PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

"ANÁLISIS Y PROPUESTA DE IMPLEMENTACION Y APLICACIÓN DE MDM EN LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES."

JORGE RAMIRO VALLEJO BASANTES

TRABAJO PREVIO LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN REDES DE COMUNICACIÓN

QUITO – NOVIEMBRE 2016

Dedicatoria

La concepción de este proyecto está dedicada a mi familia, pilar fundamental en mi vida. Sin el apoyo brindado por ellos no hubiera podido llegar a alcanzar esta meta. Así como también a todas las personas que de una u otra manera fueron parte de mi vida en esta etapa.

Jorge Ramiro Vallejo Basantes

Agradecimientos

En primer lugar a Dios por haberme guidado en cada uno de los pasos que he dado hasta poder llegar a la culminación del presente proyecto, a mi esposa a mis hijos por ser las personitas que me han dado fuerza y apoyo incondicional, en si a toda la familia. Un agradecimiento especial a mi Director de Tesis Dr. Gustavo Chafla, por el apoyo prestado durante el proceso de desarrollo de la misma.

INDICE GENERAL

INDICE FIGURAS

INDICE TABLAS

INDICE ECUACIONES

ABSTRACTO

En los últimos años, la popularidad de los dispositivos móviles como teléfonos inteligentes y tabletas ha aumentado de manera exponencial. Debido a que estos dispositivos se pueden utilizar en cualquier lugar, la han convertido en algo común en el lugar de trabajo en todos los sectores, incluidos los entornos institucionales, como la Agencia de Regulación y Control de las Telecomunicaciones. Cuando los Funcionarios tienen dispositivos inteligentes, que requieren por consiguiente el acceso a la red corporativa. Con el fin de hacer frente a sus necesidades de conexión, una tecnología llamada de gestión de dispositivos móviles (MDM) ha aparecido y se ha vuelto muy popular en todo el mundo en el último par de años. MDM proporciona una serie de beneficios como ayudar a aumentar la productividad y la eficiencia de los funcionarios, sin embargo se tienen inconvenientes como lo es la inversión que tiene que ser hecho por la empresa.

El objetivo de este trabajo es presentar un Análisis y propuesta de implementación y Aplicación de MDM y la Gestión de Red, con la finalidad de ver si es o no es una buena idea para la ARCOTEL adoptar una solución MDM. En la actualidad, la ARCOTEL utiliza Microsoft Exchange para dar cierto grado de gestión de dispositivos de manera que la mayoría de sus funcionarios pueden acceder a su correo electrónico corporativo. El software también ofrece la alternativa de limpieza remota en el caso de que un dispositivo ha sido robado. En el análisis efectuado también se evaluó la situación actual para determinar sus costos, beneficios y lo más importante, su retorno de la inversión. Estos resultados se compararon con el retorno de la inversión obtenido utilizando los costos y beneficios de las tres empresas que ofrecen alternativas de MDM para determinar cuál tiene el mayor retorno de la inversión. Tras el análisis de los valores de retorno de la inversión, se determinó que la mejor opción para la ARCOTEL en este momento es mantener el sistema que actualmente mantiene.

INTRODUCCIÓN

La administración de dispositivos móviles es muy importante para los usuarios y las organizaciones, debido a que con estas funciones se pueden realizar diferentes tareas como apagar, reiniciar, restablecer, entre otras funciones que permiten el manejo del dispositivo móvil.

Un sistema de gestión de dispositivos móviles (MDM) administra tos dispositivos móviles, como teléfonos inteligentes y tabletas. Es así que la evolución de las redes móviles permiten la transmisión de voz y datos, en conjunto con una creciente capacidad de procesamiento, lo cual ha permitido que los Smartphone o teléfonos inteligentes posean el equipamiento necesario para ejecutar múltiples tareas, desde entretenimiento hasta productividad, a través de la instalación de software especializado y adaptado para las pantallas y características de los equipos, mejor conocidas como aplicaciones móviles. Las soluciones MDM trabajan monitoreando su estado y controlando sus funciones de forma remota. A través de las soluciones de MDM, grandes cantidades de dispositivos pueden ser administrados simultáneamente, de modo que la configuración de este tipo de sistema no tome mucho tiempo. MDM apareció para cubrir la necesidad de las empresas para controlar los dispositivos que se estaban conectando a su red y para mejorar la eficiencia y la seguridad, como también la disminución de los costos por usos de red y tiempo de inactividad.

En los últimos años el uso de dispositivos móviles como teléfonos inteligentes y tabletas ha aumentado de manera exponencial y por sus características, estos dispositivos se utilizan en todas partes incluyendo el lugar de trabajo. La popularidad de estos dispositivos ha propuesto nuevos retos para las empresas, puesto que los trabajadores están conectando los dispositivos móviles que no son sólo propiedad de la compañía, sino también dispositivos personales a la red de la empresa. El uso de varios dispositivos en la red de la empresa puede

ser problemático y complejo. Para hacer frente a los problemas causados por la proliferación de los teléfonos inteligentes y tabletas, algunos proveedores han desarrollado sistemas llamados administración de dispositivos móviles (MDM por sus siglas en ingles). Soluciones MDM pueden ser aplicados en diferentes industrias y mercados, entre ellos un ambiente como lo es la institución pública.

Por otro lado, se ve necesaria la actualización a tecnologías de última generación de las redes inalámbricas, para la plena adopción de las aplicaciones móviles, ya que muchas de las cuales requieren de una conexión a Internet para que los usuarios exploten todos sus beneficios.

ANTECEDENTES

A un dispositivo móvil se lo puede definir como una pequeña computadora, de propósitos generales, programable, alimentado por batería que es capaz de manejar el inicio de una aplicación móvil tales como la navegación móvil en Internet y que puede ser operada de manera cómoda mientras se sostiene con una mano y permite a los usuarios móviles la interacción directa con aplicaciones móviles, es así que el fondo de MDM contiene dos aspectos importantes, la administración de dispositivos móviles y la información sobre el cliente.

Algunas de las características más importantes de la administración de dispositivos móviles (MDM) son las siguientes:

Diversidad de Dispositivos y Plataformas: La movilidad para los usuarios de telecomunicaciones ha tenido un papel relevante, actualmente al observarse que la telefonía móvil está rompiendo con todos los esquemas establecidos en las industrias, es por esto que una solución MDM tiene que ser capaz de soportar múltiples dispositivos a pesar de sus marcas y modelos. Esto es especialmente importante en entornos empresariales porque los dispositivos de los empleados no tienen uniformidad y todos ellos se conectan a la red corporativa.

Gestión de Inventario: El sistema tiene que ser capaz de determinar el número y tipo de dispositivos que los funcionarios de la Agencia de Regulación y Control de las Telecomunicaciones que se conectan a la red, incluida su ubicación, sistema operativo y la plataforma que utilizan. El sistema, además, tiene que apoyar la presentación de informes con el fin de determinar los problemas que pueden ocurrir con la disolución de MDM.

Seguridad: La solución MDM tiene que proporcionar seguridad a fin de garantizar que la información en las bases de datos de la Agencia de Regulación y Control de la Telecomunicaciones será protegida. La solución también tiene que evitar la fuga de datos

móviles y asegurarse de que los dispositivos no se verán afectados por el malware móvil que se está convirtiendo en un problema terrible ya que el número de ataques a la seguridad aumentan cada año, con lo cual se ha descubierto nuevas necesidades de las personas y las empresas por comunicarse y transmitir la información en cualquier momento y lugar de forma segura. El crecimiento exponencial del mercado de los dispositivos móviles a nivel mundial han empezado a generar una gran serie de amenazas para los usuarios de los mismos, uno de estos son los virus han migrado de los computadores personales y los servidores a estos dispositivos.

Perfiles Separados: El sistema MDM para la Institución debe soportar dos perfiles separados, uno personal y otro para la empresa. En caso de que el dispositivo sea borrado porque un empleado abandona la empresa, sólo la información de la empresa será eliminada y el usuario puede mantener su información personal intacta.

Gestión de aplicaciones móviles: MDM, además, tiene que proporcionar aplicaciones que se puedan descargar a través del perfil corporativo. Estas aplicaciones se pueden personalizar para cada empresa de manera que ayudan a aumentar la productividad de la misma. También, MDM puede tener la característica de la instalación masiva y cambios de aplicaciones como antivirus o firewalls.

Soporte: Con el fin de garantizar que la solución MDM está cumpliendo con las expectativas de la empresa y que está mejorando su productividad, las empresas que proporcionan la solución MDM tienen que dar apoyo sobre todo en las etapas de instalación y capacitación cuando los clientes están aprendiendo a utilizar el sistema.

JUSTIFICACIÓN

En países como España y Estados Unidos se ha documentado los beneficios que surgen de automatizar los procesos propios de administración de la empresa a través del uso de paquetes para la administración de relación con el cliente, o simplemente el uso de dispositivos móviles que permiten un ahorro semanal de 11.3 horas por empleado. En Canadá, la mayor adopción de dispositivos móviles (teléfonos inteligentes, tabletas, asistente personal digital) se contó en las empresas mineras, petroleras y gas con una penetración de 98.6%. El mayor uso de celulares (no teléfonos inteligentes), se registra en el de la construcción con 82.3%.

Según experiencia internacional refiere que con el uso de dispositivos móviles en el ámbito empresarial, se ha logrado movilizar a cerca del 75% de los empleados a través del uso de aplicaciones móviles consideradas de primera generación como correo o calendario. Adicionalmente, el uso de aplicaciones especializadas (o de segunda generación) aún es incipiente entre las Pequeñas y Medianas Empresas.

Cada vez el ecosistema que rodea a los dispositivos móviles, ha permitido que miles de desarrolladores utilicen la plataforma para la realización de aplicaciones que aprovechen la movilidad y los beneficios tecnológicos como la pantalla capacitiva, grabación de video y servicios de localización, entre otros. De aquí surge que los sistemas MDM sigan evolucionado y cada vez sean más fáciles de poner en práctica, puesto que en la actualidad el uso de esta aplicación tiene que ser descargado e instalado en todos los dispositivos que les permite conectarse al servidor que los administra. Las soluciones de MDM han aumentado en popularidad en los últimos años en todo el mundo y cada vez más empresas han desarrollado sus propias soluciones con características especiales de acuerdo a sus requerimientos. Como los sistemas de gestión de datos sólo requieren de una conexión a Internet para su funcionamiento, la empresa que proporciona puede estar ubicada en cualquier parte del

mundo, así como también los enlaces de comunicación son totalmente transparentes para el consumidor, lo cual actualmente se ve potenciado con la eficiencia de las redes móviles que soportan tráfico de voz y datos a mayor velocidad con las redes 4G.

En el caso de la Agencia de Regulación y Control de las Telecomunicaciones, se maneja diferentes perfiles entre ellos los técnicos, administrativos, informáticos, jurídicos, financieros, entre otros, los cuales están distribuidos en las Coordinaciones Zonales, Oficinas Técnicas y demás edificios, que conforman la Agencia de Regulación y Control de las Telecomunicaciones, los mismos que son administrados desde la oficina Matriz, por tal razón, esta aplicación beneficiarla de manera significativa a toda la organización, puestos que cada área tiene un perfil diferente y por tanto acceso y restricción a los sistemas que cada una de estas manejan, ya sean estos programas y/o aplicaciones que se utilizan para efectos de gestión y control de todos los servicios de Telecomunicaciones a nivel nacional.

OBJETIVOS

Contar con el análisis y propuesta de implementación y aplicación de un sistema de administración de dispositivos móviles (MDM) así como el análisis de la gestión de rendimiento de la red, que administre todos los dispositivos móviles, como teléfonos inteligentes y tabletas que dispone la Agencia de Regulación y Control de la Telecomunicaciones, en sus distintas oficinas.

Analizar técnicamente las propuestas de implementación y aplicación de un sistema de administración de dispositivos móviles (MDM), para la Agencia de Regulación y Control de la Telecomunicaciones.

Concluir de acuerdo a los requerimientos de la Agencia de Regulación y Control de la Telecomunicaciones la mejor opción tanto en costo como beneficio.

Plantear la propuesta para la Implementación y aplicación del sistema de Administración de dispositivos móviles (MDM) y Análisis de la Gestión de rendimiento de la Red, en la Agencia de Regulación y Control de la Telecomunicaciones.

CAPÍTULO I.

1. INTRODUCCIÓN A MDM

1.1. ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES[1]

1.1.1. MDM A NIVEL MUNDIAL

Empezaremos con un análisis de los principales Sistemas Operativos que actualmente se encuentran en el mercado, el objetivo del estudio de estas arquitecturas, permitirá tener un conocimiento amplio de los niveles en donde se desarrollan las aplicaciones y cuáles son los lugares donde se encuentran los riesgos y las vulnerabilidades de cada uno de los sistemas.

Tabla 1.1: Sistemas Operativos a Nivel Mundial.

	Android	iPhone	WINDOWS Mobile	Blackberry
Personal Identification Number	YES	YES	YES	YES
Remote WIPE	NO	YES	YES	YES
Remote POLICY	NO	YES (Exchange)	YES (Exchange)	YES (BES)
LoJack	Not yet	Not yet	Third party	Third Party
Local mail encryption	NO	NO	NO	YES
File encryption	NO	Keychain	YES	YES
Application sandbox	YES	NO	NO	YES
Application signing	YES	YES	YES	YES
Permission model	Fine grained, kernel and IPC enforced	Sandbox, multiple users	Two tiers	Fine grained, JME class based
OS buffer overflow protection	Propolice, safe_iop, OpenBSD malloc and calloc	Non executable heap+stack	/GS stack protection	N/A (Java/JME based OS)
Forensic Analysis viability	HIGH	MEDIUM	HIGH	MEDIUM
Web agent	Webkit	Webkit	Trident	Webkit

Adaptado de: DWIVEDI. H.. CLARK. C. y THIEL. D. (2010) *Mobile application security*. McGraw Hill. Pág. 360

1.1.2. MERCADO ACTUAL DE LAS PLATAFORMAS MÓVILES

De acuerdo con la consultora Gartner para el año 2012 el Sistema Operativo Móvil más utilizado en el mundo de la computación móvil es Android con el 64% del mercado

[1] http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_13_desarrollo_de_aplicaciones.html

mundial, seguido por iOS con un 19%, esto quiere decir que las plataformas móviles con más riesgo de ser atacadas y con más usuarios y personas trabajando para realizar violaciones o mejores se encuentran en este segmento de los sistemas operativos móviles.

