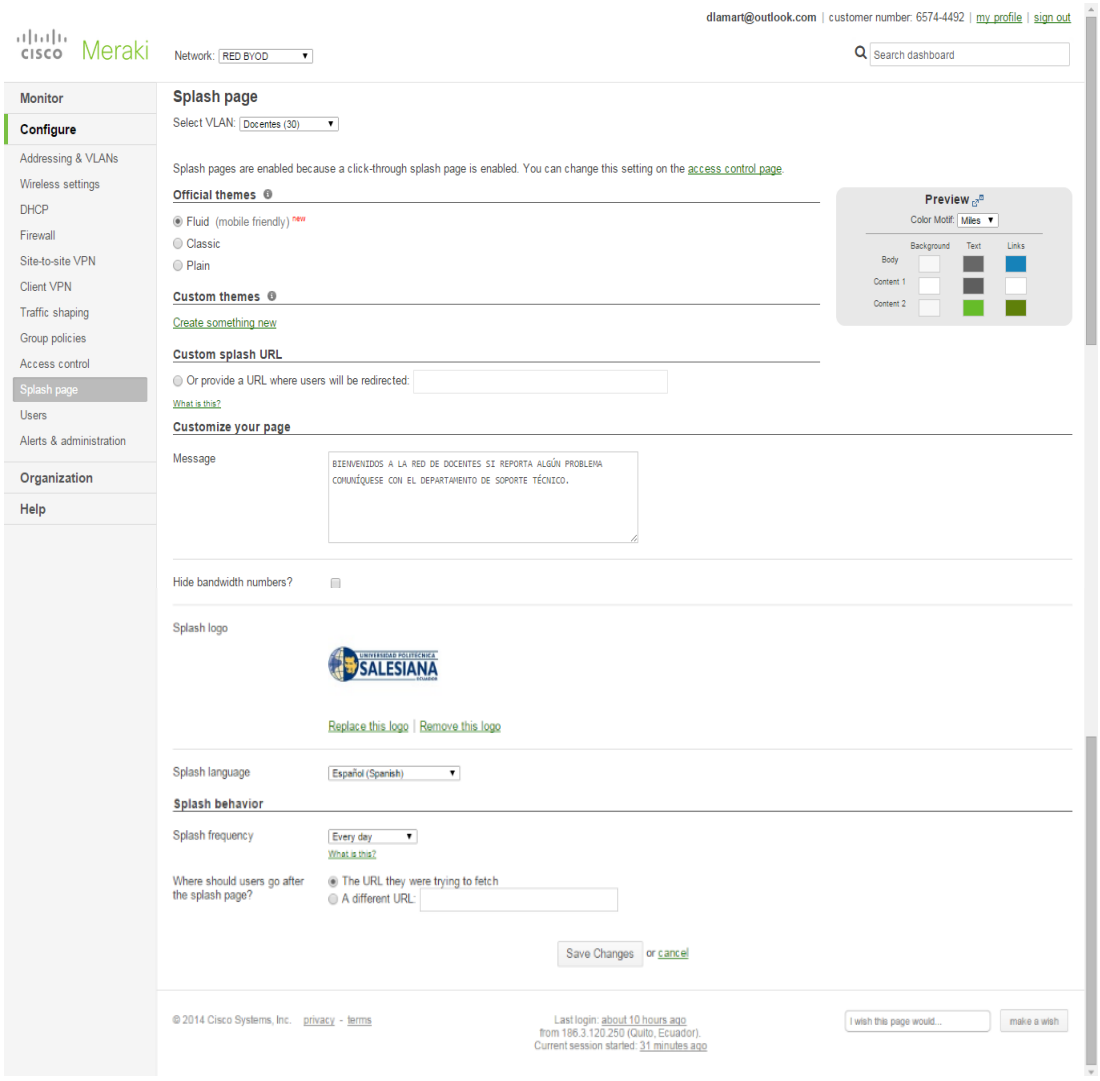
Anexo 20. Control de Acceso VLAN Invitados.



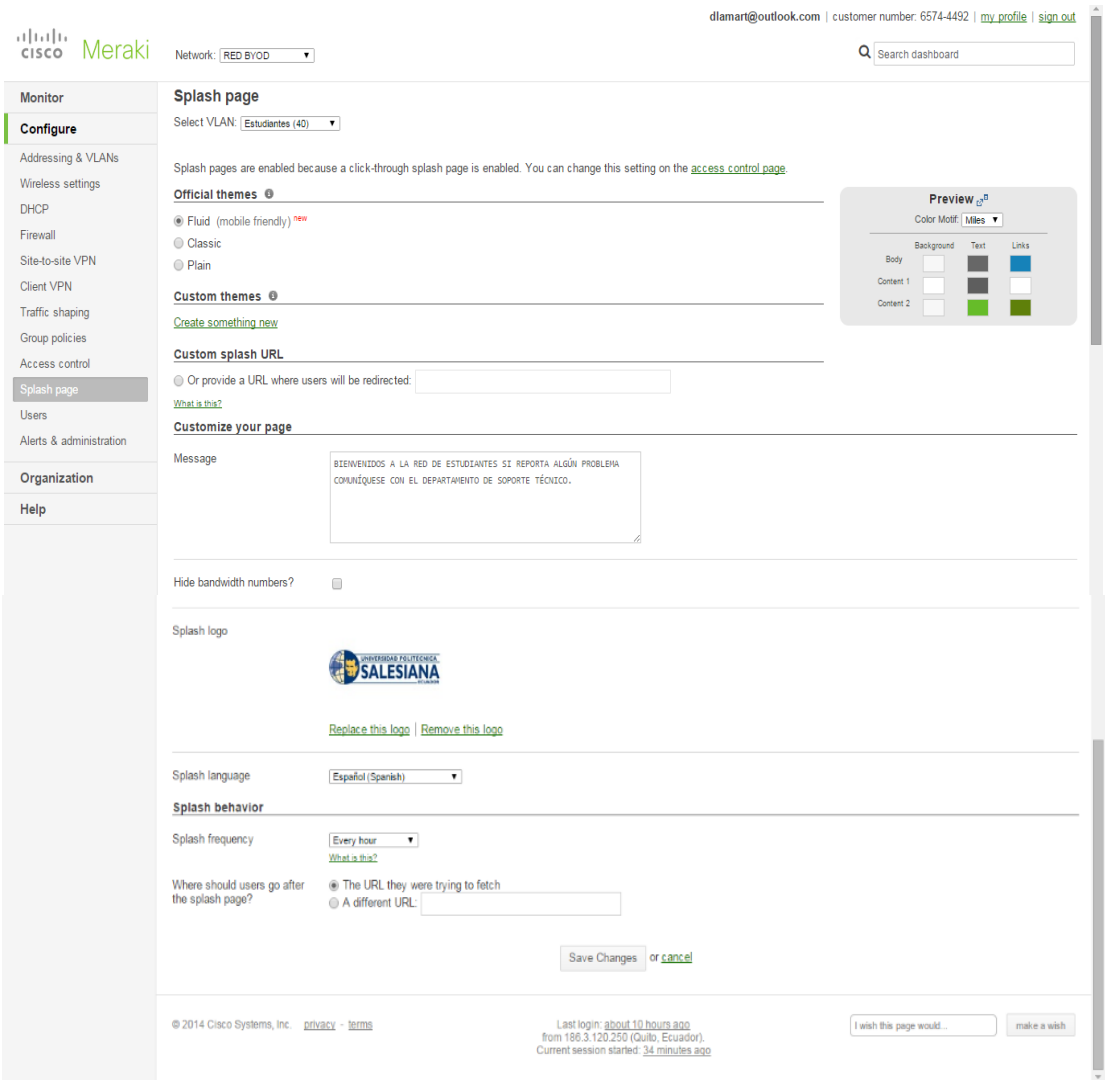
Anexo 21. Página de Bienvenida VLAN Administrativos.



Anexo 22. Página de Bienvenida VLAN Docentes.

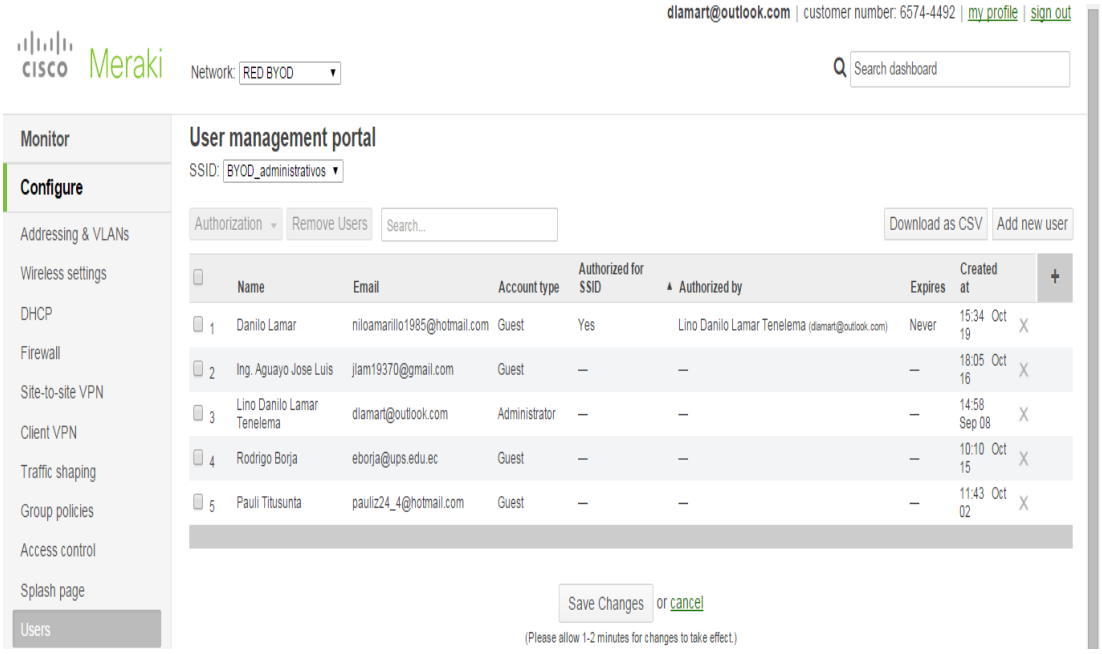


Anexo 23. Página de Bienvenida VLAN Estudiantes.