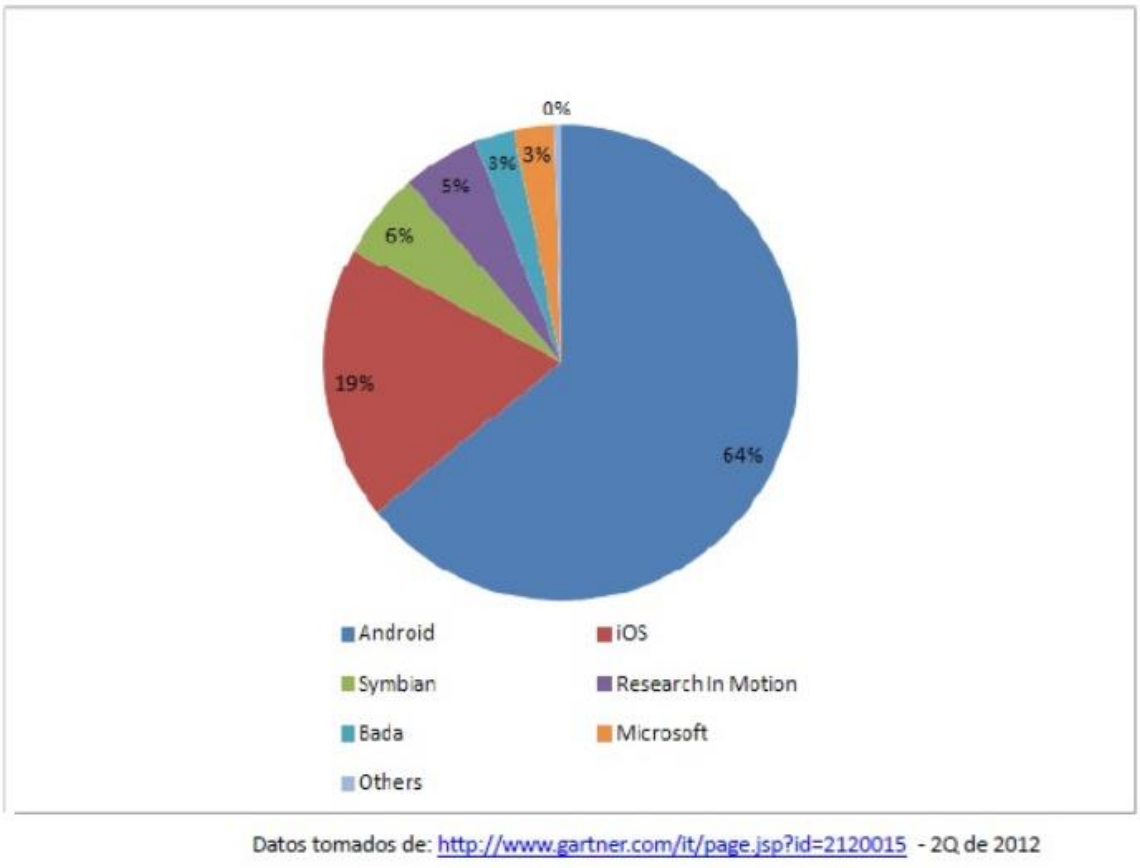


Figura 1.1: Mercado actual de las Plataformas Móviles a nivel Mundial.

Las arquitecturas de los sistemas operativos móviles más comunes son: Android, iOS, BlackBerry y Windows Phone, los cuales son los más utilizados en la actualidad a nivel mundial.

1.1.2.1. *ANDROID*

El sistema operativo Android está basado en el núcleo del sistema operativo Linux, es decir un sistema de código abierto diseñado específicamente para dispositivos móviles.

Android es un conjunto de software que incluye un sistema operativo, un middleware o software de conectividad que permite el funcionamiento de aplicaciones distribuidas sobre plataformas diferentes y múltiples aplicaciones claves. El Kit de desarrollo de software de

Android provee herramientas para crear aplicaciones y las interfaces de programación para desarrollar las mismas en la plataforma Android.

Es una plataforma de software y un sistema operativo que está basado en una versión modificada del sistema operativo Linux, inicialmente fue desarrollado por la compañía Google Inc., después se conformó la fundación Open Handset Alliance, el cual es un consorcio de 48 compañías de hardware, software y telecomunicaciones, la cual es la encargada de proveer estándares abiertos de comunicación para dispositivos móviles, a la cabeza del consorcio se encuentra Google.

La plataforma permite que cualquier usuario puede modificar el código, crear y desarrollar aplicaciones para el sistema operativo, permite controlar dispositivos por medio de bibliotecas desarrolladlas o adaptados por Google mediante el lenguaje de programación Java.

La arquitectura del Sistema Operativo Android está definida por 4 capas:

Linux Kernel: La primera desde la base hacia arriba es el Kernel o Núcleo de Linux aquí se encuentran 8 componentes específicos del núcleo que permiten el funcionamiento del sistema operativo con el hardware del dispositivo móvil, controlador de la pantalla, controlador del teclado, el controlador de la cámara, el controlador del audio, el controlador de la tarjeta de memoria, el controlador de la antena WiFi, el controlador de comunicaciones internas y el administrador de la energía.

Librerías: Las librerías de Android se encuentran en el segundo nivel después del Kernel, aquí se encuentra la librería Surface manager encargada de dibujar las diferentes pantallas, la librerías del entorno de medios controla todos los códec de multimedia, la librería de almacenamiento SQLite encargada de manejar el almacenamiento del dispositivo, la librería OpenGL es la encargada de manejar los gráficos 3D y las interacciones que los gráficos 2D, la librería FreeType es la encargada de administrar las fuentes, la librería

WebKit que provee un navegador web que provee las herramientas para el trabajo en dispositivos móviles y pantallas pequeñas, la librería SGL representa las gráficas de Android, la librerías SSL provee los protocolos para la comunicaciones seguras y la librería Libc incluye todas las cabeceras y funciones según el estándar del lenguaje C. Todas las demás librerías se definen en este lenguaje.

En este mismo nivel se encuentra el Runtime de Android, que está compuesto por dos componentes, el núcleo de las librerías que tiene clases en Java y la máquina virtual de Android Dalvik Virtual Machine.

Framework de Aplicaciones: Representa fundamentalmente el conjunto de herramientas de desarrollo de cualquier aplicación. Toda aplicación que se desarrolle para Android, ya sean las propias del dispositivo, las desarrolladas por Google o terceras compañías, o incluso las que el propio usuario cree, utilizan el mismo conjunto de API y el mismo "framework", representado por este nivel.

Entre las API más importantes ubicadas aquí, se pueden encontrar las siguientes:

Activity Manager: Conjunto de API que gestiona el ciclo de vida de las aplicaciones en Android.

Window Manager: Gestiona las ventanas de las aplicaciones y utiliza la librería Surface Manager.

Telephone Manager: Incluye todas las API vinculadas a las funcionalidades propias del teléfono (llamadas, mensajes, etc.).

Content Provider: Permite a cualquier aplicación compartir sus datos con las demás aplicaciones de Android. Por ejemplo, gracias a esta API la información de contactos, agenda, mensajes, etc. será accesible para otras aplicaciones.

View System: Proporciona un gran número de elementos para poder construir interfaces de usuario (GUI), como listas, mosaicos, botones, "check-boxes", tamaño de

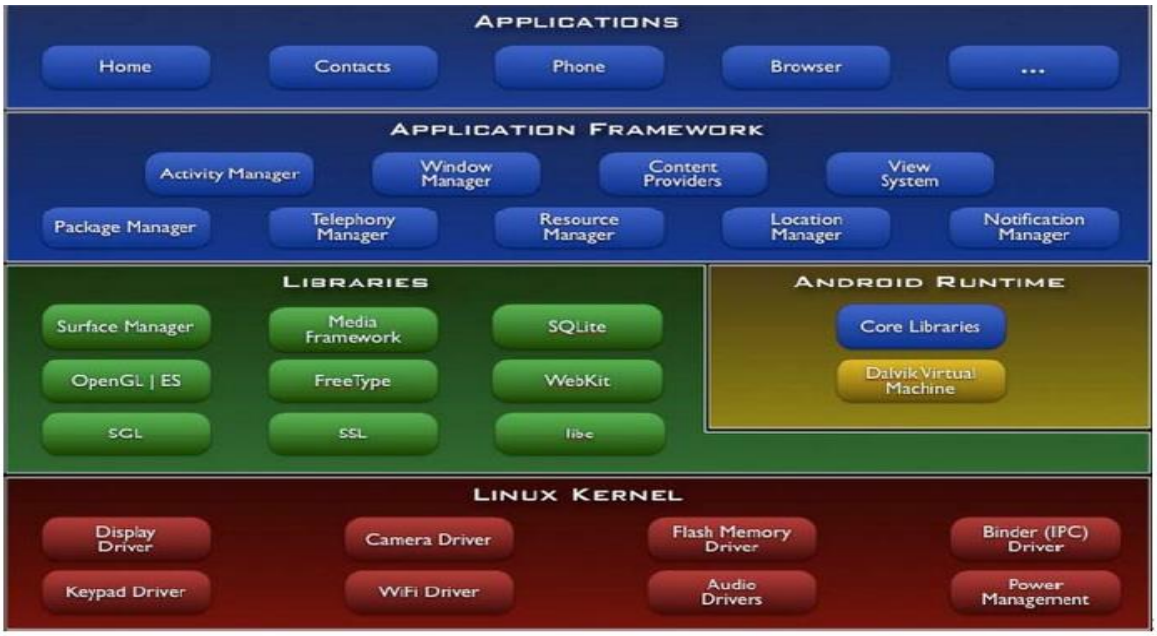
ventanas, control de las interfaces mediante teclado, etc. Incluye también algunas vistas estándar para las funcionalidades más frecuentes.

Location Manager: Posibilita a las aplicaciones la obtención de información de localización y posicionamiento.

Notification Manager: Mediante el cual las aplicaciones, usando un mismo formato, comunican al usuario eventos que ocurran durante su ejecución: una llamada entrante, un mensaje recibido, conexión Wi-Fi disponible, ubicación en un punto determinado, etc. Si llevan asociada alguna acción, en Android denominada Intent, (por ejemplo, atender una llamada recibida) ésta se activa mediante un simple clic.

XMPP Service: Colección de API para utilizar este protocolo de intercambio de mensajes basado en XML.

Aplicaciones: En la capa de aplicaciones se ubican las aplicaciones que utilizan todos los recursos del sistema operativo, aquí se encuentra las aplicaciones del teléfono, contactos, navegadores, las aplicaciones que se descargan del Google Play y las aplicaciones que programan los desarrolladores de Android.



Tomado de: http://elinux.org/Android_Architecture

Figura 1.2: Arquitectura del Sistema Operativo Android.

1.1.2.2. *IOS*

iOS es un sistema operativo móvil de la empresa Apple Inc. Originalmente desarrollado para el iPhone (iPhone OS), siendo después usado en dispositivos como el iPod Touch, iPad y el Apple TV, la instalación de este sistema operativo no es permitida en hardware de terceros.

La interfaz de usuario de iOS está basada en el concepto de manipulación directa, usando gestos multitáctiles. Los elementos de control consisten de deslizadores, interruptores y botones. La respuesta a las órdenes del usuario es inmediata y provee de una interfaz fluida. La interacción con el sistema operativo incluye gestos como deslices, toques, pellizcos, los cuales tienen definiciones diferentes dependiendo del contexto de la interfaz. Se utilizan acelerómetros internos para hacer que algunas aplicaciones respondan a sacudir el dispositivo (por ejemplo, para el comando deshacer) o rotarlo en tres dimensiones (un resultado común es cambiar de modo vertical al apaisado u horizontal).

iOS se deriva del sistema operativo de equipos de escritorio Mac OS X, que a su vez está basado en Darwin BSD, y por lo tanto es un sistema operativo Unix.

Pantalla principal (llamada «SpringBoard») es donde se ubican los iconos de las aplicaciones y el Dock en la parte inferior de la pantalla donde se pueden anclar aplicaciones de uso frecuente, aparece al desbloquear el dispositivo o presionar el botón de inicio. La pantalla tiene una barra de estado en la parte superior para mostrar datos, tales como la hora, el nivel de batería, y la intensidad de la señal.

Multitarea Antes de iOS 4, la multitarea estaba reservada para aplicaciones por defecto del sistema. A Apple le preocupaba los problemas de batería y rendimiento si se permitiese correr varias aplicaciones de terceros al mismo tiempo. A partir de iOS 4, dispositivos de tercera generación y posteriores permiten el uso de 7 APIs para multitarea, específicamente: Audio en segundo plano, Voz IP, Localización en segundo plano,

Notificaciones push, Notificaciones locales, Completado de tareas y Cambio rápido de aplicaciones

Game Center Fue anunciado en el evento donde se presentó iOS 4 el 8 de Abril de 2010. Game Center se lanzó en junio de 2010 para los iPhone y iPods Touch con iOS 4 (excepto para el iPhone 2G, 3G y iPod Touch 1g). En iOS 5 se perfeccionó, pudiendo agregar una foto a tu perfil, pudiendo ver los amigos de tus amigos y pudiendo encontrar adversarios con recomendaciones de nuevos amigos en función de tus juegos y jugadores favoritos, actualmente se encuentra operativa la versión de iOS 9.1.

Tecnologías no admitidas iOS no permite Adobe Flash ni Java. Steve Jobs escribió una carta abierta donde critica a Flash por ser inseguro, con errores, consumir mucha batería, ser incompatible con interfaces multitouch e interferir con el servicio App Store. En cambio iOS usa HTML5 como una alternativa a Flash.

Esta ha sido una característica muy criticada tanto en su momento como la actualidad. Sin embargo por métodos extraoficiales se le puede implementar aunque conllevaría la pérdida de la garantía.

Las aplicaciones deben ser escritas y compiladas específicamente para la arquitectura ARM, por lo que las desarrolladas para Mac OS X no pueden ser usadas en iOS. Al igual que otros navegadores, Safari admite aplicaciones web. Aplicaciones nativas de terceros están disponibles para dispositivos corriendo iPhone OS 2.0 o posterior, por medio del App Store.

La arquitectura del sistema operativo iOS tiene 4 capas definidas:

Núcleo o Core OS: La primera es la capa del núcleo del sistema la cual contiene las características de bajo nivel, los archivos del sistema, el manejo del procesador, la memoria, las seguridad, el manejo de archivos, la administración de la energía, en general todo lo referente al hardware del dispositivo, este sistema operativo está basado en el sistema operativo Unix.

Núcleo o Core de Servicios: Esta capa es la encargada de proveer y contener todos los servicios básicos y fundamentales del sistema operativo que usan todas las aplicaciones, como por ejemplo SQLite para almacenamiento de información.

Medios: La capa de medios es la encargada de proveer los servicios de los gráficos y multimedia a la capa Cocoa Touch.

Cocoa Touch: Esta capa contiene tiene todas las funciones y herramientas para desarrollar aplicaciones para el sistema operativo iOS, posee un conjunto de frameworks que proporciona el API de Cocoa, que provienen de la plataforma del MAC, aquí se encuentran todas las funcionalidades para desarrollar aplicaciones móviles en iOS, como por ejemplo el acelerómetro, los eventos multi Touch, cámara, localización, entre otros.

Esta capa está formada por dos Frameworks fundamentales:

UIKit: contiene todas las clases que se necesitan para el desarrollo de una interfaz de usuario

Foundation Framework: define las clases básicas, acceso y manejo de objetos, servicios del sistema operativo.

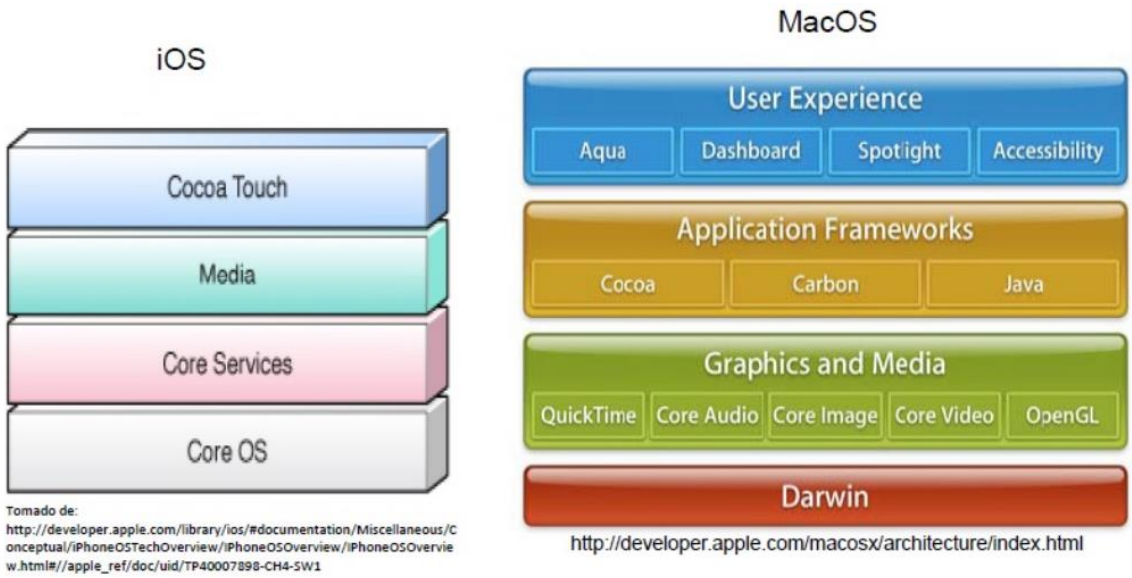


Figura 1.3: Arquitectura del Sistema Operativo iOS.

1.1.2.3. *BLACKBERRY*

El BlackBerry OS es un sistema operativo móvil desarrollado por Research In Motion para sus dispositivos BlackBerry. El sistema permite multitarea y tiene soporte para diferentes métodos de entrada adoptados por RIM (Research In Motion Limited) para su uso en computadoras de mano, particularmente la trackwheel, trackball, touchpad y pantallas táctiles.

Su desarrollo se remonta la aparición de los primeros handheld en 1999. Estos dispositivos permiten el acceso a correo electrónico, navegación web y sincronización con programas como Microsoft Exchange o Lotus Notes aparte de poder hacer las funciones usuales de un teléfono móvil.

El Sistema Operativo BlackBerry está claramente orientado a su uso profesional como gestor de correo electrónico y agenda. Desde la cuarta versión se puede sincronizar el dispositivo con el correo electrónico, el calendario, tareas, notas y contactos de Microsoft Exchange Server además es compatible también con Lotus Notes y Novell GroupWise.

BlackBerry Enterprise Server (BES) proporciona el acceso y organización del email a grandes compañías identificando a cada usuario con un único BlackBerry PIN. Los usuarios más pequeños cuentan con el software BlackBerry Internet Service, programa más sencillo que proporciona acceso a Internet y a correo POP3 / IMAP / Outlook Web Access sin tener que usar BES.

Al igual que en otros sistemas operativos los desarrolladores independientes también pueden crear programas para BlackBerry pero en el caso de querer tener acceso a ciertas funcionalidades restringidas necesitan ser firmados digitalmente para poder ser asociados a una cuenta de desarrollador de RIM (Research In Motion Limited).

La arquitectura del sistema operativo BlackBerry OS tiene 4 capas definidas:

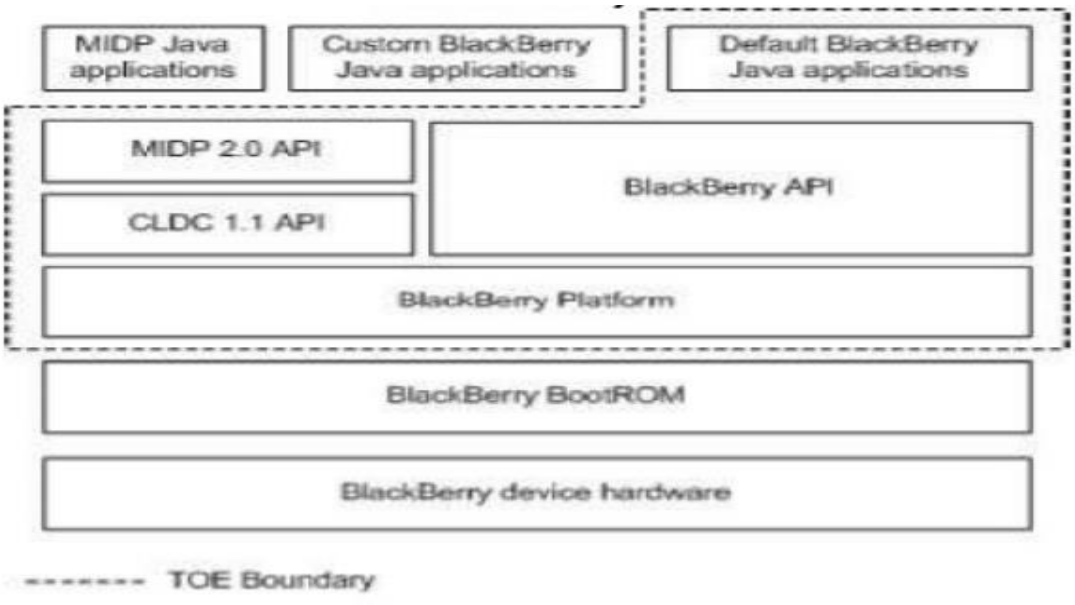
BlackBerry Device Hardware: Esta capa del sistema operativo es la encargada de trabajar con el hardware de los dispositivos móviles.

BlackBerry BootRoom: Esta capa de la arquitectura de la plataforma es la encargada de realizar un arranque seguro del hardware y del sistema operativo, este inicia en la memoria flash y verifica la firma del dispositivo en la memoria ROM del equipo para verificar que se encuentre correctamente asignado, esta es una medida de seguridad de los dispositivos BlackBerry para ejecutar los procesadores y los sistemas operativos.

BlackBerry Plaform: Esta capa es la encargada de proveer toda la plataforma del sistema operativo de BlackBerry por ejemplo la identificación, la seguridad entre otras.

BlackBerry API: Esta capa provee todas las funciones y servicios de la plataforma de Blackberry a los desarrolladores de aplicaciones, también en esta capa se encuentran las API de Java para Android para los CLDC y los MIDP que pueden ejecutarse en BlackBerry.

Aplicaciones: La capa de aplicaciones contiene las aplicaciones desarrolladas por defecto de BlackBerry, las aplicaciones Java caracterizadas, las aplicaciones MIDP y las aplicaciones desarrolladas en otras plataformas que provee BlackBerry.



Tomado de: http://www.cse-cst.gc.ca/its-sti/services/cc/blackberry-v410-sec-eng.html

Figura 1.4: Arquitectura del Sistema Operativo Blackberry.

1.1.2.4. *WINDOWS PHONE*

Windows Phone es un sistema operativo móvil desarrollado por Microsoft, como sucesor de la plataforma Windows Mobile. A diferencia de su predecesor, está enfocado en el mercado de consumo generalista en lugar del mercado empresarial por lo que carece de muchas funcionalidades que proporcionaba la versión anterior. Microsoft ha decidido no hacer compatible Windows Phone con Windows Mobile por lo que las aplicaciones existentes no funcionan en Windows Phone haciendo necesario desarrollar nuevas aplicaciones. Con Windows Phone, Microsoft ofrece una nueva interfaz de usuario que integra varios servicios en el sistema operativo. Microsoft planeaba un estricto control del hardware que implementaría el sistema operativo, para evitar la fragmentación con la evolución del sistema, pero han reducido los requisitos de hardware de tal forma que puede que eso no sea posible.

El 29 de octubre de 2012 se lanzó al mercado Windows Phone 8 solo para nuevos dispositivos, debido a un cambio completo en el Kernel que lo hace incompatible con dispositivos basados en la versión anterior. Esta versión incluye nuevas funciones que de acuerdo a Microsoft lo harán competitivo con otros sistemas operativos.

La arquitectura de Windows Phone cambió radicalmente en su estructura y funcionamiento, la nueva arquitectura es más simple y sencilla pero más potente con respecto al funcionamiento y a los usos que se le puede dar al dispositivo móvil.

La arquitectura del sistema operativo Windows Phone tiene 4 capas definidas:

Hardware: Es la capa que representa cualquier hardware de dispositivo móvil existente en el que se encuentre instalada el sistema operativo.

Kernel: En la capa del núcleo se encuentran los drivers, el sistema de archivos, las redes, el sistema de reinderizado, los gráficos, el sistema de actualizaciones entre otros.

Modelo: En esta capa se encuentran los modelos de aplicación, de interfaces de usuario y la integración a la nube, en esta capa se provee las herramientas base para el uso del sistema operativo.

Application Runtime: En esta capa de la aplicación se ejecutan todas las aplicaciones del sistema operativo.

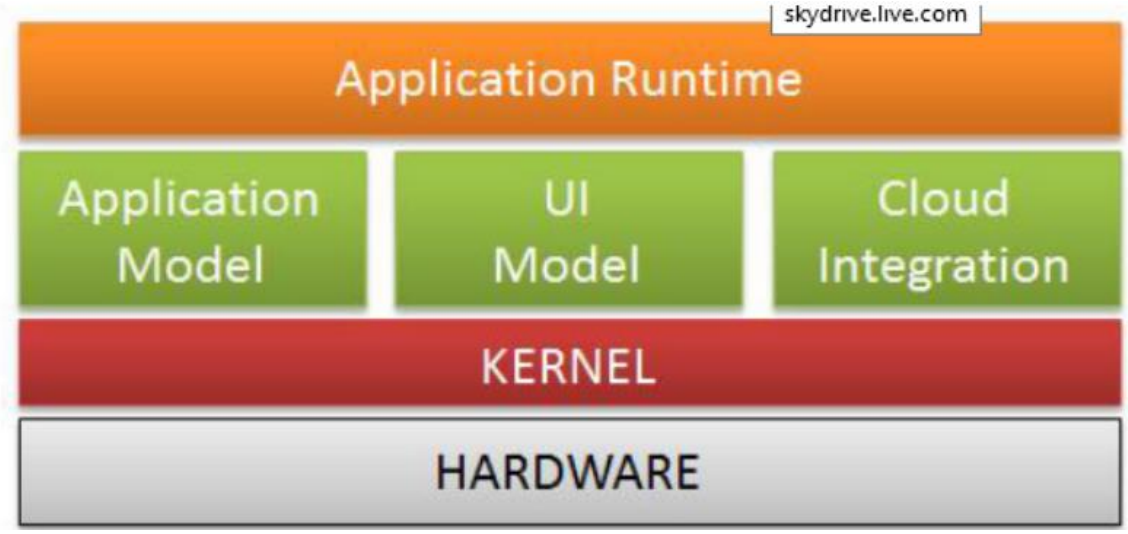


Figura 1.5: Arquitectura del Sistema Operativo Windows Phone.

Con este antecedente se puede considerar que en todo el mundo donde existen teléfonos inteligentes se usa la administración de dispositivos móviles, un ejemplo claro de su uso es la localización y gestión de cuentas de contactos, correos, entre otras aplicaciones, adicionalmente una de las mayores tendencias móviles que los analistas de Gartner presentaron en el Gartner Symposium/ITxpo se muestra a continuación:[2]

Específicamente en los próximos cinco años, el 65% de las corporaciones van a adoptar MDM para enfrentar los temas de seguridad que generan los teléfonos inteligentes y las tabletas.

Las razones que impulsan esta tendencia son obvias: Gartner predice que hasta el 2017, el 90% de las empresas tendrán dos o más sistemas operativos móviles que soportar. En el año pasado, muchas compañías se han trasladado a Apple como su principal plataforma

de dispositivos móviles, mientras que otras harán lo mismo en los próximos 12 a 18 meses. A medida que otros sistemas operativos como las plataformas móviles de Windows 8 crezcan, se tendrán que adoptar MDM, sostuvo Gartner.

Durante sus presentaciones en el simposio, los analistas de Gartner afirmaron que la única forma en que el personal de TI pueda mantener el control sobre la proliferación de dispositivos móviles es separando los dispositivos de cómputo móviles en tres diferentes clases: dispositivos estándar confiables proporcionados por la empresa, dispositivos tolerados y dispositivos no soportados. En este escenario, a los usuarios se les proporciona una lista predefinida de tecnologías soportadas en cada clase, junto con un presupuesto de la cantidad proyectada que cada selección consume. Los usuarios pueden optimizar las tecnologías de acuerdo a sus requerimientos sin exceder el presupuesto. Los límites al gasto por parte de los individuos son mejor que la necesidad de confiar en las interpretaciones subjetivas de lo que es "un uso razonable".

"Sin embargo, al implementar un sistema de soporte estructurado con variados niveles de soporte, las organizaciones TI pueden proteger la información del negocio y hacer cumplir políticas sobre el movimiento de los datos entre el dispositivo y la red corporativa, mientras que el mismo tiempo se habilita a que los usuarios adopten el dispositivos que consideran más apropiado", sostuvo Phil Redman, vicepresidente de investigación de Gartner. "Las organizaciones van a encontrar que es complicado lograr un sistema de soporte móvil eficiente si todas las plataformas no son administradas de la misma forma bajo los requerimientos de la empresa. Al igual que las PC, los dispositivos móviles son formas de dispositivos de acceso cliente, y las políticas para ellos deberían ser similares en fuerza pero optimizadas para el uso móvil".

---

[2] http://cioperu.pe/articulo/11474/gartner-la-tecnologia-de-administracion-de-dispositivos-moviles/

Redman afirmó luego que los proveedores de MDM están yendo más allá de la seguridad y han pasado a soportar aplicaciones, datos y contenidos de la empresa y de terceros. En los próximos dos años, continuaremos viendo que las plataformas MDM se amplían y se convierten más en plataformas de administración de sistemas móviles empresariales.

Algunos otros hechos fundamentales sobre los dispositivos móviles de Gartner:

En el 2016, más de 1,6 mil millones de dispositivos móviles inteligentes serán comprados a nivel global. Dos tercios de la fuerza laboral móvil tendrá un teléfono inteligente y el 40% de la fuerza laboral será móvil. El desafío para los líderes de TI es determinar qué hacer con este nuevo canal para sus clientes y empleados.