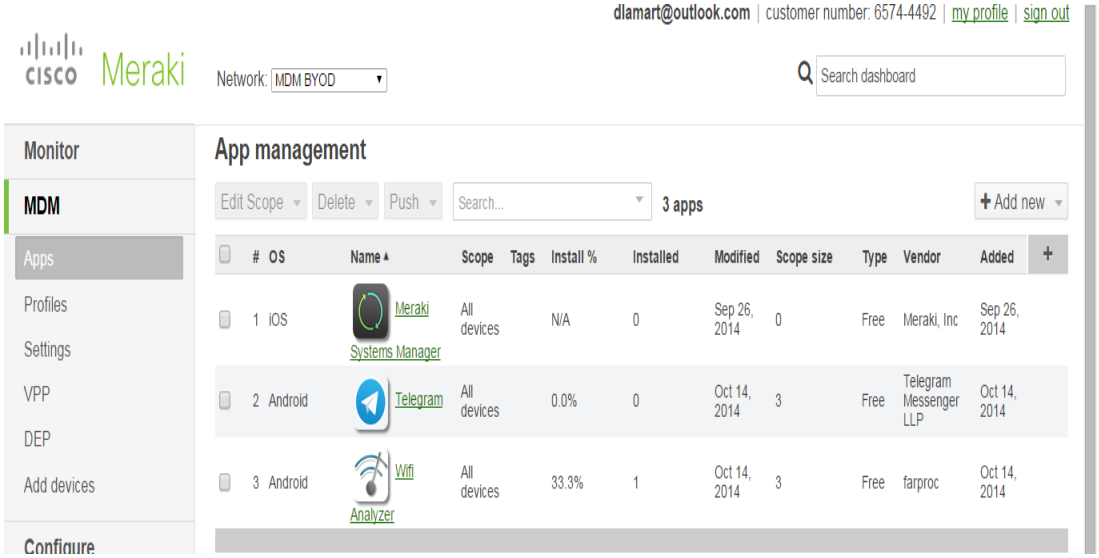
Anexo 24. Usuarios.

En esta sección se configuran los usuarios con algunos parámetros como son: nombre, email, contraseña y la autorización sobre un SSID en específico.



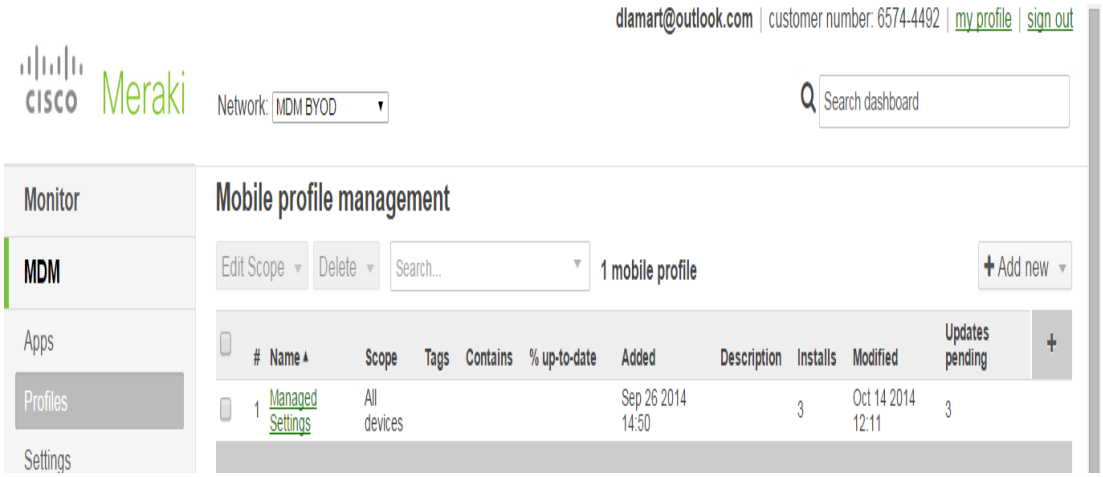
Anexo 25. Aplicaciones.

En este apartado se administra las app que pueden ser instaladas en los dispositivos.



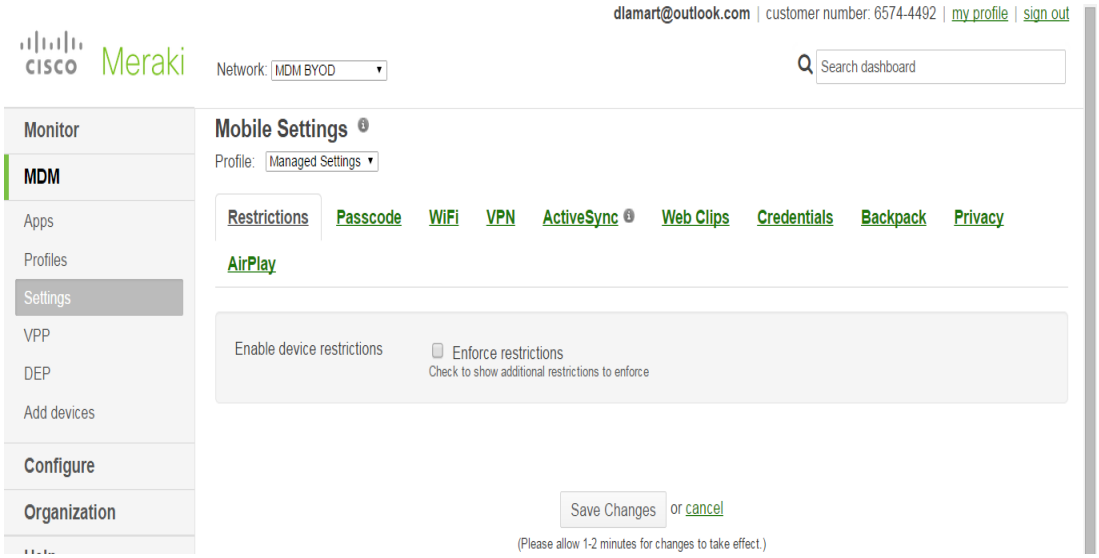
Anexo 26. Administración de perfiles móviles.

En esta sección se pueden crear distintos perfiles para los dispositivos, además de configurar algunas características como: política, alcance en los dispositivos, etc.



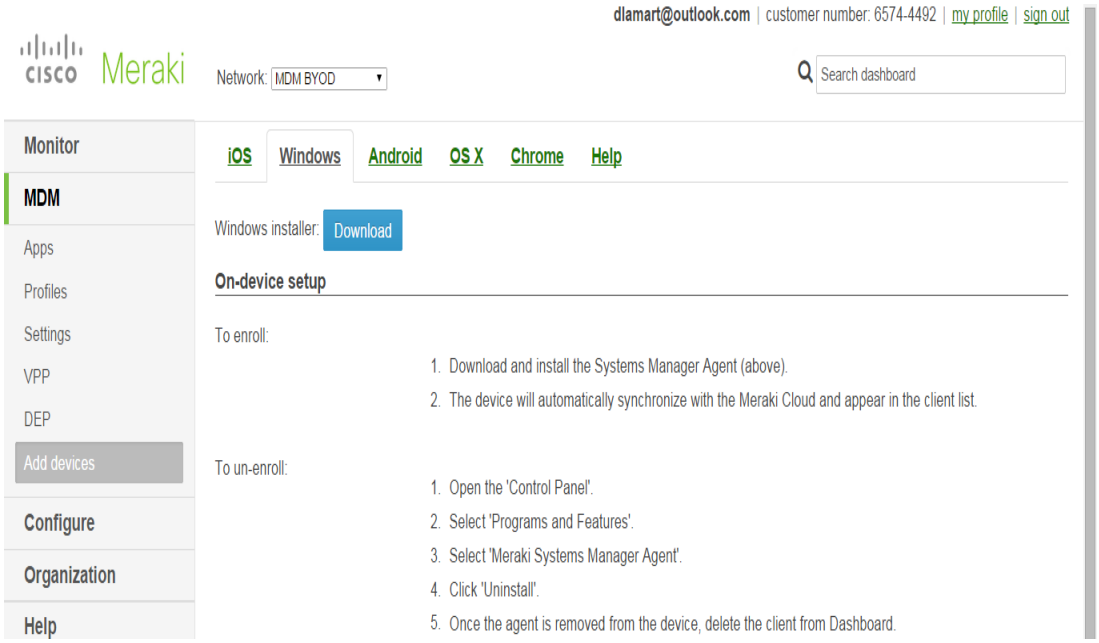
Anexo 27. Configuraciones.

En esta sección se agregan configuraciones especiales a los dispositivos móviles.



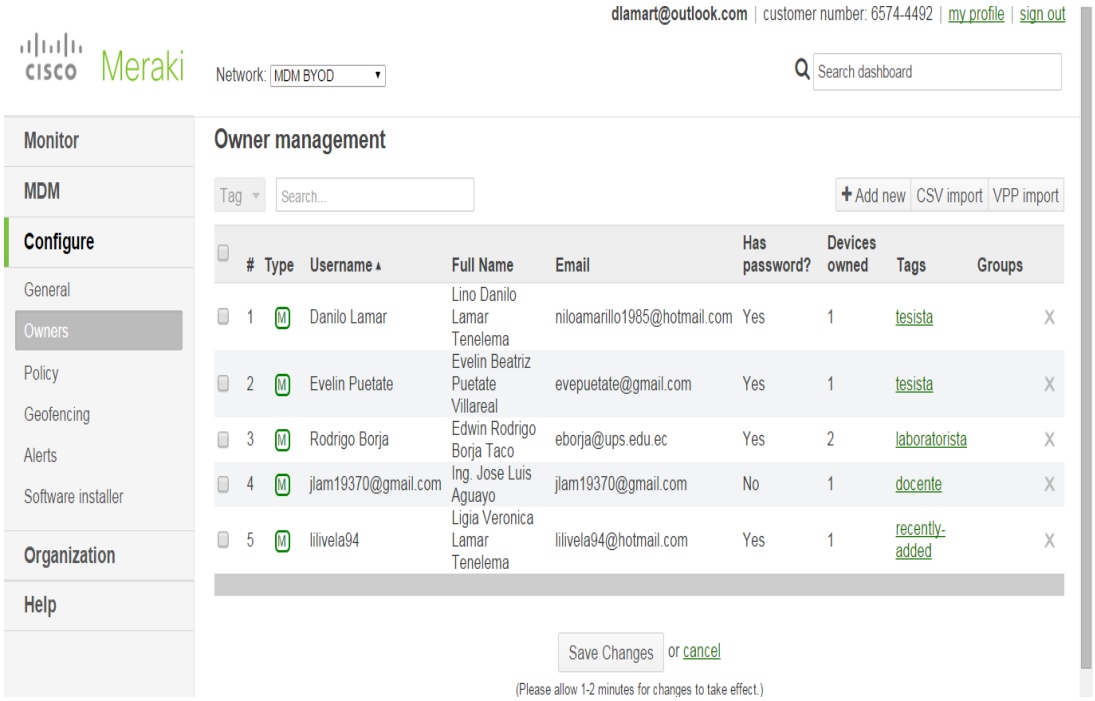
Anexo 28. Añadir dispositivos.

En esta ventana se observan los distintos dispositivos que pueden ser añadidos al MDM BYOD a través de un instalador o una aplicación.



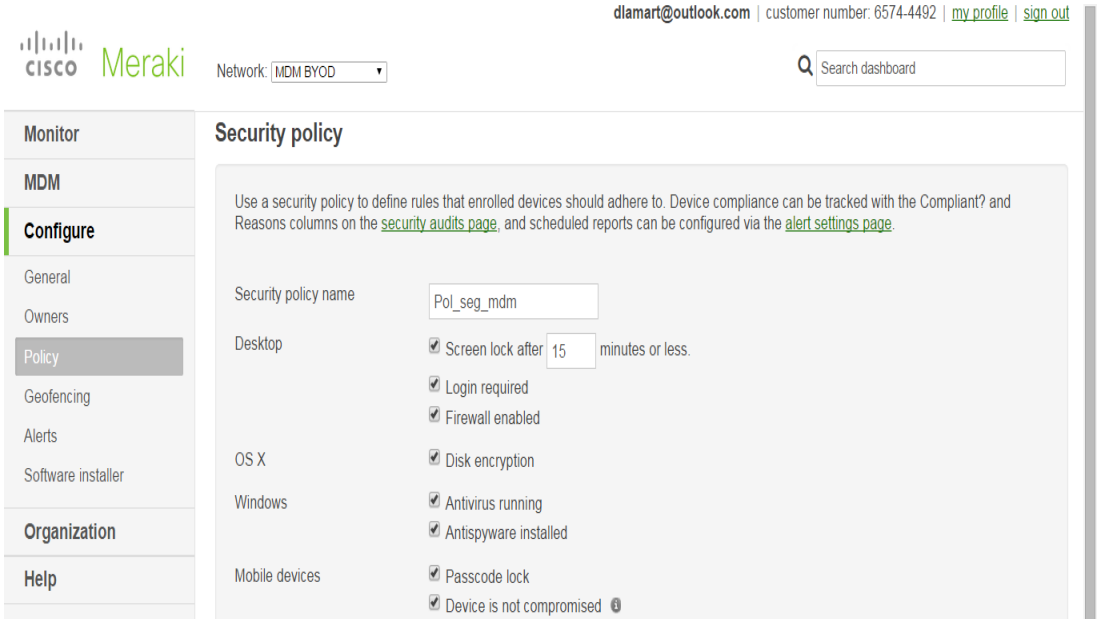
Anexo 29. Propietarios.

En este apartado se crea un usuario con algunos parámetros como son: email, usuario, etiqueta, contraseña y al cual se le puede asignar dispositivos móviles.



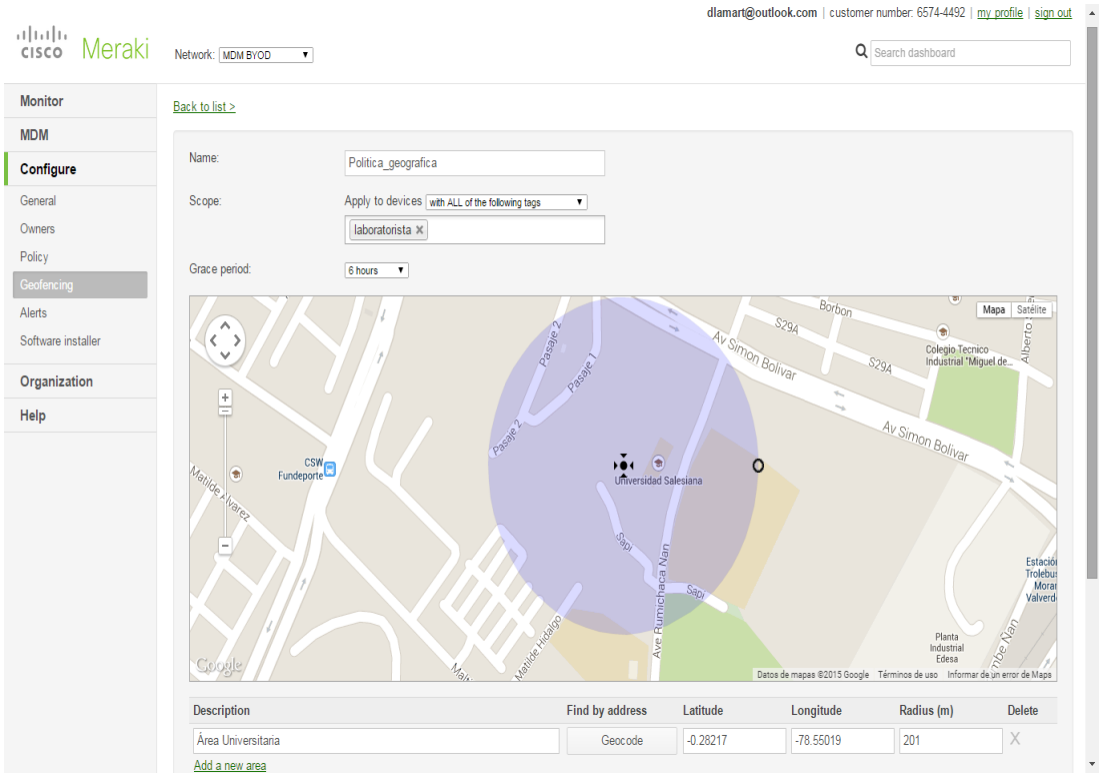
Anexo 30. Política de seguridad.

Aquí se configuró una política de seguridad para los distintos dispositivos que se unen al MDM BYOD.



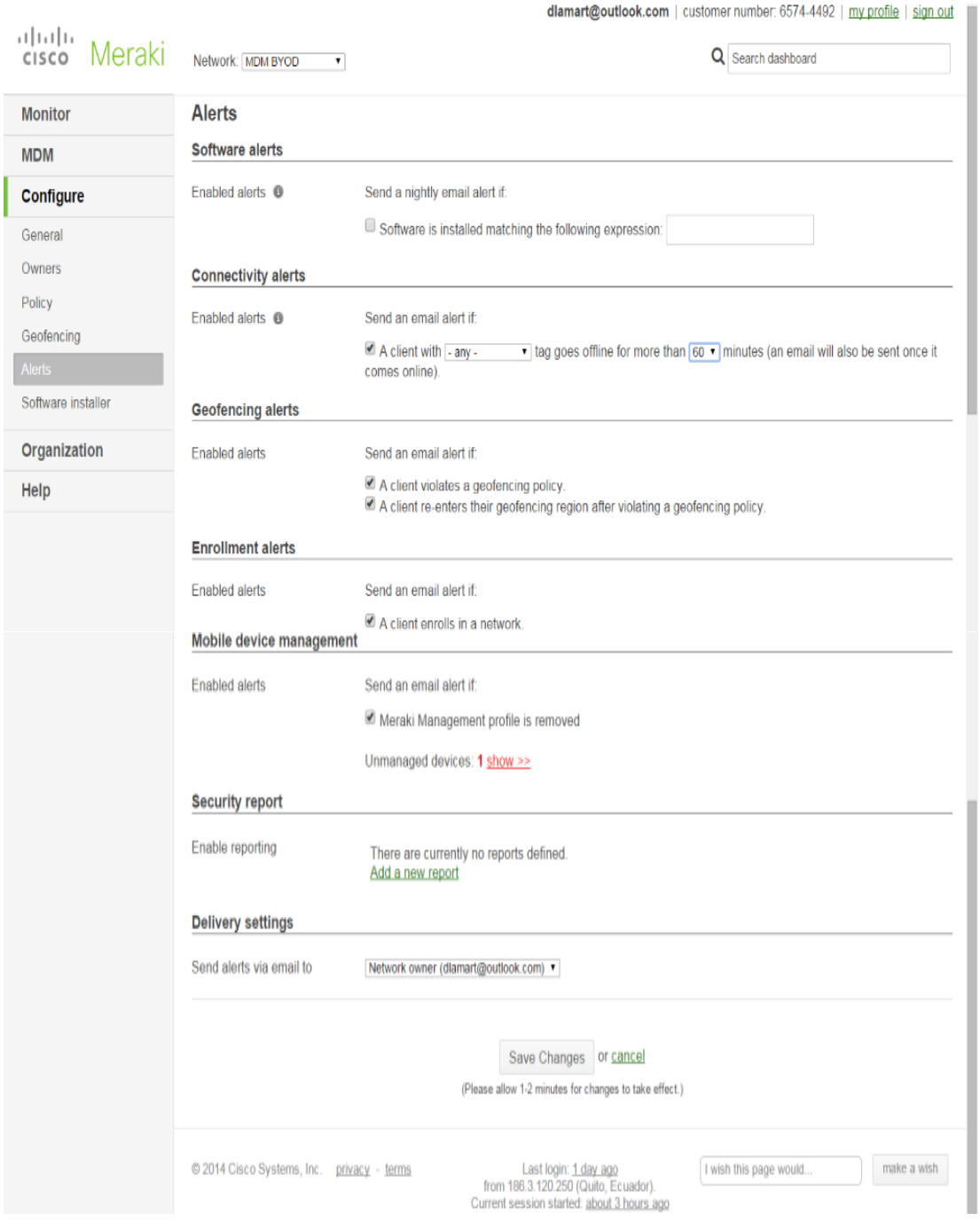
Anexo 31. Geo ubicación.

Esta es una política de geo ubicación que puede ser aplicada sobre uno o todos los dispositivos del MDM BYOD.



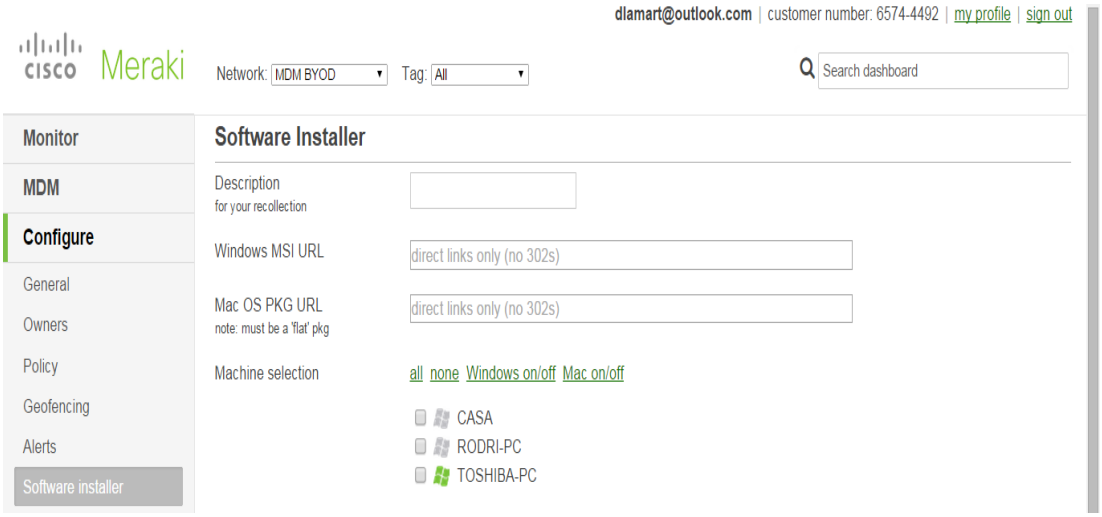
Anexo 32. Alertas.

Las alertas configuradas en el MDM BYOD son del tipo de conectividad, geo ubicación, enrolamiento en la red, administración de dispositivos móviles, todas estas alertas se envían al administrador de red.



Anexo 33. Instalador de software.

Para cada sistema operativo el instalador debe estar en .msi para Windows y .pkg para Mac, y deben estar en un repositorio en la nube, en este caso se usó Dropbox.