Gartner pronostica que en el 2016, la mitad de los dispositivos que no son PC serán comprados por parte de los empleados. Para el final de la década, la mitad de todos los dispositivos de las empresas serán comprados por los empleados.

Para el 2016, el 60% de las grandes empresas implementarán zonas de red de acceso limitado para limitar la conectividad de los dispositivos móviles de propiedad personal.

1.2. GESTIÓN DE RED

Dentro de toda red se hace indispensable contar con un control de la misma es por tal motivo que en este capítulo realizaremos un análisis de los beneficios que podríamos lograr con la misma. Es así que dentro de una Gestión de Red está el Monitoreo y el Control de la misma.

1.2.1. MONITOREO DE RED

Actualmente la complejidad de las redes, la arquitectura que presentan, así como sus dispositivos hacen que sus recursos lleguen a un punto crítico, es aquí que el monitoreo de los servicios y los recursos logran que una red tenga una confiabilidad y un desempeño optimo mismo que garantiza al Administrador de la Red, una red con un gran desempeño y una

confiabilidad elevada. Para lo cual se utiliza algunos protocolos entre los cuales se encuentran el ping, SNMP, TCP, UDP, entre otros; los cuales muestran puertos activos, tiempos de respuesta, servicios que tienen habilitados, los cuales conjuntamente con sistemas de gestión de red ayudan a lograr el objetivo deseado.

1.2.2. CONTROL DE RED

En este caso el Control nos ayuda de una manera activa a determinar el comportamiento de la Red, y de esta manera podemos modificar parámetros y ejecutar acciones. De aquí que las actividades de control potencian a los sistemas de gestión, permitiendo en todo momento remotamente determinar el comportamiento y características de la red.

1.2.3. ELEMENTOS DE LA GESTIÓN DE RED

Dentro de la Gestión de Red se encuentran los siguientes Elementos: Los Agentes, Gestores y Dispositivos Administrados.

Figura 1.6. Elementos de la gestión de Red

De acuerdo a lo indicado en el grafico anterior, se mencionan todas las componentes o elementos de la Gestión de Red.

Agentes. Aquí se considera el software de administración de red mismo que debe encontrarse en un dispositivo o nodo administrado. El cual debe contener una base de datos local de información de administración, puesto que debe responder a las peticiones del gestor de información de algún evento importante.

Gestores. También conocida como Consola de Administración, aquí se considera básicamente a la estación de trabajo o servidor donde se ejecuta o se encuentran corriendo las aplicaciones de gestión de red, el mismo que dispone de interfaces gráficas para presentar información al usuario y de esta manera se facilita la operatividad de la gestión.

Dispositivo Administrativo. A este se le considera a cualquier nodo de red que contenga un agente SNMP y que el mismo este dentro de una red administrada. Estos deben almacenar información de monitoreo y control, misma que está a disposición de los gestores por medio del uso de protocolos de administración de red.

1.2.4. ÁREAS FUNCIONALES DE LA GESTIÓN DE RED

Las áreas funcionales que se encuentra considerado dentro de la gestión de una red son: Gestión de Fallos, Gestión de Configuración, Gestión de Contabilidad, Gestión de Prestaciones y Gestión de Seguridad.

1.2.4.1. *GESTIÓN DE FALLOS*

Esta se ocupa de mantener la red con un funcionamiento correcto, tratando de protegerla de errores en conjunto con todas las componentes de la misma.

Aquí también es conveniente diferenciar Fallo de Error: El fallo (es una situación que requiere de alguna acción correctora) descubierto debido a una operación incorrecta o por una gran cantidad de errores. Sin embargo los errores ocurren ocasionalmente y no necesariamente son fallos.

Ante un fallo lo que se debe hacer es tres instancias:

- **Diagnosticar** y determinar lo más pronto posible donde se produjo el fallo.
- **Aislar** a la red del fallo, es decir configurándola de una manera que garantice que el impacto sea el menor posible
- **Resolver** el problema con la finalidad de que el funcionamiento de la red vuelva a su estado inicial, lo cual puede implicar el reemplazo de elementos fallidos.

El impacto y duración de los fallos dependen de la redundancia que se disponga en la red. Incluso aquí es necesario notar que un sistema de gestión de fallos también puede tener redundancia.

1.2.4.2. *GESTION DE CONFIGURACIÓN*

Todas y cada una de las redes están conformadas por componentes y sistemas que requieren de configuraciones para una operatividad correcta, por lo tanto es necesario establecer parámetros de operación, Asociar nombres a objetos, activar y desactivar los mismos, entre otros aspectos.

Aquí la gestión de configuración se ocupa iniciar, mantener, añadir y actualizar el estado de los componentes de la Red y la relación entre ellos.

1.2.4.3. *GESTIÓN DE CONTABILIDAD*

En todas las redes es necesario mantener actualizado un registro de uso que cada usuario hace de la red, lo cual es indispensable ya sea para facturación y/o para distribuir el gasto entre departamentos de la institución y así vigilar en caso de que exista un uso excesivo de algunos usuarios, con la finalidad de planificar un futuro crecimiento y realizar una redistribución de recursos de la red.

En este caso el gestor de la red debe ser capaz de adecuar parámetros de contabilidad los mismo que van a ser medidos en cada nodo, adicionalmente el acceso a este tipo de

información debe ser restringido. Con la finalidad de informar a los usuarios sobre los costos que han incurrido y establecer límites de consumo.

1.2.4.4. *GESTION DE PRESTACIONES*

Aquí se monitorea y se analiza las prestaciones de la red con la finalidad de verificar que las mismas estén dentro de los límites permitidos y realizar operaciones de control como también monitorizar la degradación de las prestaciones.

Esta gestión es indispensable para conocer la Calidad de Servicio que una determinada red ofrece.

También es indispensable para sacar información estadística y de esta manera modificar la operación del sistema para una correcta gestión de las prestaciones.

1.2.4.5. *GESTIÓN DE SEGURIDAD*

Este tipo de gestión se utiliza fundamentalmente para la generación, distribución y mantenimiento de las claves para control de acceso y encriptación.

Monitorización del acceso a las máquinas de red y la propia información de gestión, por lo tanto se encarga de proteger la información que es considerada como el activo más importante de la institución, mismo que se genera diariamente.

Adicionalmente se encarga de proteger los equipos de comunicación como son servidores, estaciones de trabajo de posibles ataques provenientes de agentes externos y de esta manera mantener la integridad y seguridad del sistema.

CAPÍTULO II.

2. MDM.

2.1. ARQUITECTURA DE MDM.

La arquitectura básica de un sistema de MDM incluye:

Agente: El agente es una aplicación que tiene que ser instalado en todos los dispositivos que será gestionado por el sistema de Administración de Dispositivos Móviles (MDM). El agente permite al tomar el control de servidor del dispositivo inteligente.

Servidor: El servidor es el lugar donde el software se ejecuta. Por lo general es una aplicación que se puede instalar en los servidores que la empresa ya posee.

Base de datos: La base de datos es el lugar donde todos los datos obtenidos a través de la solución MDM pueden ser almacenados para el inventario y la presentación de informes, por ejemplo, la ubicación de los dispositivos y qué tipo de aplicaciones se ejecutan en ellos.

Dispositivos: El último componente de la arquitectura la Administración de Dispositivos Móviles (MDM) son los dispositivos, incluyendo teléfonos inteligentes y tabletas que se conectarán al servidor. La comunicación entre los dispositivos y el servidor es típicamente mediante el uso de Wi-Fi, pero otras tecnologías inalámbricas como redes celulares pueden también ser utilizadas.

La siguiente figura muestra la arquitectura básica de un sistema de la Administración de Dispositivos Móviles (MDM).

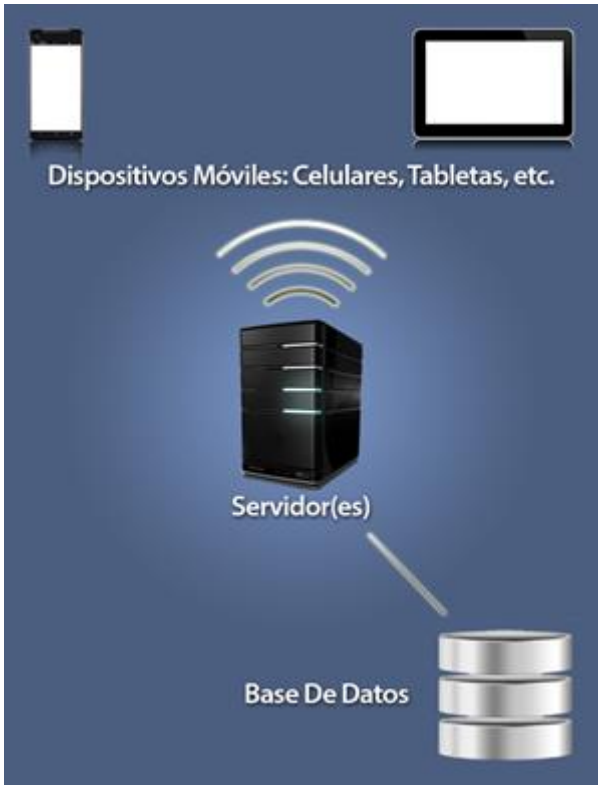


Figura 2.1: Arquitectura básica de un sistema de la Administración de Dispositivos Móviles (MDM).

2.2. TIPOS DE ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES (MDM).

Actualmente existen dos tipos de soluciones de Administración de Dispositivos Móviles (MDM):

- Basado en la nube también se conoce como software como servicio. Desarrollo y adopción de aplicaciones móviles y de software como servicio (SaaS).
- En las instalaciones que implica el uso de hardware.

La diferencia entre los dos sistemas está basada principalmente donde se encuentra el servidor. En el sistema basado en la nube, el servidor está ubicado en las instalaciones del proveedor de la Administración de Dispositivos Móviles (MDM) y es administrado por la empresa MDM. Para la solución en las instalaciones, el servidor tiene que estar ubicado en las instalaciones del cliente. Es por ello que la implementación de la solución basada en la nube es más simple, pero por otro lado, los clientes que optan por la solución en el mismo

lugar sienten una sensación de control sobre su información adicional ya que administran el servidor también.

Otro de los beneficios de la solución basada en la nube es que es más rápido de configurar, mientras que la solución en las instalaciones puede requerir más tiempo para la configuración y el mantenimiento regular. Sin embargo, los costos para los dos tipos de sistemas son similares debido a la competencia de la empresa y la evolución de la tecnología.

Los dos tipos de Administración de Dispositivos Móviles (MDM) se tendrán en cuenta en el modelo del costo actual.

La dos siguientes figuras describen la implementación básica para las en las instalaciones y soluciones basadas en la nube, respectivamente.

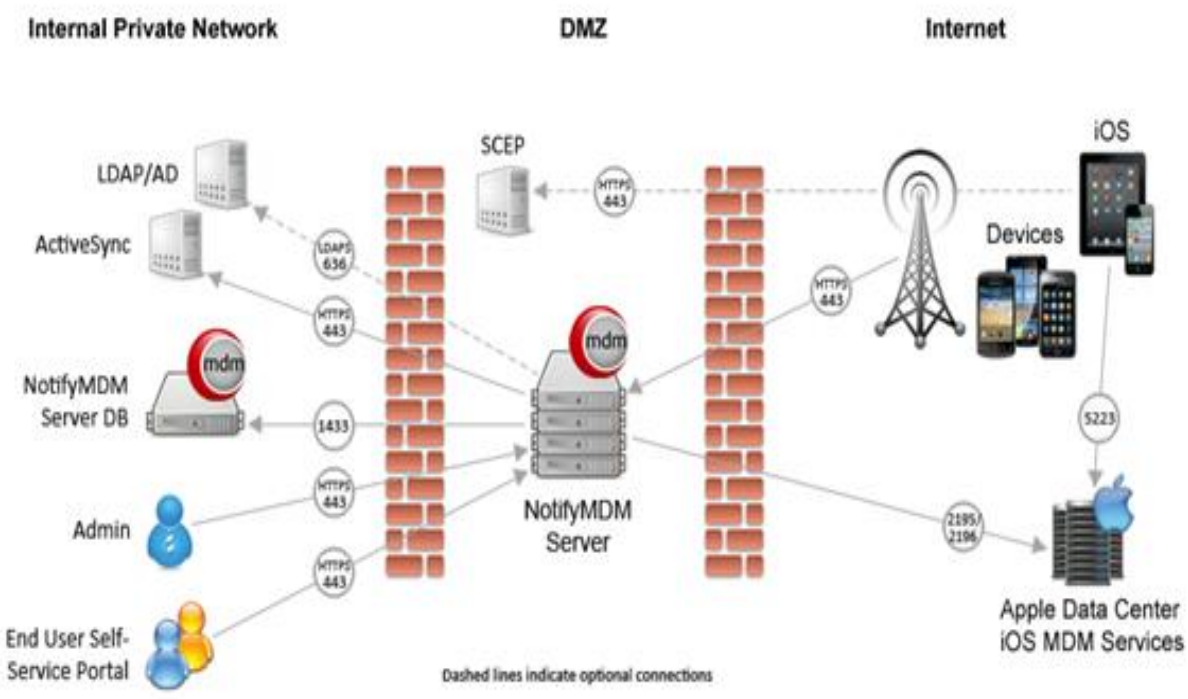


Figura 2.2: Solución implementada en servidores Locales.

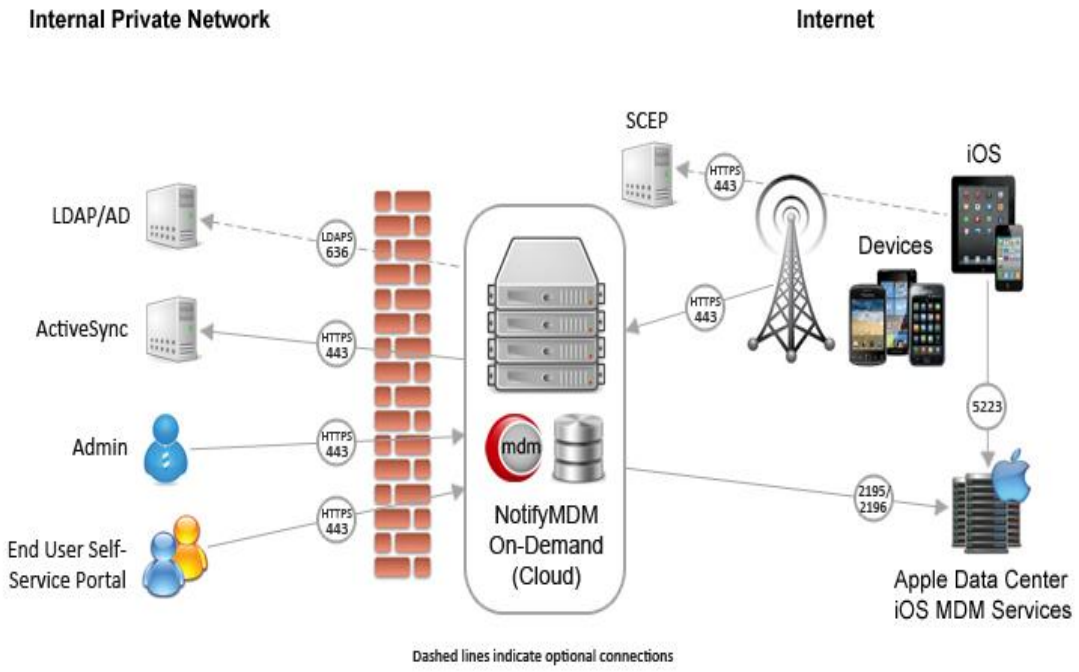


Figura 2.3: Solución implementada en la Nube.