Anexo 34. Encuesta 2 Conexión a la red piloto BYOD de la UPS.

Tema: Conexión a la red piloto BYOD de la UPS.

Marque con una X la respuesta correcta según su criterio.

1. ¿Con cuántos dispositivos usted se conectó a la red BYOD?

1 dispositivo ☐ 2 dispositivos ☐ 3 dispositivos ☐

2. ¿Qué tipo de dispositivo/s utilizó usted para conectarse?

Smartphone ☐ Tablet ☐ Laptop ☐

3. ¿Cuál es el sistema operativo de su/sus dispositivo/s?

Android ☐ iOS ☐ Windows ☐

4. Al momento que se conectó a la red BYOD_invitados tuvo problemas.

Sí ☐ No ☐

5. ¿A qué red inalámbrica o SSID permaneció conectado?

BYOD_invitados ☐ BYOD_estudiantes ☐

BYOD_docentes ☐ BYOD_administrativos ☐

6. Cuando se cambió de red tuvo problemas para conectarse. Sí ☐ No ☐
7. El acceso a la red te parece: Simple ☐ Complicado ☐
8. Fuiste enviado a un sitio de remediación de antivirus. Sí ☐ No ☐
9. El enrolamiento en la red fue: Rápido ☐ Lento ☐
10. ¿Cuál es la velocidad de su conexión o ancho de banda?

1 Mbps ☐ 2Mbps ☐ 3Mbps ☐ Ilimitado ☐

11. La navegación te pareció: Rápida ☐ Lenta ☐
12. Accede a este enlace http://www.sidar.org/traducciones/wcag20/es/

La carga de la página fue: Rápida ☐ Lenta ☐

13. Al reproducir un video fue: Rápido ☐ Lento ☐

14. Logro descargar un archivo: Sí ☐ No ☐

15. La descarga del archivo fue: Rápida ☐ Lenta ☐

16. Al cambiarte de política se notaron los cambios. Sí ☐ No ☐

17. Él envió de notificaciones fue satisfactorio. Sí ☐ No ☐

18. Su dispositivo fue localizado. Sí ☐ No ☐

19. Él envió de app a su dispositivo fue satisfactorio. Sí ☐ No ☐

20. En las aplicaciones en tiempo real, su funcionamiento fue:

Bueno ☐ Malo ☐

21. Al desconectar o apagar el equipo y volver a conectarse a la red la conexión a la red tuvo problemas.

Sí ☐ No ☐

22. Recomendaría usted implementarse BYOD en la Universidad.

Sí ☐ No ☐

23. Qué tipo de recomendación usted podría hacer con respecto a la red piloto.

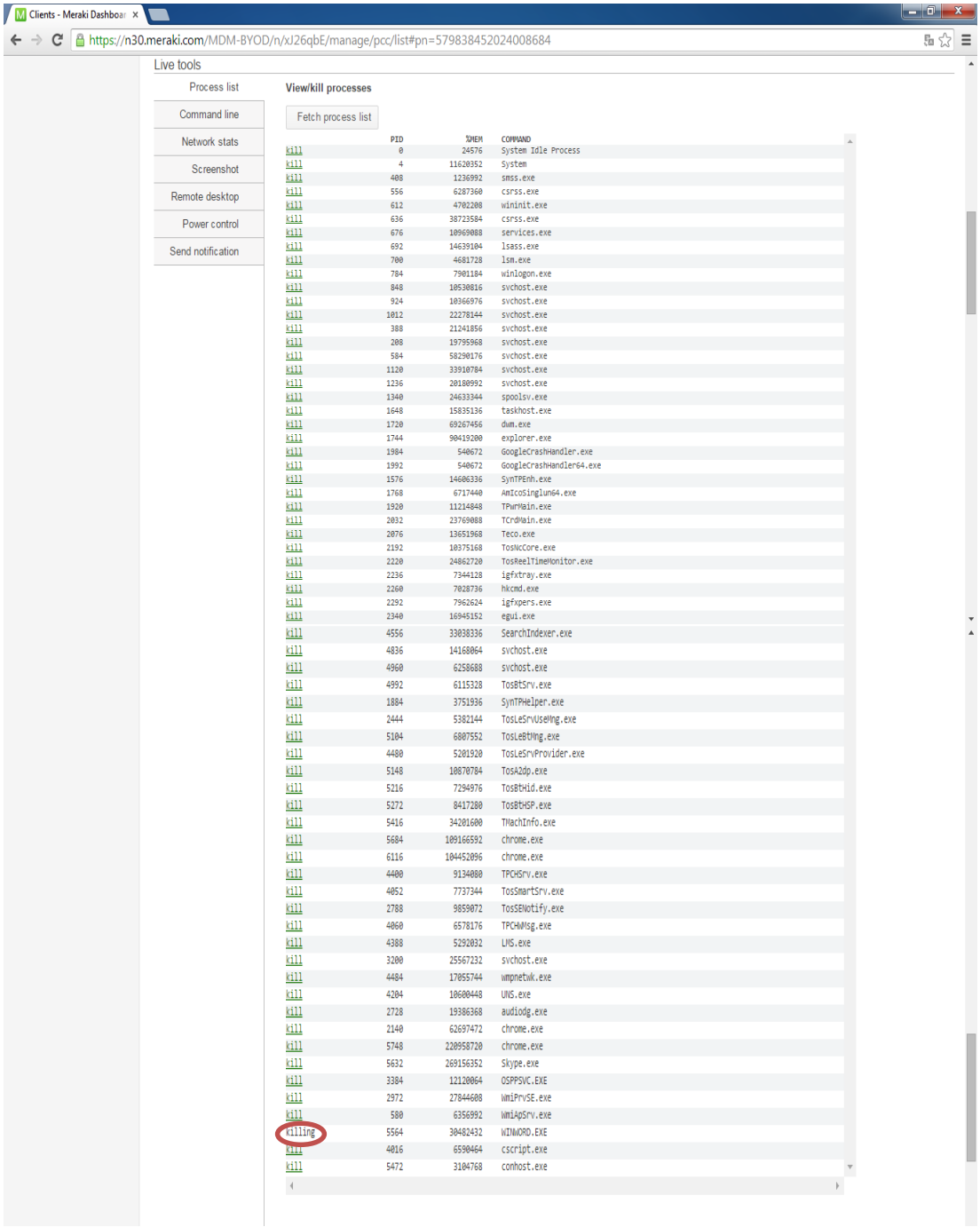
Anexo 35. Resumen de resultados de la encuesta 2.

RESULTADOS DE LAS PREGUNTAS REALIZADAS EN LA ENCUESTA				
1. ¿Con cuántos dispositivos usted se conectó a la red BYOD?	Un dispositivo 64	Dos dispositivos 8	Tres dispositivos 4	
2. ¿Qué tipo de dispositivo/s utilizó usted para conectarse?	Smartphone 45	Tablet 15	Laptop 16	
3. ¿Cuál es el sistema operativo de su/sus dispositivo/s?	Android 44	iOS 16	Windows 16	
4. Al momento que se conectó a la red BYOD_invitados tuvo problemas.	Si 3	No 73		
5. ¿A qué red inalámbrica o SSID permaneció conectado?	BYOD Invitados 20	BYOD Estudiantes 21	BYOD Docentes 18	BYOD Administrativos 17
6. Cuando se cambió de red tuvo problemas para conectarse.	Si 17	No 59		
7. El acceso a la red es:	Simple 67	Complicado 9		
8. Fue enviado a un sitio de remediación de antivirus.	Si 15	No 61		
9. El enrolamiento en la red es:	Rápido 54	Lento 22		
10. ¿Cuál es la velocidad de su conexión o ancho de banda?	1 Mbps 27	2 Mbps 19	3 Mbps 21	Ilimitado 9
11. La navegación te pareció:	Rápida 59	Lenta 17		
12. Accede a este enlace http://www.sidar.org/traducciones/wcag20/es/ La carga de la página fue:	Rápida 57	Lenta 19		
13. Al reproducir un video fue:	Rápido 51	Lento 25		
14. Se logró descargar un archivo:	Si 50	No 26		
15. La descarga del archivo fue:	Rápida 28	Lenta 20		
16. Al cambiarse de política los cambios fueron notorios.	Si 33	No 43		
17. Él envió de notificaciones fue satisfactorio.	Si 50	No 26		
18. Su dispositivo fue localizado.	Si 51	No 25		
19. Él envió de app a su dispositivo fue satisfactorio.	Si 60	No 16		
20. En las aplicaciones en tiempo real, su funcionamiento fue:	Bueno 57	Malo 19		
21. Al desconectar o apagar el equipo y volver a conectarse a la red la conexión a la red tuvo problemas.	Si 12	No 64		
22. Recomendaría usted implementarse BYOD en la Universidad.	Si 72	No 4		
23. Qué tipo de recomendación usted podría hacer con respecto a la red.	• Ninguna. • Aumentar la velocidad. • Sin restricciones. • Aplicarse en la universidad. • Eficiencia en la conexión.			

Elaborado por: Andrea Díaz y Danilo Lamar.

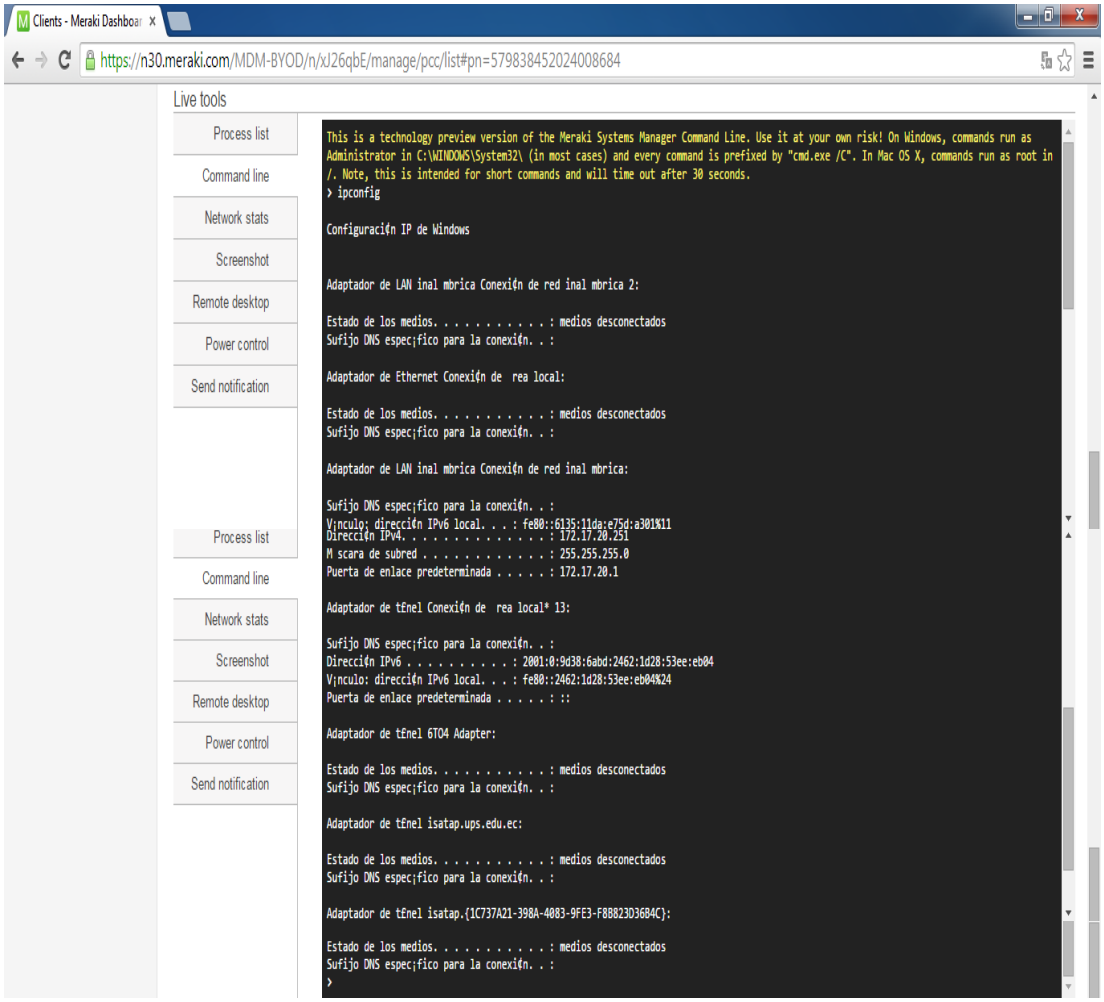
Anexo 36. Lista de Procesos.