2.3. PROS Y CONTRAS DE LA ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES.

Las Soluciones de Administración de Dispositivos Móviles (MDM) al igual que otras tecnologías tienen algunas ventajas y desventajas. De las cuales las siguientes se pueden mencionar:

- Permite el acceso a la infraestructura de la empresa: El beneficio más obvio de la Administración de Dispositivos Móviles (MDM) es que los empleados podrán acceder a la red corporativa y hacer su trabajo utilizando la información de la misma.
- Fomenta la productividad y la eficiencia: Porque los empleados son capaces de trabajar virtualmente desde cualquier lugar y en cualquier momento en que tienen conexión a Internet. Ellos tendrán la oportunidad de hacer su trabajo después de las horas de trabajo desde su casa, por ejemplo.
- La instalación masiva de aplicaciones: Es muy útil profesionalmente, ya que puede ahorrar tiempo a los usuarios y el dinero a la empresa. A pesar de que la instalación de una aplicación toma unos segundos, si sumamos esos segundos para cada empleado, los

resultados son considerables y pueden costar mucho tiempo y dinero de los empleados de la empresa.

- Limpieza remota: La limpieza remota es un beneficio porque en el caso de que un empleado deja una empresa o si un dispositivo es robado, la información corporativa puede ser borrada del dispositivo con el fin de evitar problemas de seguridad.
- Aplicaciones de bloqueo: Es un útil desde el punto de vista de seguridad, debido a que los empleados no podrán acceder a las aplicaciones que se consideran perjudiciales o que puedan contener malware móvil malicioso.
- La localización de dispositivos: Este es un beneficio porque si un dispositivo es robado, puede ser localizado y recuperado.
- Acceso basado en roles: En función de su papel en la empresa, los empleados pueden tener acceso únicamente a las bases de datos que necesitan para realizar su trabajo. Es un profesional ya que la información sensible no estará al alcance de todos.

Entre las desventajas de la utilización de una solución de administración de dispositivos móviles (MDM), se puede mencionar las siguientes:

- Inversión: La empresa que quiere implementar una solución de Administración de Dispositivos Móviles (MDM) tiene que pagar los costos tangibles e intangibles. Los costos tangibles que vienen del dinero que hay que pagar al proveedor de MDM para la solución. Intangibles incluyen el tiempo que los usuarios tienen que gastar aprender a usar el nuevo sistema.
- Los problemas de privacidad: Es en parte muy crítica, ya que algunos empleados pueden no sentirse cómodos dejando que la empresa instale una aplicación en sus dispositivos que podrían permitir que sus jefes ver dónde se encuentren, en cualquier momento y las aplicaciones que están utilizando.

También hay desventajas cuando en una empresa se quiere utilizar la técnica BYOD (siglas en inglés de Trae tu propio dispositivo), entre las más comunes detallo a continuación:

- Cuando los empleados comparten archivos dentro y fuera de la oficina con sus tabletas y teléfonos inteligentes, es difícil para TI proteger y controlar esos datos.
- Si un dispositivo se pierde o es robado fuera de la oficina, o si se despide a un empleado, la información corporativa contenida software malicioso en dicho dispositivo se hace vulnerable a un uso malintencionado.
- Puede introducirse fácilmente en la red corporativa a través de los dispositivos infectados.
- Puede robarse la información corporativa utilizando aplicaciones que contienen caballos de Troya, obtenidas en tiendas de aplicaciones de terceros en la Internet.

2.4. CAPACIDADES DE LA ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES (MDM).

Las capacidades de una solución de Administración de Dispositivos Móviles (MDM) se pueden dividir en las siguientes categorías:

1. La gestión del programa: Esta es la capacidad de gestionar y soportar aplicaciones móviles, datos y sistemas operativos.
2. La gestión de servicios de red: Esto es la capacidad de obtener información fuera del dispositivo que captura ubicación , uso y LAN (WLAN) información de la red celular o Wi-Fi , utilizando la tecnología GPS .
3. Gestión de hardware: Esta gestión está más allá de la gestión básica de activos ya que incluye aprovisionamiento de dispositivos y apoyo.
4. Gestión de la seguridad: Se trata de la ejecución y el apoyo de dispositivo estándar y seguridad de datos, autenticación y cifrado. Contenerización de aplicaciones, VPN y software de cifrado son también parte de esta capacidad.

2.5. VISIÓN GENERAL DEL MERCADO

La Administración de dispositivos móviles (MDM) ha ganado importancia en los últimos dos años debido a la popularidad de los dispositivos móviles en el lugar de trabajo, lo cual puede reportar numerosos beneficios a una organización, entre ellos una mayor productividad y satisfacción de los empleados, así como mejoras en la contratación y la conservación del equipo de trabajo.

1,2 MILLONES DE ECUATORIANOS TIENEN UN TELÉFONO INTELIGENTE (SMARTPHONE)[3]

El 16,9% (1’261.944) de las personas de cinco años y más que tienen celular poseen un teléfono inteligente (Smartphone), lo que representa un crecimiento de 141% frente al 2011, según los últimos datos de la Encuesta de Tecnologías de la Información y la Comunicación (TIC) del Instituto Nacional de Estadística y Censos (INEC).

El estudio, que se realizó en diciembre de 2013, se hizo en 21.768 hogares a personas de 5 años y más, a nivel nacional, regional, provincial, de nivel urbano y rural.

Según la encuesta, el 51,3% de la población de 5 años y más tiene por lo menos un celular activado, en el 2011 ese porcentaje era del 46,6%.

Por edades, el grupo con mayor uso de teléfono celular activado es la población que se encuentra entre 25 y 34 años con el 76,5%, seguido de los de 35 a 44 años con el 76%.

La provincia con mayor número de personas que tiene un teléfono celular activado es Pichincha con el 60,9%, mientras que la menor es Chimborazo con el 37,4%.

En los datos de Internet, el 40,4% de la población de Ecuador ha utilizado Internet en los últimos 12 meses. En el área urbana el 47,6% de la población ha utilizado Internet, mientras que en el que el área rural refleja el mayor crecimiento con 25,3% frente al 17,8% del año anterior.

[3] http://www.ecuadorencifras.gob.ec/12-millones-de-ecuatorianos-tienen-un-telefono-inteligente-smartphone/

El estudio refleja que el acceso a internet en el país también se incrementó al pasar de 11,8% en 2010 al 28,3% de hogares con acceso a internet. De acuerdo a las áreas, en la zona rural el porcentaje de hogares que tienen acceso a internet es el 9,1% mientras que en el área urbana es de 37%.

Así también en el 2013, el 20,0% de las personas en el Ecuador son analfabetas digitales[4], 9,2 puntos menos que en el 2010

Mientras la Encuesta de Ingresos y Gastos en Hogares (ENIGHUR 2011-2012) refleja que los hogares ecuatorianos gastaron mensualmente $118.37 dólares en promedio en TIC, este monto incluye: Gastos en equipos celulares, alquiler de internet, Tarjetas de prepago para servicio celular e internet, recargas electrónicas a celular, planes de celular y de internet.

LA TECNOLOGÍA DE ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES VA A DESPEGAR SEGÚN GARTNER [5]

Del artículo presentado por un grupo de analistas de la compañía Gartner en el Gartner Symposium/ITxpo, manifiestan que en los próximos cinco años, un 65% de las compañías y corporaciones van a adoptar la Administración de Dispositivos Móviles (MDM) para enfrentar los temas de seguridad que generan los teléfonos inteligentes y las tabletas.

De los análisis realizados manifiestan que la única forma en que el personal de Tecnología pueda mantener el control sobre todos los dispositivos móviles es dividiéndolos en tres diferentes clases: dispositivos estándar confiables proporcionados por la empresa, dispositivos tolerados y dispositivos no soportados. De acuerdo a esto Gartner predice que hasta el 2017, un 90% de las empresas tendrán dos o más sistemas operativos móviles que soportar.

[4] Se considera a una persona como Analfabeta Digital cuando cumple simultáneamente tres características: 1) No tiene celular activado 2) En los últimos 12 meses no ha utilizado computadora 3) En los últimos 12 meses no ha utilizado internet.

[5] http://cioperu.pe/articulo/11474/gartner-la-tecnologia-de-administracion-de-dispositivos-moviles/

Algunos otros hechos fundamentales sobre los dispositivos móviles manifiesta Gartner:

En el 2016, más de 1,6 mil millones de dispositivos móviles inteligentes serán comprados a nivel global. Dos tercios de la fuerza laboral móvil tendrá un teléfono inteligente y el 40% de la fuerza laboral será móvil.

Gartner pronostica que en el 2016, la mitad de los dispositivos que no son PC serán comprados por parte de los empleados. Para el final de la década, la mitad de todos los dispositivos de las empresas serán comprados por los empleados.

Para el 2016, el 60% de las grandes empresas implementarán zonas de red con la finalidad de limitar la conectividad de los dispositivos móviles de propiedad personal.

2.5.1. CLIENTE – AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

Mediante la promulgación de la Ley Orgánica de Telecomunicaciones (LOT) el 18 de febrero de 2015, se crea la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), adscrita al Ministerio rector de las Telecomunicaciones y de la Sociedad de la Información. Es la entidad encargada de la administración, regulación y control de las telecomunicaciones y del espectro radioeléctrico y su gestión, así como de los aspectos técnicos de la gestión de medios de comunicación social que usen frecuencias del espectro radioeléctrico o que instalen y operen redes.

De esta manera en su disposición final primera indica: Se suprime la Superintendencia de Telecomunicaciones (SUPERTEL), el Consejo Nacional de Telecomunicaciones (CONATEL) y la Secretaría Nacional de Telecomunicaciones (SENATEL). Las partidas presupuestarias, los bienes muebles e inmuebles, activos y pasivos, así como los derechos y obligaciones derivados de contratos, convenios e instrumentos nacionales e internacionales

correspondientes a dichas entidades, pasan a la Agencia de Regulación y Control de las Telecomunicaciones.

Los derechos y obligaciones derivados de contratos, convenios e instrumentos nacionales e internacionales relacionados con la planificación del uso del espectro radioeléctrico, así como la elaboración del Plan Nacional de Frecuencias, son asumidos por la Agencia de Regulación y Control de las Telecomunicaciones.

2.5.2. NÚMERO DE FUNCIONARIOS Y PERSONAL DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES[6]

De acuerdo al detalle presentado de manera mensual en la página web de la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, el número de funcionarios que laboran en la institución son quinientos veinte y seis (526), mismos que se encuentran distribuidos en varias direcciones de acuerdo al esquema organizacional actual el cual detallo en el anexo 1.

2.5.3. NÚMERO Y CARACTERÍSTICAS DE LOS DISPOSITIVOS

El número de dispositivos que actualmente están siendo conectados a la red de ARCOTEL es 223. Los tipos de dispositivos utilizados en la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), provienen de diferentes proveedores y utilizan diferentes sistemas operativos. La siguiente tabla resume el número y el sistema operativo de los dispositivos presentes en la ARCOTEL, Anexo 2, sin embargo se pretende implementar la solución para el total de funcionarios (526).

[6] http://www.arcotel.gob.ec/wp-content/uploads/downloads/2016/01/literal-b2-distributivo-de-personal.pdf

Tabla 2.1: Número de dispositivos que dispone la ARCOTEL y los que debe adquirir o aplicar BYOD.

Dispositivos presentes en ARCOTEL		Dispositivos a adquirir por ARCOTEL o aplicar BYOD	Numero de dispositivos a Administrar
iOS	88	200	288
Android	97	103	200
Windows Phone	31	0	31
Other	7	0	7
Total	223	303	526

2.5.4. LAS NECESIDADES DEL CLIENTE Y EL SISTEMA

Es importante que los funcionarios tanto administrativos como técnicos de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) deban tener acceso a la red corporativa. Actualmente, existe una red wi-fi “Arcotel-Invi”, a la cual se puede conectar equipos institucionales y personales previa a la obtención de la clave de seguridad, por medio de esta se tiene acceso a correo electrónico corporativo de una manera segura mediante Microsoft Exchange que forma parte de las licencias de Microsoft ya adquiridos por la Agencia de Regulación y Control de las Telecomunicaciones. Sin embargo existen varios aplicativos que se maneja a nivel de control, de gestión y de administración, de las cuales se enumera algunas de ellas: Sistema de Inspecciones, Interfaces de acceso a bases de datos de concesiones como SIRATV y SIGER bases donde se encuentra toda la información concerniente a los parámetros técnicos de cada sistema de telecomunicaciones que concesiono el estado.

Con el acceso en línea a todas las aplicaciones que son manejadas por cada departamento, esto evidencia un aprovechamiento eficiente de los recursos que dispone la institución.

2.5.5. POLÍTICAS DE IMPLEMENTACIÓN

Dentro de la implementación lo primero que tenemos que tener en cuenta al elegir una solución MDM, es que existe una necesidad estratégica. Es decir que, que desde el área de Tecnologías de la Información se haya planteado cuestiones como: ¿Existe elementos corporativos que los funcionarios no saben configurar como por ejemplo cuentas de correo, redes Wi-Fi, conexiones VPN?; ¿aplicaciones corporativas que utiliza cada área de la ARCOTEL?; o ¿podemos gestionar la seguridad de los dispositivos móviles de igual manera que la de los equipos de escritorio?.

El siguiente paso será analizar cuáles son las necesidades reales de la Agencia de Regulación y Control de las Telecomunicaciones y cuáles serán en un futuro próximo, de manera que rentabilicemos la inversión del sistema de Administración de Dispositivos Móviles (MDM) que cubra no sólo mis requerimientos actuales sino también aquellos que puedan surgir en un futuro.

Una vez que la ARCOTEL cuenta ya con algunos dispositivos móviles, tendremos que centrarnos en el equipo y el sistema operativo que manejan cada uno de los equipos ya sea, iOS, Android, Windows Phone y BlackBerry. El mercado ofrece muchas opciones, por lo tanto tendremos que valorar principalmente cómo responde la capa de gestión de cada uno de los sistemas operativos, disponiendo de esto debo combinar diferentes plataformas, creando un catálogo corporativo que ofrezca una respuesta completa ante el escenario multiplataforma de la ARCOTEL.