Con esta herramienta se puede terminar un proceso que se esté ejecutando en un cliente. A continuación un ejemplo el cual se está eliminando el proceso de WINDWORD.EXE, con esto se cierra el programa de WORD en el cliente.



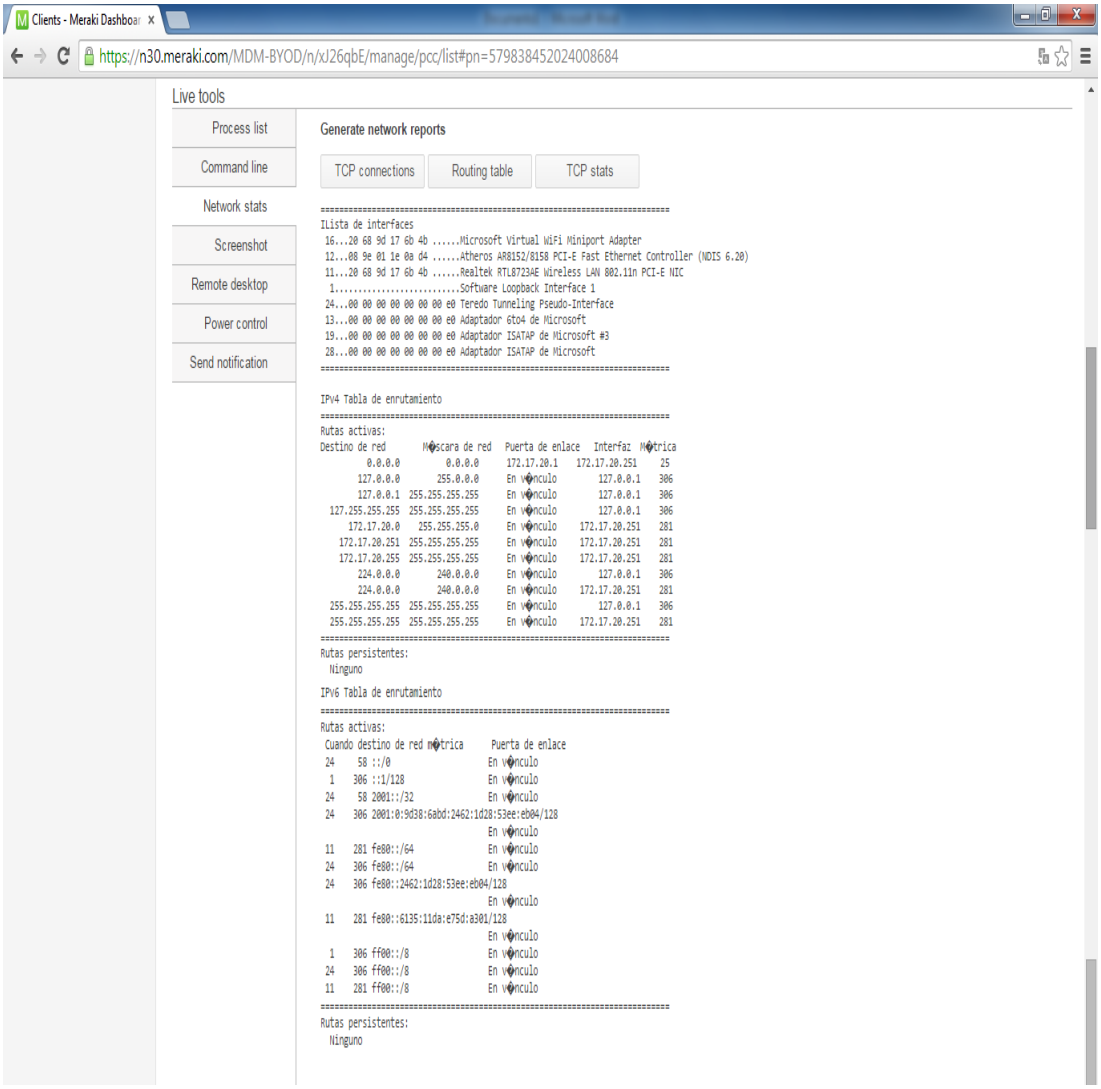
Anexo 37. Línea de Comandos.

Esta herramienta permite ejecutar comandos en un cliente remoto. A continuación se muestra un ejemplo.



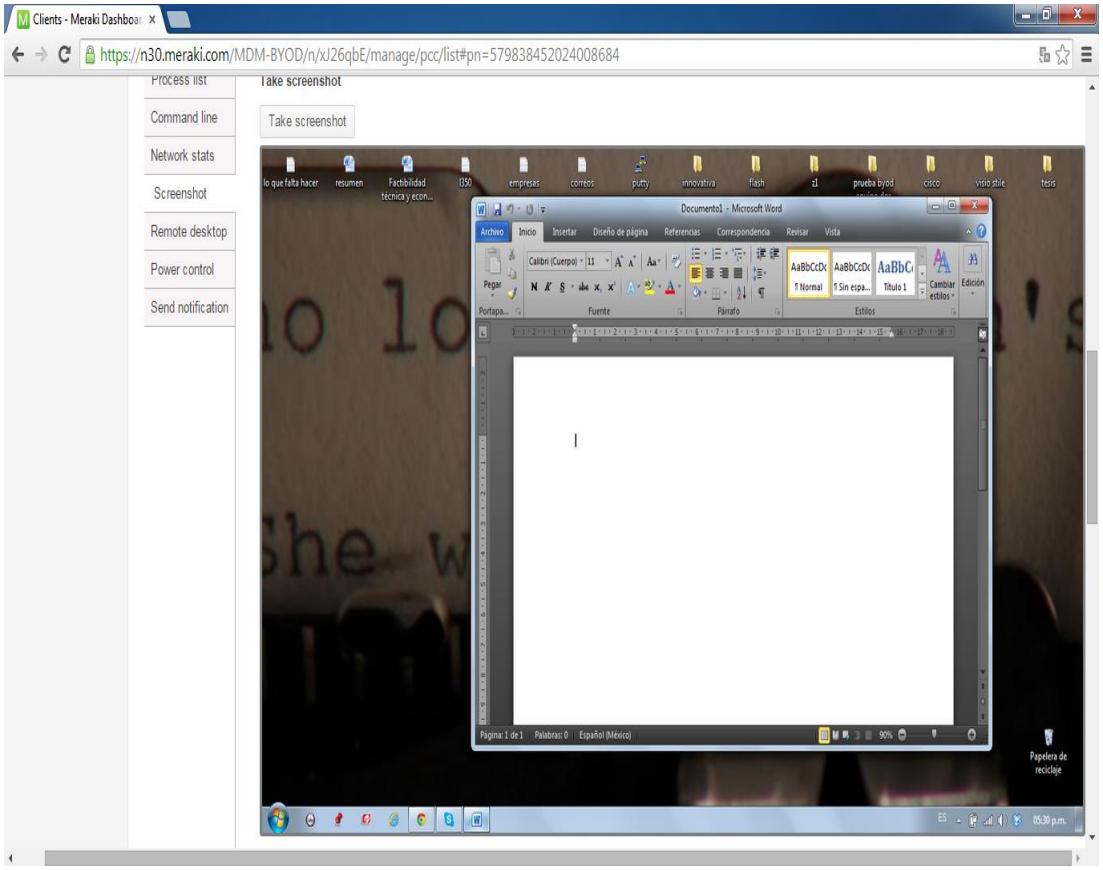
Anexo 38. Reportes de Red.

Esta herramienta brinda la facilidad de saber las conexiones TCP del cliente, su tabla de ruteo y sus estadísticas TCP. A continuación se muestra la tabla de ruteo del cliente.