La implantación de estos sistemas es crucial con el fin de mantener la seguridad de los datos y sistemas de la ARCOTEL que van a ser accesibles desde los equipos móviles.

De acuerdo a experiencias investigadas se propone la implantación como un proyecto con un ciclo de vida en cinco fases, que nos permite determinar qué puntos son más relevantes en el despliegue de soluciones para dispositivos móviles con el fin de mitigar todo lo posible las vulnerabilidades que generan la incorporación de estos dispositivos en la vida diaria.

Las cinco fases que se comenta son las siguientes:

Fase 1: Inicialización. Esta fase involucra las tareas que una organización debería realizar antes de iniciar el diseño de una solución de dispositivos móviles:

Identificar necesidades para garantizar la implementación Administración de dispositivos móviles.

Proporcionar una visión general de cómo las soluciones de dispositivos móviles debería soportar la misión de la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, creando una estrategia de alto nivel para implementar soluciones de movilidad desplegando una política de seguridad para dispositivos móviles y especificando los requerimientos funcionales y operativos de la solución.

Fase 2: Despliegue. En esta fase, se especifican las características técnicas de la solución y de los componentes relacionados. Esto incluye los métodos de autenticación y de cifrado utilizados para proteger las comunicaciones y los datos almacenados. También tienen que considerarse los tipos de dispositivos móviles cliente que van a ser usados, los cuales se verán afectados por las políticas definidas. Es necesario asegurarse que las políticas de seguridad son soportadas por todos los clientes. Al final de esta fase se han obtenido los componentes de la solución.

Fase 3: Implementación. En esta fase se configuran los equipos para que cumplan los requerimientos funcionales y de seguridad, incluyendo las políticas de seguridad de los

dispositivos móviles. La implementación incluye la integración con otros sistemas de seguridad, tales como servidores de login y autenticación.

Fase 4: Operaciones y mantenimiento. Esta fase incluye las tareas relacionadas con la operativa de seguridad que una organización debe llevar a cabo de manera continua una vez que la solución de dispositivos móviles están en funcionamiento, incluyendo la revisión de registro y detección de ataques.

Fase 5: Eliminación. Esta fase abarca tareas que ocurren cuando una solución de dispositivos móviles o sus componentes están siendo retiradas, generando la documentación necesaria para preservar el cumplimiento de los requisitos legales, medios de desinfección y eliminación de los equipos correctamente.

La conclusión que debemos sacar de todo esto es que los sistemas de Administración de Dispositivos Móviles MDM son elementos cruciales a la hora de estructurar las soluciones de movilidad, pero su implantación debe estructurarse en un proyecto más amplio en el que se tengan en cuenta todos los elementos asociados a la solución.

CAPÍTULO III.

3. ANALISIS COMPARATIVO DE ALTERNATIVAS.

En este capítulo se procederá a realizar un análisis de las ofertas presentadas por las distintas empresas que ofrecieron el sistema de Administración de Dispositivos Móviles (MDM) a la Agencia de Regulación y Control de las Telecomunicaciones.

3.1. METODOLOGIAS.

Las metodologías incluidas en este análisis son: Metodología Técnica y de acuerdo a las propuestas presentadas por las empresas ofertantes.

3.1.1. METODOLOGIAS TÉCNICAS.

En este campo se realiza un análisis técnico de todas las ofertas presentadas, es decir una breve descripción de cada oferta presentada.

3.1.2. LAS EMPRESAS MDM SELECIONADAS.

Dentro del proceso para el Análisis y Propuesta de Implementación y Aplicación de MDM en la Agencia de Regulación y Control de las Telecomunicaciones, se van a detallar las características técnicas de cada propuesta presentada, con la finalidad de llegar a elegir la más idónea o cuya implementación y aplicación sea la más conveniente para la ARCOTEL. A continuación empezamos detallando las características de cada oferta presentada por las tres empresas que remitieron información o estuvieron interesadas en la Propuesta.

INFORC ECUADOR®

Es una empresa ecuatoriana fundada en el año 2005, con experiencia en proveer servicios y productos para la seguridad de la información, consultoría, gestión de procesos, riesgos tecnológicos y auditorias de seguridad, soportados por la experiencia de nuestros especialistas y consultores, desde hace 10 años estamos colaborando con la seguridad de la información de empresas públicas y privadas del Ecuador.

Nuestra gestión se apoya en dos premisas básicas: Búsqueda permanente de la satisfacción del Cliente y Excelencia en la provisión de productos y prestación de servicios.

Nuestro personal, en su mayoría ingenieros y técnicos, fue seleccionado teniendo en cuenta una sólida formación en telecomunicaciones e informática y una marcada vocación de servicio. De esta manera aseguramos a nuestros clientes la comprensión de sus necesidades tecnológicas y una atención dedicada y profesional.

Quienes formamos parte de INFORC ECUADOR®, basados en el Sistema de la Gestión de la Calidad (en proceso de implantación de ISO 9001:2008).

En pocas palabras, algunas de las características de la solución MDM de INFORC ECUADOR® son: [7]

Implementación y Capacitación de todas las funciones de la solución MDM, entre las cuales destacan:

- Protección a varios niveles.
- Bloqueo de campañas de phishing y spam.
- Control del uso de Internet.
- Detección de liberación de dispositivos.
- Protección de datos en móviles desaparecidos.
- Gestión de aplicaciones móviles (MAM).
- Separación de las aplicaciones y los datos corporativos y personales.
- Protección de las aplicaciones y los datos almacenados en los contenedores.
- Prevención del acceso a las aplicaciones y los datos por parte de antiguos empleados.
- Control de aplicaciones.

[7] Datos de Propuesta presentada por INFORC ECUADOR®.

- Safe Browser.
- Compatibilidad de MDM con diferentes plataformas.
- Gestión inalámbrica de seguridad.
- Gestión centralizada.
- Control a través de un único panel centralizado.
- Ayuda para que los usuarios sean autosuficientes.
- División de responsabilidades entre los administradores.
- Activación de la gestión remota.

MOBILEIRON

MobileIron es la plataforma móvil de tecnologías de la información (TI) especialmente diseñada para que las empresas puedan asegurar y administrar aplicaciones móviles, contenido y dispositivos, a la vez que permite a sus empleados elegir sus dispositivos, mantener la privacidad y disfrutar de una experiencia de usuario nativa.

LA PLATAFORMA MOBILEIRON

La plataforma MobileIron se creó para asegurar y administrar sistemas operativos modernos en un mundo de dispositivos con diferentes usos. Incorpora la obligatoriedad de identidad, contexto y privacidad con el fin de establecer el nivel adecuado de acceso a los datos y servicios corporativos. MobileIron asegura los datos en reposo en el dispositivo, en las aplicaciones y el almacenamiento de la nube, además de proteger los datos en movimiento mientras se transfieren entre la red corporativa, los dispositivos y el almacenamiento en la nube. Con MobileIron, el área de informática puede asegurar la información corporativa esté donde esté, a la vez que mantiene la privacidad del empleado.

La plataforma MobileIron está formada por tres componentes de software integrados y distribuidos:

- MobileIron Core: un motor de políticas que permite al departamento informático definir la seguridad y las políticas de administración.
- MobileIron Client: el software en el dispositivo que garantiza el cumplimiento de dichas políticas en el mismo dispositivo.
- MobileIron Sentry: una puerta de enlace inteligente que asegura los datos a medida que se desplazan entre aplicaciones, dispositivos y la red corporativa.

En pocas palabras, algunas de las características de la solución MDM de MOBILEIRON son:[8]

- Core
- Sentry
- Apps@Work
- AppConnect
- Docs@Work
- Web@Work

GMS

Fundada en 1978, GMS es una de las empresas de seguridad informática de mayor trayectoria en la región. Nuestra visión es ser el líder a nivel regional de seguridad de la información que aporta de manera innovadora a la productividad de nuestros clientes.

Las redes actuales y las exigencias informáticas siguen haciéndose más complejas, pero la seguridad no tiene por qué serlo. No es necesario envolver los sistemas existentes con sistemas de seguridad nuevos. Hay una solución mejor.

Simplificada, potente y probada. Desde la red pasando por las estaciones de trabajo hacia la protección de los servidores, nuestros productos están diseñados para eliminar las complicaciones simplificando los flujos de trabajo. Los usuarios pierden menos tiempo

[8] Datos de Propuesta presentada por MOBILEIRON.

discutiendo con los administradores, los responsables informáticos dedican menos tiempo a solucionar problemas. Sophos UTM - Firewall de Próxima Generación, un todo-en-uno robusto y fácil de utilizar, escogido para proteger más de 100.000 redes a nivel mundial.

En pocas palabras, algunas de las características de la solución MDM de GMS son: [9]

- Essential Firewall (GRATUITO).- Ofrece funciones de seguridad básicas para ayudar a proteger una red corporativa, con funciones de networking, QoS automático, Stateful Packet Inspection, VPN para acceso remoto (PPTP/L2TP), reportes y administración 100% gráfica vía web.
- Network Protection.- Protección y administración avanzada de red, con IPS para prevenir más de 18.000 ataques, sistema avanzado contra Protección de Amenazas Persistentes (APT´s): Anti-Bot, One-Time Password (OTP) / autenticación de dos factores (2FA), control DoS, VPN (IPSec, SSL, sitio-a-sitio), balanceo de enlaces WAN, QoS avanzado, alta disponibilidad e integración a directorio activo.
- Mail Protection.- Filtra el correo electrónico desde y hacia la red contra spam, virus y phishing. Adicionalmente permite manejar cifrado SPX de una vía, sistema de prevención de fugas de información DLP e incluye un portal de usuario para facilitar la autogestión sin sobrecargar al administrador.
- Web Protection.- Optimiza el tráfico web con filtrado y categorización URL, control de aplicaciones IM y P2P, antivirus y antispyware. Permite la creación de reglas por usuarios, grupos y horarios, y se integra con el directorio activo. Autenticación de inicio de sesión único en modo transparente con Active Directory. Live AV Lookups and Sandbox Execution via Sophos Labs.
- Web Server Protection.- Protege servidores de aplicaciones publicados en la web contra ataques avanzados como inyecciones SQL y Cross Site Scripting (XSS).

[9] Datos de Propuesta presentada por GMS solución Sophos

Facilita la configuración con descubrimiento automático y reglas preestablecidas. Reverse Authentication (Authentication Offloading) para Web Server Protection.

- Wireless Protection.- Con Access Points (AP's) propietarios, provee administración centralizada y verdadera seguridad a redes inalámbricas. Soporta múltiples SSID's por equipo, roaming automático entre AP's, encripción avanzada y autenticación fuerte. El Sophos AP 50 tiene funcionalidades de repetidor y bridge.

Ninguna solución ofrece la flexibilidad de Sophos UTM en el momento de configurar una implementación. Además de poder combinar los módulos según los requerimientos de la empresa, Sophos UTM ofrece sus soluciones en modalidad de Hardware, Software y equipos virtuales (sobre todas las principales plataformas disponibles). La escalabilidad también es una gran ventaja, con soporte transparente.

3.2. CUANTIFICACIÓN METODOLOGÍA.

Dentro de la metodología de cuantificación se describen las medidas adoptadas para transformar todas las variables de las ofertas presentadas, en un modelo de cantidades cuantificables monetarias que pueden ser manipulados. Las variables pueden clasificarse en tangibles e intangibles.

3.2.1. TANGIBLES.

Los elementos tangibles incluyen la información que se puede cuantificar directamente porque ya se expresan en dinero. Una de estas variables es el costo real en dinero para la aplicación de la solución de MDM que se describe en la siguiente Tabla.

Tabla 3.1: Fijación de precios de las soluciones de MDM.

Compañía	Tipo	Costo ($)	Descripción
INFORC ECUADOR®	Local	10313.75	Tarifa por año
	Basado en la Nube	No Disponible	

Compañía	Tipo	Costo ($)	Descripción
MOBILEIRON	Local	44089.32	Tarifa Única
	Basado en la Nube	No Disponible	
GMS	Local	25042.86	Tarifa por año
	Basado en la Nube	No Disponible	

La información sobre precios de las tres empresas se obtuvo directamente de ellos. Se procedió a enviar correos electrónicos solicitando esta información y me proporcionaron la misma. Otros costos tangibles incluyen el costo de mantenimiento y de instalación que tiene que ser pagado directamente a las compañías de gestión de datos.

Otros costos tangibles adicionales vienen en el caso de que se realicen compras de dispositivos inteligentes para funcionarios y personal de la Agencia de Regulación y Control de las Telecomunicaciones.

3.2.2. INTANGIBLES.

En este tema se pueden analizar como costos intangibles, por ejemplo, se podría determinar como un costo intangible que la Agencia de Regulación y Control de las Telecomunicaciones tenga que instalar o actualizar una o varias aplicaciones, en esto está inmerso el tiempo que se tarda en descargar una determinada aplicación, el tiempo que ocupa el funcionario que realiza esta tarea.

Otro costo intangible es la seguridad de parámetros. Con el fin de cuantificar la seguridad se tendría que determinar el valor que las empresas tienen que pagar en promedio cuando se ven afectadas por un ataque de seguridad y la probabilidad de que este tipo de ataques podrían ocurrir.

3.3. MODELO SELECCIONADO.

En esta sección se procede a realizar un análisis de cada una de las propuestas presentadas, con la finalidad de llegar a determinar la más idónea y que se encuentre acorde a los requerimientos que la Agencia de Regulación y Control de las Telecomunicaciones plantea.

3.3.1. ANÁLISIS DE ESCENARIOS.

Para el modelo del costo, los sistemas de gestión de datos maestros serán analizados en dos escenarios diferentes:

Escenario i: Los dispositivos administrados serán adquiridos por la Agencia de Regulación y Control de las Telecomunicaciones y entregados a sus funcionarios. En este caso, la Agencia de Regulación y Control de las Telecomunicaciones tendrá que gastar dinero comprando dispositivos inteligentes (303 faltantes) además de adquirir el Sistema de Administración de Dispositivos Móviles (MDM). En este caso, ya que la Agencia proporciona los dispositivos, los usuarios estarán más dispuestos a aceptar que van a ser controlados por la solución MDM. Deberán tener entrenamiento para aprender a utilizar el sistema MDM. Si todos los dispositivos adquiridos pueden ser de la misma marca y las características específicas de los proveedores también pueden ser aprovechadas. La Agencia de Regulación y Control de las Telecomunicaciones podría adquirir una tableta o un smartphone para cada uno de los 303 funcionarios que no tendrían dispositivo móvil, ya que el resto de funcionarios tendría asignado el respectivo equipo. Entonces, el número total de dispositivos administrados será 526. Se procederá a entregar los dispositivos a todos los funcionarios que no disponen de teléfonos Smartphone institucionales, luego se podría ir renovando paulatinamente todos los terminales que se vayan discontinuando.