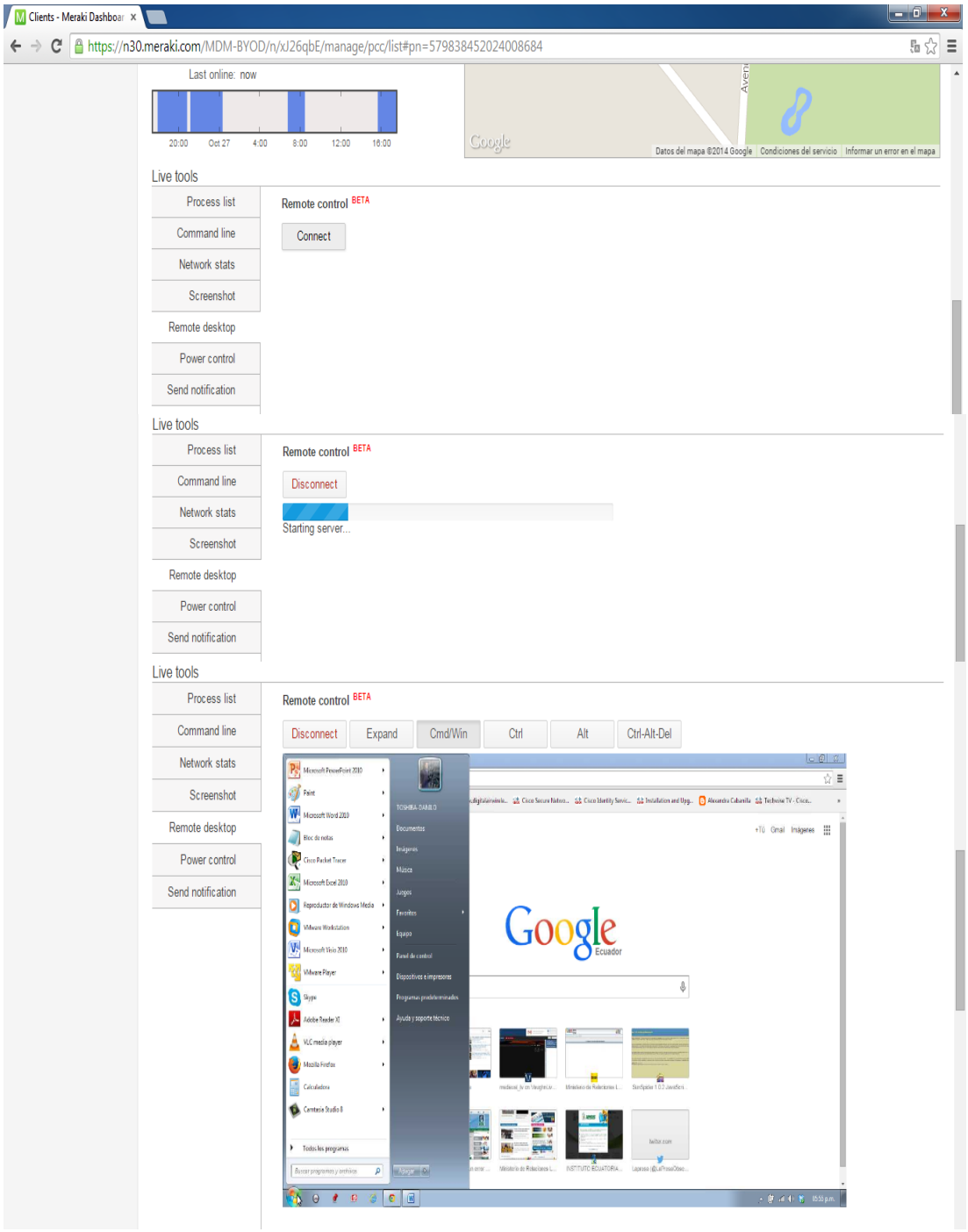
Anexo 39. Captura de Pantalla.

Con esta herramienta el administrador de la red puede realizar capturas de pantalla de los usuarios sin que estos se den cuenta. A continuación se muestra un ejemplo.



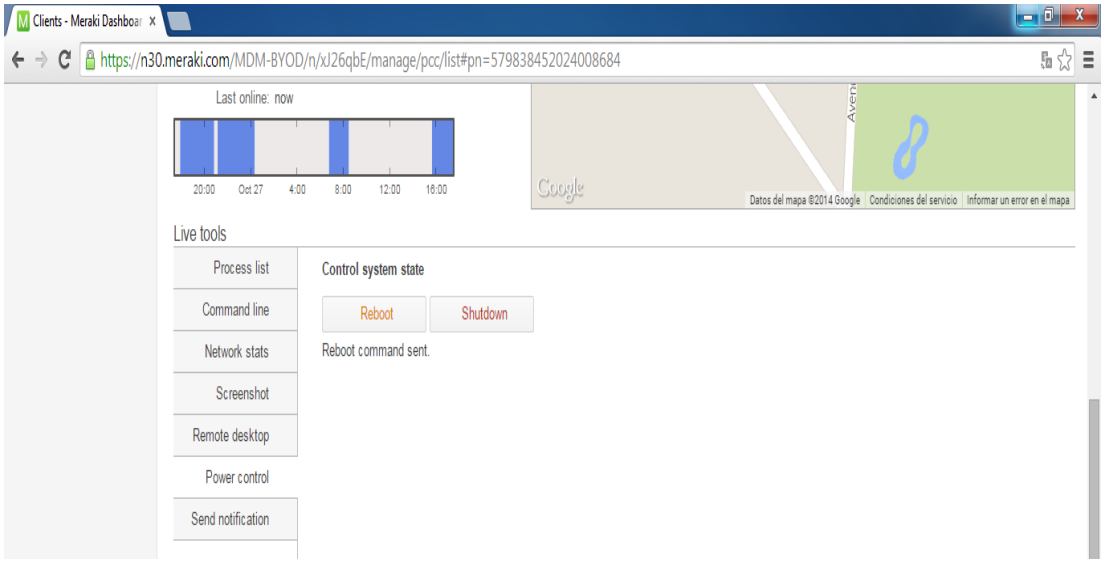
Anexo 40. Escritorio Remoto.

Esta herramienta permite al administrador de red conectarse al computador de un cliente desde su ubicación y realizar varias tareas sobre este dispositivo. A continuación se muestra un ejemplo.



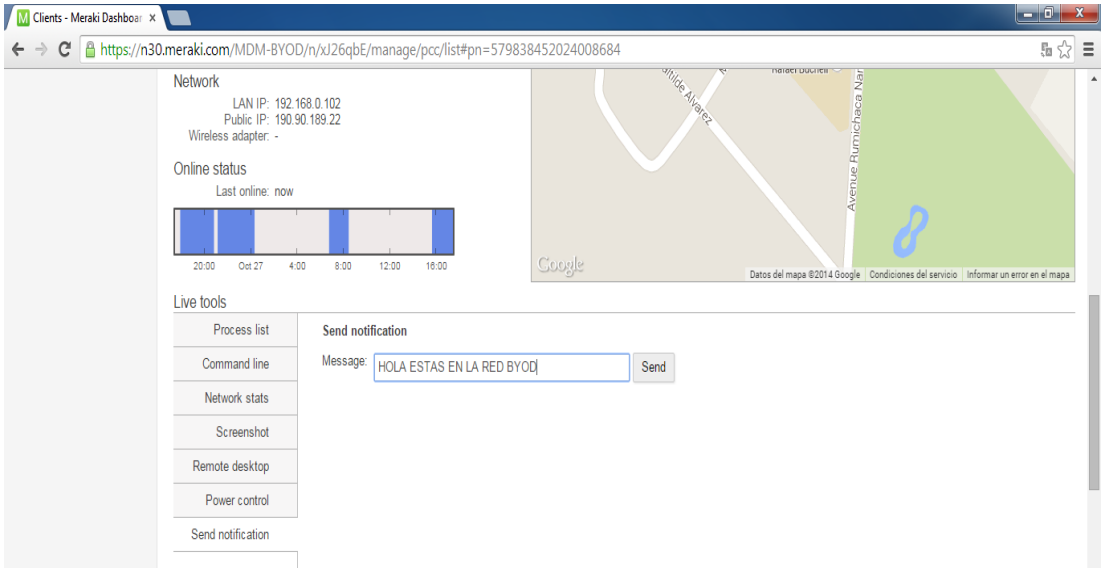
Anexo 41. Control de Encendido.

La utilización de esta herramienta permite reiniciar o apagar a cualquier equipo del usuario que este unido a la red MDM BYOD.

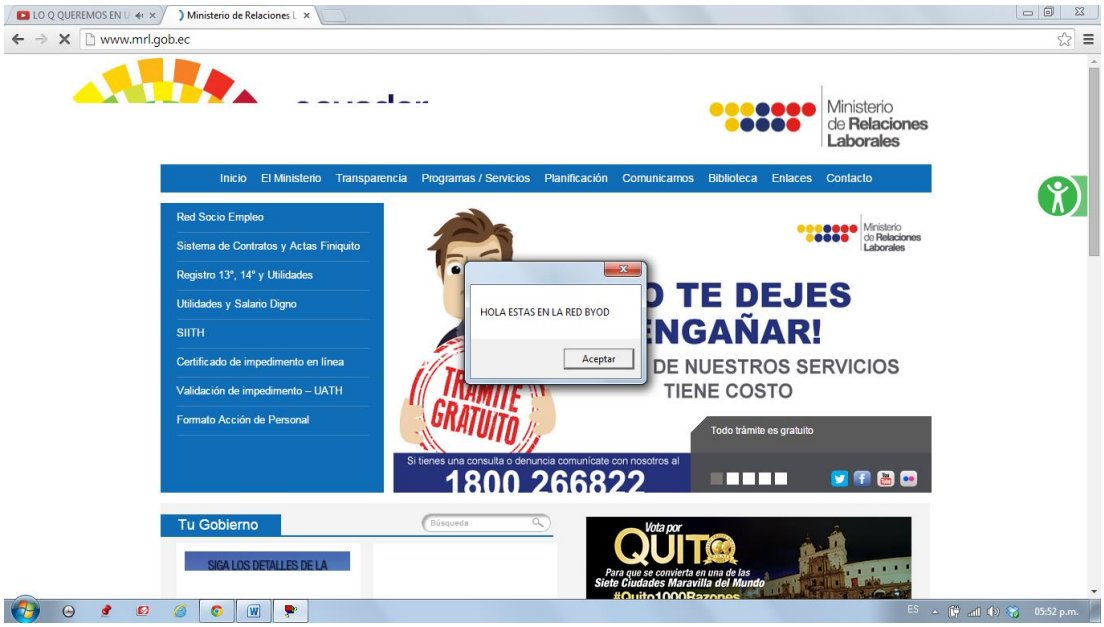


Anexo 42. Envió de Notificaciones.

La utilización de esta herramienta permite enviar mensajes a los usuarios, los cuales podrán ser notificados por el administrador de red si se va a sufrir de algún cambio en la red u otra información de interés para el cliente o el administrador.

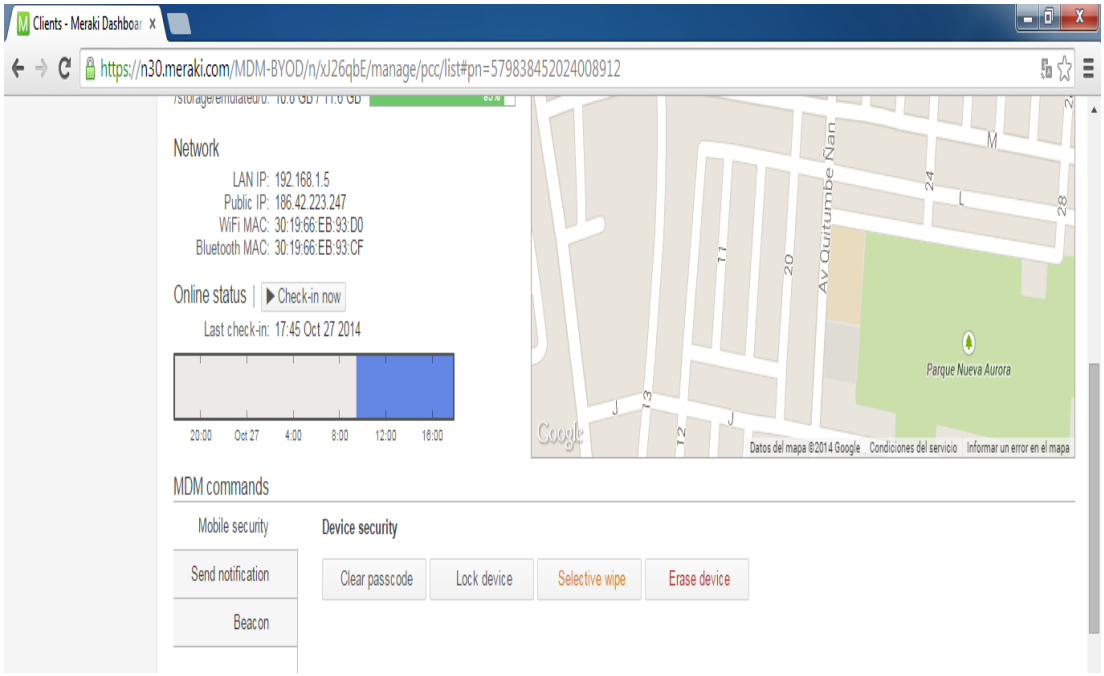


Aquí se puede observar que el mensaje le llegó satisfactoriamente al cliente.



Anexo 43. Seguridad Móvil.

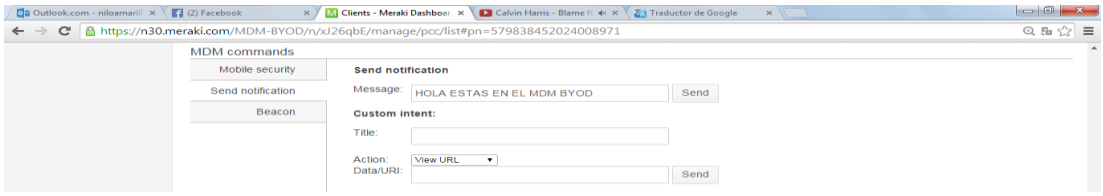
Esta herramienta es utilizada para los dispositivos como son: celulares o Tablet, y tiene algunas funciones de seguridad como se muestra a continuación.



Anexo 44. Envió de Notificaciones.

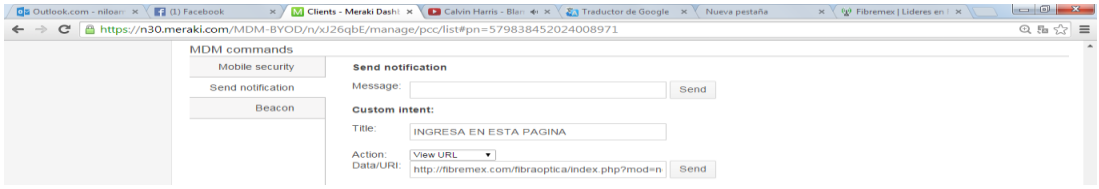
Esta herramienta permite enviar mensajes a los dispositivos móviles. A continuación se muestran dos ejemplos de notificación.

Notificación simple.

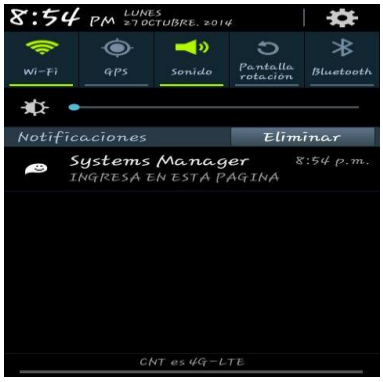


Verificación en el cliente.

Notificación con contenido.



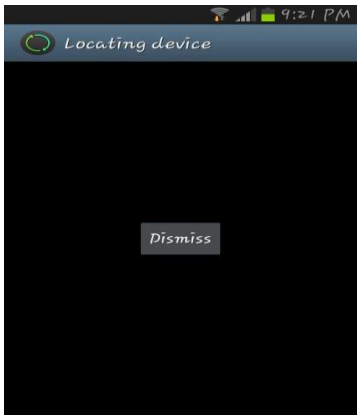
Verificación en el cliente y el contenido al que accedió en este caso la URL enviada.



Anexo 45. Localización de dispositivo.

Esta herramienta permite localizar el dispositivo del cliente, mediante una alarma que se enviará al dispositivo durante un tiempo determinado. A continuación se muestra su funcionamiento.

Verificación en el dispositivo del cliente.



Anexo 46 Cotización Propuesta.

Configset ID:	**10534617**
Configset Name:	**BYOD Universidad Salesina**
Created On:	**27 oct 2014**
Created By:	[redacted]
Last Update On:	**28 oct 2014**
Last Update By:	[redacted]
Main Currency:	**USD**
Price List:	**Global PriceList-Latin America**

ITEM	PARTE	DESCRIPCION	GARANTIA	INCLUIDO	CANTIDAD	PVP
1.0	**SNS-3415-K9**	Small Secure Network Server for ISE NAC & ACS Applications	N/A	No	1	$ -
1.0.1	CON-SNT-SNS3415	SMARTNET 8X5XNBD Small Secure Network	12 month(s)	No	1	$ 2,129.54
1.1	CAB-9K12A-NA	Power Cord 125VAC 13A NEMA 5-15 Plug North America	N/A	No	1	$ -
1.2	SNS-N2XX-ABPCI01	Broadcom 5709 Dual Port 10/100/1Gb NIC w /TOE iSCSI	N/A	Yes	1	$ -
1.3	SNS-UCS-TPM	Trusted Platform Module for UCS servers	N/A	Yes	1	$ -
1.4	SNS-RAID-ROM5	Embedded SW RAID 0/1/10 8 ports SAS/SATA	N/A	Yes	1	$ -
1.5	SNS-CPU-2609-E5	2.4 GHz E5-2609/80W 4C/10MB Cache/DDR3 1600MHz	N/A	Yes	1	$ -
1.6	SNS-4GBSR-1X041RY	4GB 1600 Mhz Memory Module	N/A	Yes	4	$ -
1.7	SNS-650W-PSU	650W power supply for C-series rack servers + cord (configur	N/A	Yes	1	$ -
1.8	SNS-600GB-HDD	600 GB Hard Disk Drive	N/A	Yes	1	$ -
1.9	SW-3415-ISE-K9	Cisco ISE Software version 1.2.1 for the SNS-3415-K9	N/A	No	1	$ 10,148.04
1.10	ISE-SNS-ACCYKIT	ISE SNS Accessory Kit	N/A	Yes	1	$ -
						$ -
2.0	**L-ISE-BSE-1k=**	Cisco Identity Services Engine 1k EndPoint Base License	N/A	No	1	$ 3,352.99
						$ -
3.0	**L-ISE-ADV-S-1k=**	Cisco ISE 1k EndPoint Advanced Subscription License	N/A	No	1	$ -
3.0.1	ISE-ADV-5YR-1k	Cisco ISE 5-Yr 1k EndPoint Advanced License	60 month(s)	No	1	$ 32,547.99
						$ -
4.0	**ASA5555-2SSD120-K9**	NGFW ASA 5555-X w / SW 8GE Data 1GE Mgmt AC 3DES/AES 2 SSD120	N/A	No	1	$ 10,355.53
4.0.1	CON-SNT-A55SDK9	SMARTNET 8X5XNBD ASA 5555-X with SW8	12 month(s)	No	1	$ 4,051.53
4.1	SF-ASA-CX-9.2-K8	ASA 5500 Series CX Software v9.2.1	N/A	Yes	1	$ -
4.2	ASA5555AWI5Y	ASA 5555-X AVCWSE IPS 5 Year	N/A	No	1	$ 8,726.49
4.3	SF-ASA-X-9.1.3-K8	ASA 9.1.3 Software image for ASA 5500-X Series5585-XASA-SM	N/A	Yes	1	$ -
4.4	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	N/A	No	1	$ -
4.5	ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows Solaris Linux Mac)	N/A	Yes	1	$ -
4.6	ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	N/A	Yes	1	$ -
4.7	ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client + Cisco Security Desktop Software	N/A	Yes	1	$ -
4.8	ASA5555-MB	ASA 5555 IPS Part Number with which PCB Serial is associated	N/A	Yes	1	$ -
4.9	ASA-PWR-AC	ASA 5545-X/5555-X AC Power Supply	N/A	Yes	1	$ -
4.10	ASA5500X-SSD120INC	ASA 5512-X through 5555-X 120GB MLC SED SSD (Incl.)	N/A	Yes	2	$ -
4.11	ASA-PWR-BLANK	ASA 5545-X/5555-X Power Slot Blank Cover	N/A	Yes	1	$ -
4.12	ASA-IC-6GE-SFP-C	ASA 5545-X/5555-X Interface Card 6-port GE SFP (SXLHLX)	N/A	No	1	$ 5,078.25
4.12.0.1	CON-SNT-ASASFC1	SMARTNET 8X5XNBD ASA 5545-X/5555-X In	12 month(s)	No	1	$ 928.13
4.13	GLC-LH-SMD	1000BASE-LX/LH SFP transceiver module MMF/SMF 1310nm DOM	N/A	No	2	$ 1,684.29
						$ -
5.0	**AIR-CT5508-50-K9**	5508 Series Controller for up to 50 APs	N/A	No	1	$ 19,039.21
5.0.1	CON-SNT-CT5508	SMARTNET 8X5XNBD 5508 Series Controller for up to 50 APs	12 month(s)	No	1	$ 3,769.23
5.1	SWC5500K9-76	Cisco Unified Wireless Controller SW Release 7.6	N/A	No	1	$ -
5.2	AIR-PWR-CORD-NA	AIR Line Cord North America	N/A	Yes	1	$ -
5.3	PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE	N/A	Yes	1	$ -
5.4	LIC-CT5508-BASE	Base Software License	N/A	Yes	1	$ -
5.5	LIC-CT5508-50	50 AP Base license	N/A	Yes	1	$ -
						$ -
6.0	**AIR-CAP3702I-A-K9**	802.11ac Ctrlr AP 4x4:3SS w /CleanAir; Int Ant; A Reg Domain	N/A	No	19	$ 24,041.28
6.0.1	CON-SNT-3702IA	SMARTNET 8X5XNBD 802.11ac Ctrlr AP 4x	12 month(s)	No	19	$ 1,469.54
6.1	AIR-AP-BRACKET-1	802.11n AP Low Profile Mounting Bracket (Default)	N/A	No	19	$ -
6.2	SWAP3700-RCOVRY-K9	Cisco 3700 Series IOS WIRELESS LAN RECOVERY	N/A	No	19	$ -
6.3	AIR-AP-T-RAIL-R	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	N/A	No	19	$ -
						$ -
7.0	**WS-C3750G-48TS-E**	Catalyst 3750G 48 Port Data IP Base	N/A	No	6	$ 51,074.70
7.0.1	CON-SNT-3750X4TS	SMARTNET 8X5XNBD Catalyst 3750G 48 Port Data IP Base	12 month(s)	No	6	$ 5,336.70
7.1	CAB-3KX-AC	AC Power Cord for Catalyst 3K-X (North America)	N/A	No	6	$ -
7.3	S375XVK9T-15002SE	CAT 3750G IOS UNIVERSAL WITH WEB BASE DEV MGR	N/A	No	6	$ -
7.4	CAB-STACK-50CM	Cisco StackWise 50CM Stacking Cable	N/A	Yes	6	$ -
7.5	CAB-SPWR-30CM	Catalyst 3750G and 3850 Stack Power Cable 30 CM	N/A	Yes	6	$ -
7.6	C3KX-PWR-350WAC	Catalyst 3K-G 350W AC Power Supply	N/A	Yes	6	$ -
						$ -
				Equipos y Licencias		**$ 183,733.41**
				Instalacion y configuracion		**$ 45,933.35**
				Subtotal		**$ 229,666.76**
				Iva		**$ 27,560.01**
				Total		**$ 257,226.77**

Anexo 47. Cotización equipamiento completo.