Escenario ii: Los dispositivos que disponen los funcionarios de la ARCOTEL se conectarán a la red y serán administrados. Este es el escenario BYOD porque la ARCOTEL

no proporcionará a sus funcionarios los dispositivos. En este caso, la Agencia de Regulación y Control de las Telecomunicaciones no tendrá que invertir en la compra de dispositivos móviles, ya que cada funcionario aporta su propio equipo. El reto aquí es la definición de las capacidades que el sistema MDM debe tener porque los funcionarios no se sienten cómodos con dar acceso a sus dispositivos personales de modo que la Agencia de Regulación y Control de las Telecomunicaciones instalará software adicional MDM. He aquí es necesaria una capacitación para aprender a utilizar el sistema MDM. En este caso, el número de dispositivos administrados es igual al número total de los teléfonos inteligentes y las tabletas conectadas a la red de la Agencia de Regulación y Control de las Telecomunicaciones que fue presentado anteriormente (526).

3.4. VARIABLES PARA EL ANÁLISIS.

Las variables a analizar en este caso se puede subdividir en dos categorías: los Costos Variables y las Variables de Beneficios.

3.4.1. LAS VARIABLES DE COSTOS.

Las variables de costos se refieren a los diferentes costos que la Agencia de Regulación y Control de las Telecomunicaciones deberá hacer frente, si una solución MDM es implementada. Hay tres subdivisiones de estas variables: Costos asumidos por la ARCOTEL al implementar la solución MDM. Costos en tiempo que va a ser utilizado por los funcionarios para hacer frente a la solución MDM. Los costos en sí que la Agencia tendrá que afrontar se refieren al tiempo que tendrán que invertir en el seguimiento y dar apoyo a la solución de MDM. Todos estos costos se consideran gastos de los funcionarios de las diferentes áreas.

Tabla 3.2: Costos establecidos a cada uno de los involucrados en la Implementación.

ARCOTEL	FUNCIONARIOS	DEPARTAMENTO DE TECNOLOGÍA
• Fijación de precios • Mantenimiento • Instalación • Formación • Soporte • Los teléfonos inteligentes • Las tabletas • Sitio web y no de alojamiento	• Configuración • Actualizaciones • Parches • Apoyo • Duración de la batería • Contraseña • Autenticación • Antivirus	• Aprovisionamiento • Software de supervisión • Soporte de Mesa de ayuda • Inventario de activos • Activación • Desactivación • Limpieza remota • Bloqueo remoto

Como hay costos para La Agencia, Los Funcionarios y El Departamento de Tecnológica, los costos totales se calcularon utilizando la siguiente formula:

$$Costos\ Totales = Costos_{Arcotel} + Costos_{Funcionarios} + Costos_{Departamento\ Tecnología}$$

Ecuación 3.1: Costos Totales.

Después de la cuantificación y la manipulación de las variables de costos en una hoja de cálculo de Microsoft Excel, los siguientes resultados para las soluciones de Administración de Dispositivos Móviles se obtuvieron y se presentan en las siguientes gráficas:

Escenario i:

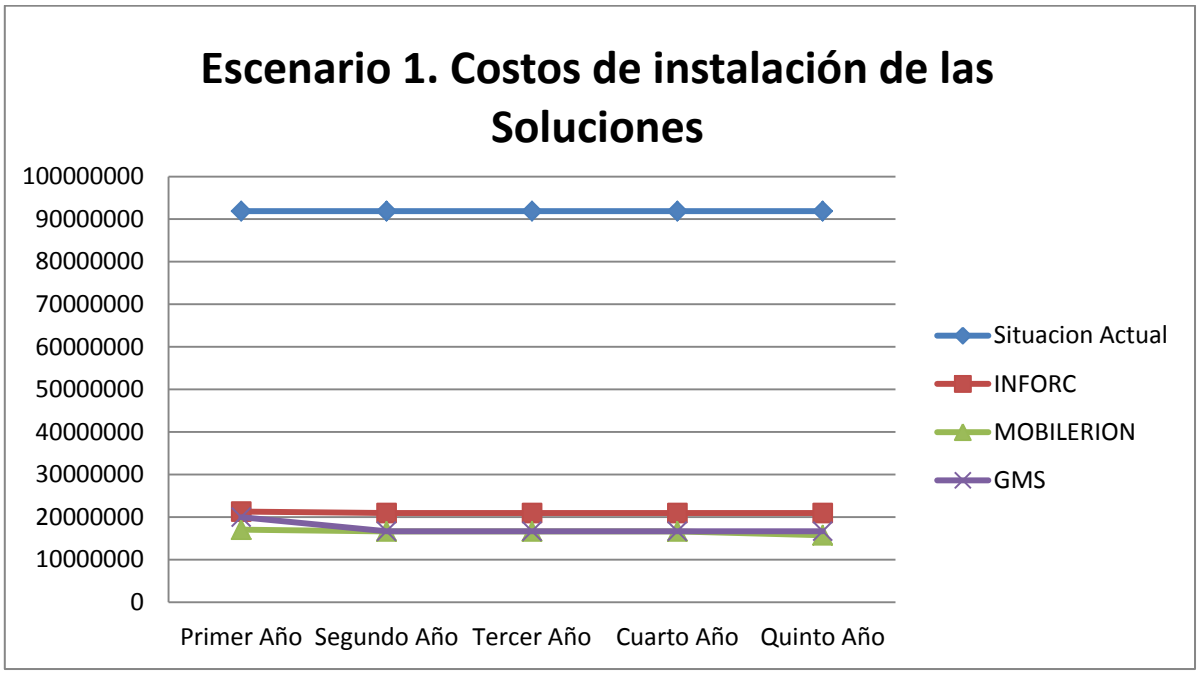


Figura 3.1: Costos de instalación de las Soluciones, Escenario 1.

Escenario ii:

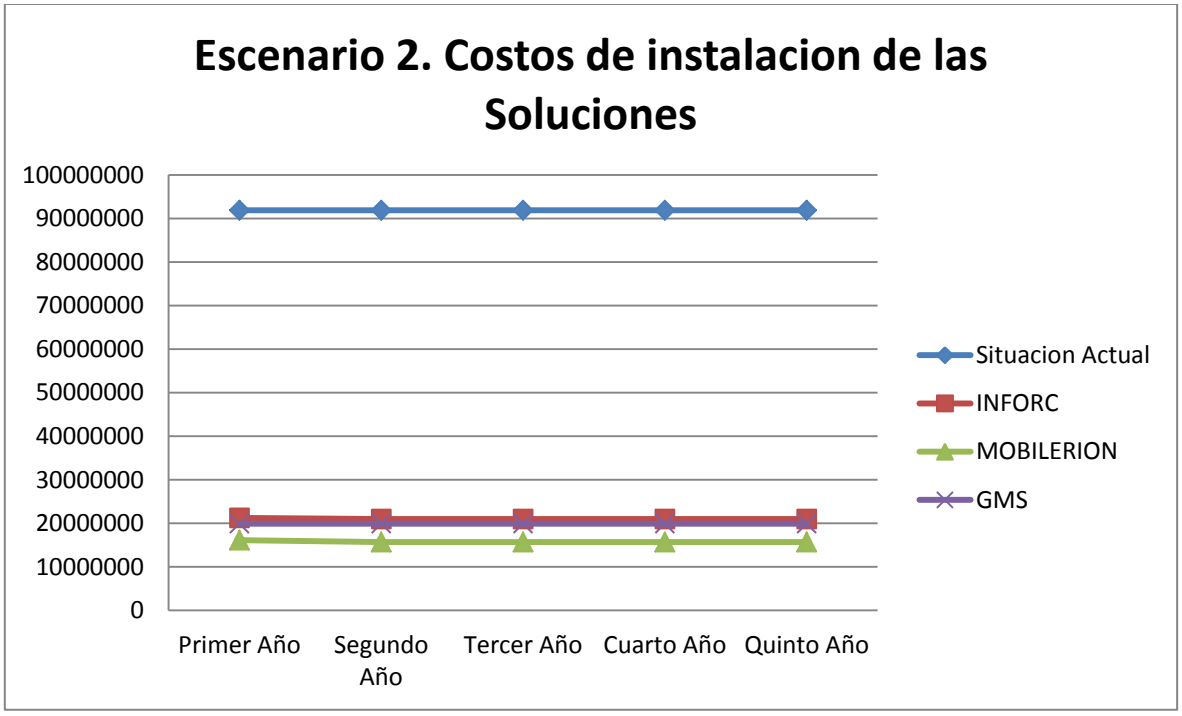


Figura 3.2: Costos de instalación de las Soluciones, Escenario 2.

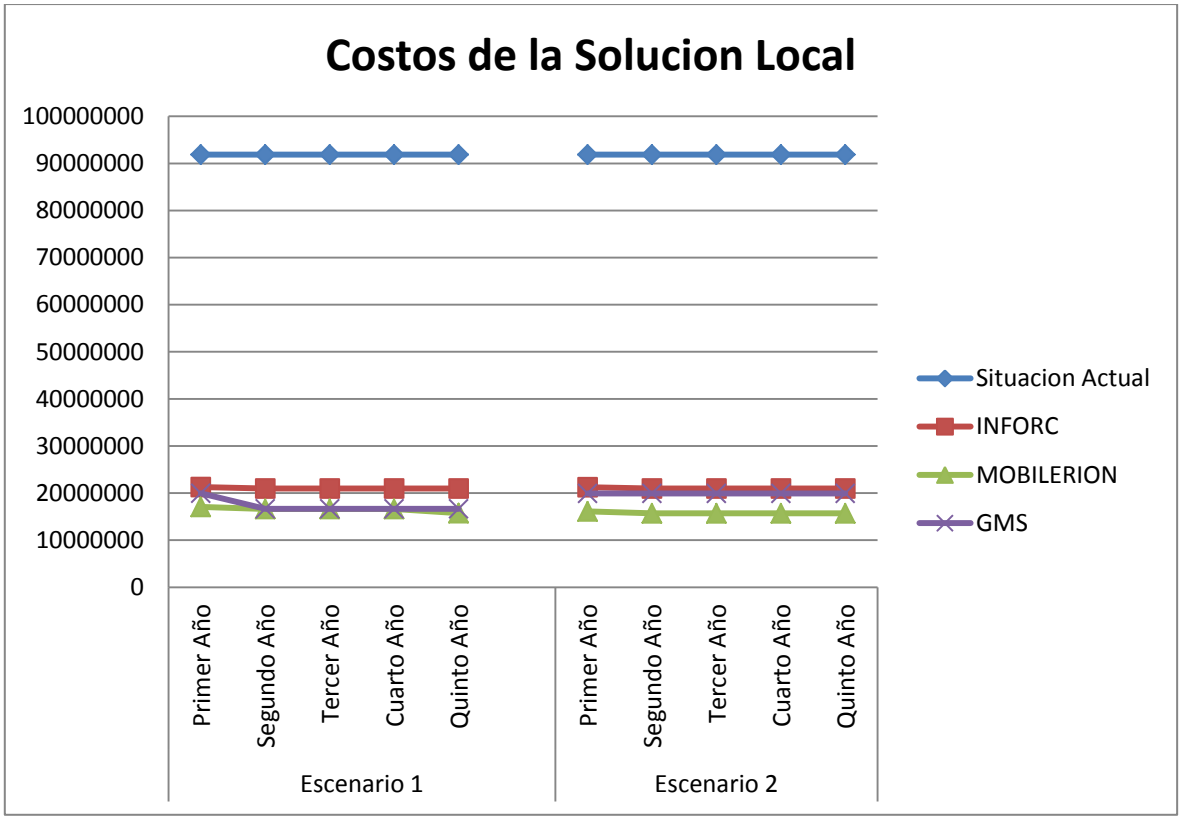


Figura 3.3: Costos de la Soluciones con implementación Local.

En la figura anterior se muestra la diferencia entre las dos opciones, la primera solución se basa en la instalación de la solución en equipos de ARCOTEL y la segunda en equipos de los usuarios. La diferencia de costos entre los dos escenarios proviene del hecho de que en el Escenario 1 la ARCOTEL tendrá que comprar dispositivos para los funcionarios.

3.4.2. LAS VARIABLES DE BENEFICIOS.

Dentro de esta categoría, se pueden analizar tres tipos de beneficios: Beneficios para la Agencia de Regulación y Control de las Telecomunicaciones, a los funcionarios, así como al administrador o funcionario de informática que administre el sistema. Los beneficios para la Agencia de Regulación y Control de las Telecomunicaciones se refieren a los costos que se pueden ahorrar debido a problemas de seguridad que van a ser evitados. Beneficios para los funcionarios están relacionados con el tiempo que los mismos van a ahorrar si se adopta una solución de Administración de Dispositivos Móviles MDM. Beneficios para su administrador

de informática, también incluyen el tiempo que va a ahorrar en trabajar con la solución MDM, ya que no tendrán que supervisar la red tan de cerca como lo hacen actualmente.

La lista de variables de beneficios se resume en la siguiente tabla, los mismos son constantes para todas las empresas, porque estas variables son comunes para todas.

Tabla 3.3: Beneficios atribuidos a cada uno de los involucrados en la Implementación.

ARCOTEL	FUNCIONARIOS	DEPARTAMENTO DE TECNOLOGÍA
• Evitar ataques de seguridad. • Tiempo de remediación	• Eficiencia • Productividad • Comunicaciones libres • Aplicaciones	• Menos apoyo en soporte

Como hay Beneficios para La Agencia, Los Funcionarios y El Departamento de Tecnológica, los Beneficios totales se calcularon utilizando la siguiente formula:

$$Benef\ Totales = Benef_{Arcotel} + Benef_{Funcionarios} + Benef_{Departamento\ Tecnología}$$

Ecuación 3.2: Beneficios Totales.

Gráficamente los beneficios que adquirirá la Agencia de Regulación y Control de las Telecomunicaciones se muestran en la siguiente figura.

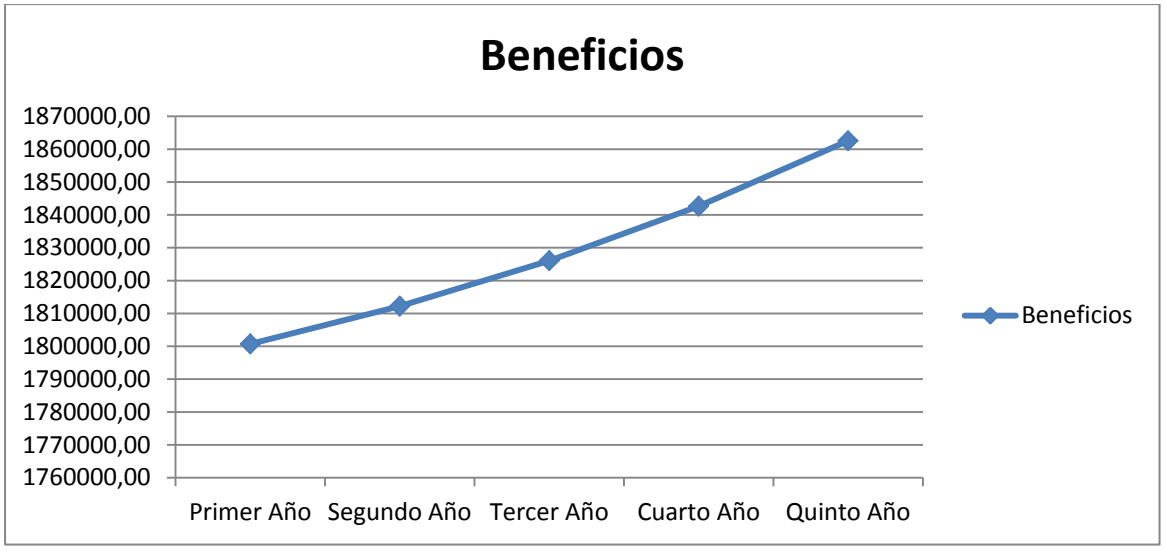


Figura 3.4: Beneficios en los próximos cinco años.