Configset ID:	**10534617**
Configset Name:	**BYOD Universidad Salesina**
Created On:	**27 oct 2014**
Created By:	[redacted]
Last Update On:	**28 oct 2014**
Last Update By:	[redacted]
Main Currency:	**USD**
Price List:	**Global PriceList-Latin America**

ITEM	PARTE	DESCRIPCION	GARANTIA	INCLUIDO	CANTIDA	PVP
1.0	**SNS-3415-K9**	Small Secure Network Server for ISE NAC & ACS Applications	N/A	No	1	$ -
1.0.1	CON-SNT-SNS3415	SMARTNET 8X5XNBD Small Secure Network	12 month(s)	No	1	$ 2,129.54
1.1	CAB-9K12A-NA	Power Cord 125VAC 13A NEMA 5-15 Plug North America	N/A	No	1	$ -
1.2	SNS-N2XX-ABPCI01	Broadcom 5709 Dual Port 10/100/1Gb NIC w/TOE iSCSI	N/A	Yes	1	$ -
1.3	SNS-UCS-TPM	Trusted Platform Module for UCS servers	N/A	Yes	1	$ -
1.4	SNS-RAID-ROM5	Embedded SW RAID 0/1/10 8 ports SAS/SATA	N/A	Yes	1	$ -
1.5	SNS-CPU-2609-E5	2.4 GHz E5-2609/80W 4C/10MB Cache/DDR3 1600MHz	N/A	Yes	1	$ -
1.6	SNS-4GBSR-1X041RY	4GB 1600 Mhz Memory Module	N/A	Yes	4	$ -
1.7	SNS-650W-PSU	650W power supply for C-series rack servers + cord (configur	N/A	Yes	1	$ -
1.8	SNS-600GB-HDD	600 GB Hard Disk Drive	N/A	Yes	1	$ -
1.9	SW-3415-ISE-K9	Cisco ISE Software version 1.2.1 for the SNS-3415-K9	N/A	No	1	$ 10,148.04
1.10	ISE-SNS-ACCYKIT	ISE SNS Accessory Kit	N/A	Yes	1	$ -
						$ -
2.0	**L-ISE-BSE-2500=**	Cisco Identity Services Engine 2500 EndPoint Base License	N/A	No	1	$ 10,568.25
						$ -
3.0	**L-ISE-ADV-S-2500=**	Cisco ISE 2500 EndPoint Advanced Subscription License	N/A	No	1	$ -
3.0.1	ISE-ADV-5YR-2500	Cisco ISE 5-Yr 2500 EndPoint Advanced License	60 month(s)	No	1	$ 110,486.25
						$ -
4.0	**ASA5555-2SSD120-K9**	NGFW ASA 5555-X w/ SW 8GE Data 1GE Mgmt AC 3DES/AES 2 SSD120	N/A	No	1	$ 22,170.79
4.0.1	CON-SNT-A55SDK9	SMARTNET 8X5XNBD ASA 5555-X with SW8	12 month(s)	No	1	$ 4,051.53
4.1	SF-ASA-CX-9.2-K8	ASA 5500 Series CX Software v9.2.1	N/A	Yes	1	$ -
4.2	ASA5555AWI5Y	ASA 5555-X AVCWSE IPS 5 Year	N/A	No	1	$ 40,626.00
4.3	SF-ASA-X-9.1.3-K8	ASA 9.1.3 Software image for ASA 5500-X Series5585-XASA-SM	N/A	Yes	1	$ -
4.4	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	N/A	No	1	$ -
4.5	ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows Solaris Linux Mac)	N/A	Yes	1	$ -
4.6	ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	N/A	Yes	1	$ -
4.7	ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client + Cisco Security Desktop Software	N/A	Yes	1	$ -
4.8	ASA5555-MB	ASA 5555 IPS Part Number with which PCB Serial is associated	N/A	Yes	1	$ -
4.9	ASA-PWR-AC	ASA 5545-X/5555-X AC Power Supply	N/A	Yes	1	$ -
4.10	ASA5500X-SSD120INC	ASA 5512-X through 5555-X 120GB MLC SED SSD (Incl.)	N/A	Yes	2	$ -
4.11	ASA-PWR-BLANK	ASA 5545-X/5555-X Power Slot Blank Cover	N/A	Yes	1	$ -
4.12	ASA-IC-6GE-SFP-C	ASA 5545-X/5555-X Interface Card 6-port GE SFP (SXLHLX)	N/A	No	1	$ 5,078.25
4.12.0.1	CON-SNT-ASASFC1	SMARTNET 8X5XNBD ASA 5545-X/5555-X In	12 month(s)	No	1	$ 928.13
4.13	GLC-LH-SMD	1000BASE-LX/LH SFP transceiver module MMF/SMF 1310nm DOM	N/A	No	2	$ 1,684.29
						$ -
5.0	**AIR-CT5508-50-K9**	5508 Series Controller for up to 50 APs	N/A	No	1	$ 19,039.21
5.0.1	CON-SNT-CT5508	SMARTNET 8X5XNBD 5508 Series Controller for up to 50 APs	12 month(s)	No	1	$ 3,769.23
5.1	SWC5500K9-76	Cisco Unified Wireless Controller SW Release 7.6	N/A	No	1	$ -
5.2	AIR-PWR-CORD-NA	AIR Line Cord North America	N/A	Yes	1	$ -
5.3	PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE	N/A	Yes	1	$ -
5.4	LIC-CT5508-BASE	Base Software License	N/A	Yes	1	$ -
5.5	LIC-CT5508-50	50 AP Base license	N/A	Yes	1	$ -
						$ -
6.0	**AIR-CAP3702I-A-K9**	802.11ac Ctrlr AP 4x4:3SS w/CleanAir; Int Ant; A Reg Domain	N/A	No	19	$ 24,041.28
6.0.1	CON-SNT-3702IA	SMARTNET 8X5XNBD 802.11ac Ctrlr AP 4x	12 month(s)	No	19	$ 1,469.54
6.1	AIR-AP-BRACKET-1	802.11n AP Low Profile Mounting Bracket (Default)	N/A	No	19	$ -
6.2	SWAP3700-RCOVRY-K9	Cisco 3700 Series IOS WIRELESS LAN RECOVERY	N/A	No	19	$ -
6.3	AIR-AP-T-RAIL-R	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	N/A	No	19	$ -
						$ -
7.0	**WS-C3750X-48T-S**	Catalyst 3750X 48 Port Data IP Base	N/A	No	14	$ 136,266.38
7.0.1	CON-SNT-3750X4TS	SMARTNET 8X5XNBD Catalyst 3750X 48 Port Data IP Base	12 month(s)	No	14	$ 12,452.35
7.1	CAB-3KX-AC	AC Power Cord for Catalyst 3K-X (North America)	N/A	No	14	$ -
7.2	C3KX-NM-1G	Catalyst 3K-X 1G Network Module option PID	N/A	No	14	$ 5,924.63
7.3	S375XVK9T-15002SE	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	N/A	No	14	$ -
7.4	CAB-STACK-50CM	Cisco StackWise 50CM Stacking Cable	N/A	Yes	14	$ -
7.5	CAB-SPWR-30CM	Catalyst 3750X and 3850 Stack Power Cable 30 CM	N/A	Yes	14	$ -
7.6	C3KX-PWR-350WAC	Catalyst 3K-X 350W AC Power Supply	N/A	Yes	14	$ -
						$ -
8.0	**WS-C2960X-48TS-L**	Catalyst 2960-X 48 GigE 4 x 1G SFP LAN Base	N/A	No	7	$ 24,853.80
8.0.1	CON-SNT-WSC248TS	SMARTNET 8X5XNBD Catalyst 2960-X 48 G	12 month(s)	No	7	$ 2,273.91
8.1	CAB-16AWG-AC	AC Power cord 16AWG	N/A	No	7	$ -
						$ -
9.0	**WS-C6506-E**	Catalyst 6500 Enhanced 6-slot chassis 12RU no PS no Fan Tray	N/A	No	1	$ 4,655.06
9.0.1	CON-SNT-WS-C6506	8x5xNBD ServiceCatalyst 6506	12 month(s)	No	1	$ 7,106.61
9.1	WS-C6506-E-FAN	Catalyst 6506-E Chassis Fan Tray	N/A	No	1	$ 418.96
9.2	CONNECTOR-KIT	Connector Kit	N/A	No	1	$ -
9.3	VS-S2T-10G	Cat 6500 Sup 2T with 2 x 10GbE and 3 x 1GbE with MSFC5 PFC4	N/A	No	1	$ 23,698.50
9.4	MEM-C6K-INTFL1GB	Internal 1G Compact Flash	N/A	Yes	1	$ -
9.5	MEM-SUP2T-2GB	Catalyst 6500 2GB memory for Sup2T and Sup2TXL	N/A	Yes	1	$ -
9.6	VS-F6K-PFC4	Cat 6k 80G Sys Daughter Board Sup2T PFC4	N/A	Yes	1	$ -
9.7	VS-SUP2T-10G	Catalyst 6500 Supervisor Engine 2T Baseboard	N/A	Yes	1	$ -
9.8	S2TIBK9-15102SY	Cisco CAT6000-VS-S2T IOS IP BASE FULL ENCRYPT	N/A	No	1	$ -
9.9	WS-X6748-SFP	Catalyst 6500 48-port GigE Mod: fabric-enabled (Req. SFPs)	N/A	No	1	$ 21,159.38
9.10	MEM-XCEF720-256M	Catalyst 6500 256MB DDR xCEF720 (67xx interface DFC3A)	N/A	No	1	$ -
9.11	WS-F6700-CFC	Catalyst 6500 Central Fwd Card for WS-X67xx modules	N/A	No	1	$ -
9.12	GLC-SX-MMD	1000BASE-SX SFP transceiver module MMF 850nm DOM	N/A	No	28	$ 11,849.25
9.13	WS-X6748-GE-TX	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled RJ-45	N/A	No	1	$ 12,695.63
9.14	MEM-XCEF720-256M	Catalyst 6500 256MB DDR xCEF720 (67xx interface DFC3A)	N/A	No	1	$ -
9.15	WS-F6700-CFC	Catalyst 6500 Central Fwd Card for WS-X67xx modules	N/A	No	1	$ -
9.16	WS-CAC-4000W-US	4000Watt AC Power Supply for US (cable attached)	N/A	No	2	$ 8,463.75
						$ -
10.0	**GLC-SX-MMD=**	1000BASE-SX SFP transceiver module MMF 850nm DOM	N/A	No	28	$ 11,849.25
						$ -
				Equipos y Licencias		$ 539,857.75
				Instalacion y configuracion		$ 134,964.44
				Subtotal		$ 674,822.19
				Iva		$ 80,978.66
				Total		$ 755,800.85