3.5. SECCIÓN DE ANÁLISIS.

La sección de análisis se divide en tres partes, Análisis Técnico, Análisis de los costos y Retorno de la inversión.

3.5.1. ANÁLISIS TÉCNICO.

En este caso vamos a realizar un análisis de acuerdo a las características técnicas del sistema MDM que cada empresa presenta en su oferta.

INFORC ECUADOR®

A continuación se detallan las características de la solución MDM de INFORC ECUADOR®:

- Protección a varios niveles.
- Bloqueo de campañas de phishing y spam.
- Control del uso de Internet.
- Detección de liberación de dispositivos.
- Protección de datos en móviles desaparecidos.
- Gestión de aplicaciones móviles (MAM).
- Separación de las aplicaciones y los datos corporativos y personales.

- Protección de las aplicaciones y los datos almacenados en los contenedores.
- Prevención del acceso a las aplicaciones y los datos por parte de antiguos empleados.
- Control de aplicaciones.
- Safe Browser.
- Compatibilidad de MDM con diferentes plataformas.
- Gestión inalámbrica de seguridad.
- Gestión centralizada.
- Control a través de un único panel centralizado.
- Ayuda para que los usuarios sean autosuficientes.
- División de responsabilidades entre los administradores.
- Activación de la gestión remota.

MOBILEIRON

A continuación se detallan las características de la solución MDM de MOBILEIRON:

- Asegurar y administrar los dispositivos móviles a través de múltiples sistemas operativos.
- Asegurar el correo electrónico corporativo, configuración automática de dispositivos, la seguridad basada en certificados.
- Borrar selectivamente los datos empresariales para ambos dispositivos corporativos y propiedad de los usuarios.
- Acceso, anotar y compartir documentos de correo electrónico, Sharepoint y otros sistemas de gestión de contenidos empresariales, así como el contenido que residen en el negocio y repositorios nube personales
- Adjuntos de correo electrónico seguras a través de la encriptación y sólo visible mediante aplicaciones autorizadas

- Acceso a contenido de la intranet corporativa con un navegador web seguro sin necesidad de un cliente VPN en el dispositivo

GMS

A continuación se detallan las características de la solución MDM de GMS:

- Essential Firewall (GRATUITO).
- Network Protection.
- Mail Protection.
- Web Protection.
- Web Server Protection.
- Wireless Protection.

De acuerdo al análisis efectuado a las propuestas presentadas, así como a las plataformas y conforme a reuniones efectuadas, se ha decidido que la oferta idónea para la necesidad de la ARCOTEL es la presentada por MOBILERION representada localmente por la empresa TAURUSTECH.

A continuación se presenta los equipos y requerimientos de red necesarios para la implementación del sistema para Administración de Sistemas Móviles:

Tabla 3.4: Características y requerimientos del sistema

Sistema			DISPONIBILIDAD IMPLEMENTACIÓN ARCOTEL
	Procesador	2.53 GHz Quad core Xeon CPU	SI
	Memoria	16 GB	SI
	Drives	2x 250 GB Enterprise Hard Disk Drives (RAID 1) 1x DVD drive	SI

Sistema			DISPONIBILIDAD IMPLEMENTACIÓN ARCOTEL
Chasis			SI
	Form Factor	19” 1U Rackmount	SI
	Dimensiones (D x H x W)	15.75” x 1.7” x 16.8” (400mm x 43mm x 426 mm)	SI
	Peso	17 lbs (7.7 kg)	SI
Panel anterior			SI
	Botones	Power On/Off	SI
	LEDs	Power LED System Overheat LED	SI
	USB	2x USB Ports	SI
	Serial	1x Serial Console (RJ45)	SI
Panel posterior			SI
	IPMI	Intelligent Platform Management Inter- face (IPMI) 2.0 with virtual media over LAN and KVM-over-LAN support; 1x 10/100BASE-T (RJ45)	SI
	Ethernet	2x 10/100/1000BASE-T (RJ45)	SI
	VGA	1x VGA (DB15)	SI
	PS/2	2x PS/2 keyboard and mouse ports	SI
	USB	2x USB Ports	SI

Sistema			DISPONIBILIDAD IMPLEMENTACIÓN ARCOTEL
	Serial	1x Serial port (DB9)	SI
Suministro de energía			SI
	Power	200 W maximum	SI
	Voltage	100 – 240V, 50-60Hz, 4 - 2 Amp Max	SI
	Connector	IEC 60320-C13	SI
Entorno Operativo			SI
	Operación	Temperature: 50° to 95°F (10° to 35°C) Relative Humidity: 8% to 90% (non-condensing)	SI
	No operar	Temperature: -40° to 158°F (-40° to 70°C) Relative Humidity: 5% to 95% (non-condensing)	SI
	Heat Output	682 BTU/hr (3.412 BTU/hr/W * 200 W)	SI

Todos los requerimientos necesarios manifestados anteriormente se pueden implementar en servidores de la Institución, sin embargo por razones de confidencialidad no es posible mostrar la estructura de la red de ARCOTEL, sin embargo se detalla a manera de check list en la tabla anterior las características que se pueden implementar.

3.5.2. NÚMERO DE DISPOSITIVOS ADMINISTRADOS.

De acuerdo al número de funcionarios que actualmente laboran en la Agencia de Regulación y Control de las Telecomunicaciones en cada una de las diferentes áreas el detalle del número de dispositivos a ser administrados por cada área de trabajo se encuentra como documento anexo.

3.5.3. ANÁLISIS DE COSTOS.

Una vez que se estableció el modelo del costo, es posible determinar los diferentes tipos de costos involucrados en la adopción de la solución MDM. Los costos incluyen:

COSTOS INICIALES: Se incluyen en esta categoría la instalación del sistema MDM y su configuración en los dispositivos y el aprovisionamiento de la red. También incluye los sistemas de gestión de datos maestros que se pueden comprar a perpetuidad.

COSTOS OPERACIONALES: Se incluyen los gastos operacionales que tienen que ser efectuados periódicamente, estos costos incluyen el mantenimiento y soporte del sistema. Además, las soluciones de gestión de datos maestros que tienen que ser pagados en forma mensual o anual.

COSTOS GENERALES: En estos costos se incluyen los costos que ya estaban considerados y no se tendrá que gastar de nuevo. Este es el caso de la instalación de los parámetros, el aprovisionamiento de la red y licencias para la situación actual de la ARCOTEL, es decir que estos costos ya se contemplaban en el pasado.

COSTOS DE OPORTUNIDAD: En estos costos están los asociados con la selección de una opción sobre otra. En el presente análisis, en el caso de permanecer con la situación actual, los costos de oportunidad incluyen el no tener que efectuar ningún gasto adicional para su operatividad.

COSTOS CORREGIDOS: Entre los costos fijos que tendrán que ser cubiertos, se pueden mencionar las soluciones MDM que se pueden comprar a través de un pago por única vez debido a que el valor de este parámetro no cambiaría en el futuro.

COSTOS VARIABLES: Los costos son variables cuando se pueden cambiar. Un costo variable proviene de la cantidad de dispositivos que serán administrados debido a que las empresas cobran en base al número de dispositivos. Entonces, si se gestionan más dispositivos, el precio se incrementará.

El análisis de costos también incluye el cálculo de los costos por usuario y los beneficios acumulados.

3.5.3.1. *COSTO POR USUARIO.*

Desde el modelo del costo planteado, el costo promedio por usuario también se puede obtener con el fin de determinar la cantidad que le costaría a la ARCOTEL la implementación de una solución MDM en cada dispositivo.

Los siguientes gráficos representan el costo de la implementación de una solución MDM por usuario. Hay gráficos por cada empresa y por cada Escenario. Para los dos escenarios, el número de dispositivos administrados es 526.

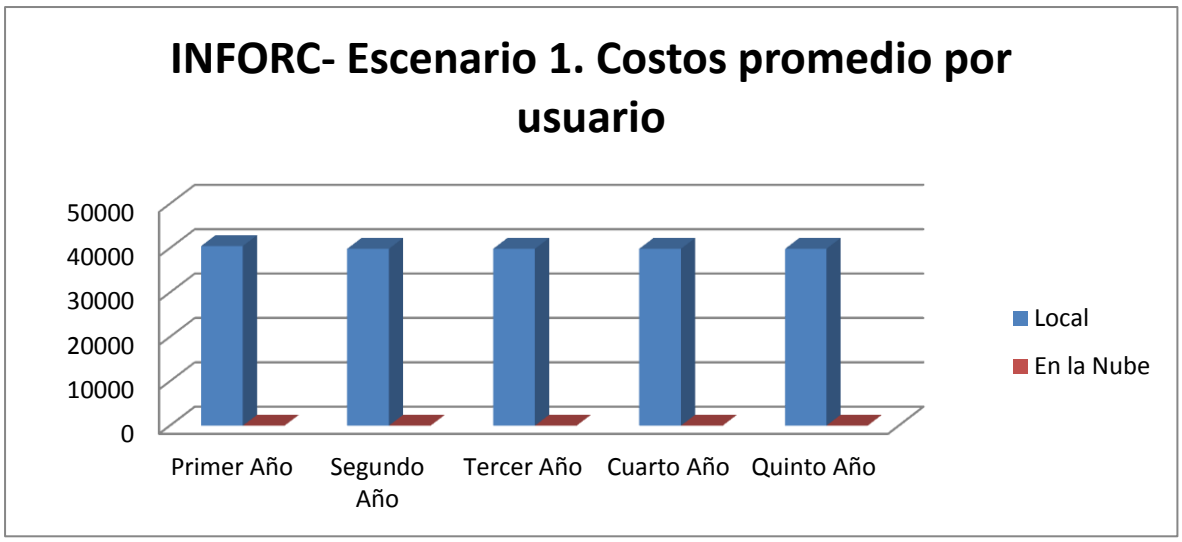


Figura 3.5: INFORC Costos promedio por usuario, Escenario 1.

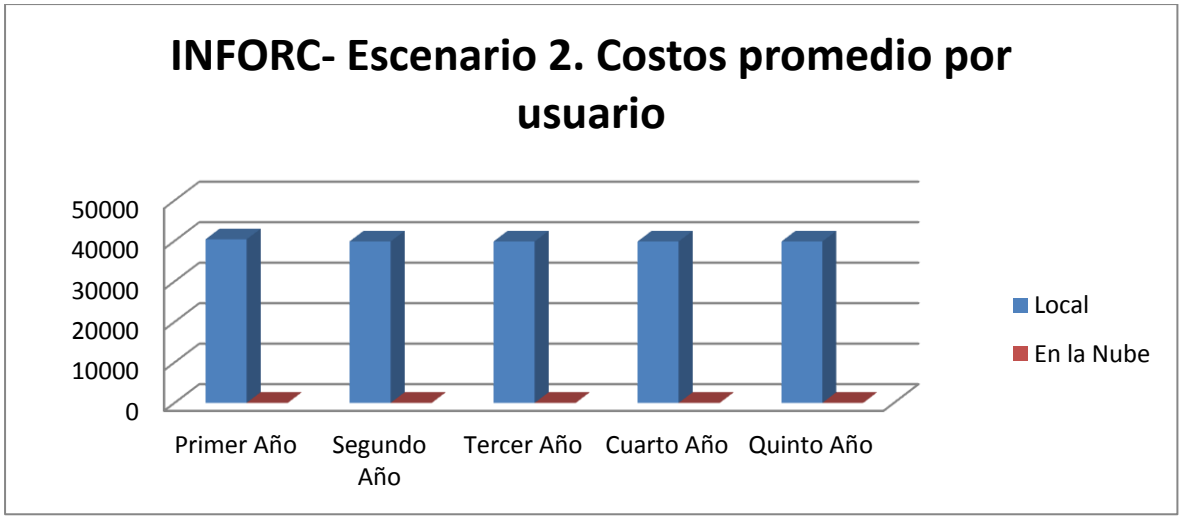


Figura 3.6: INFORC Costos promedio por usuario, Escenario 2.

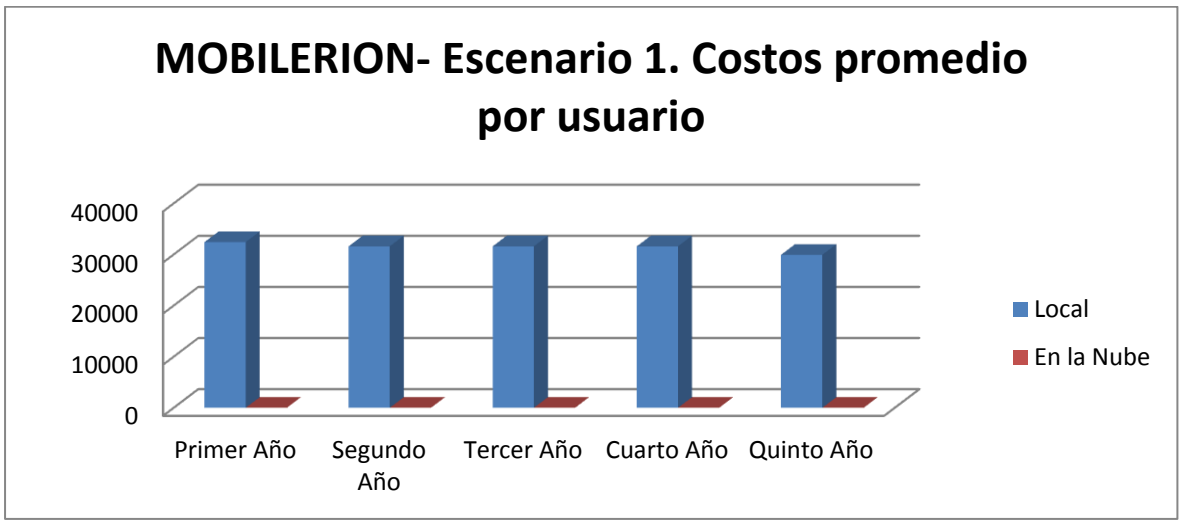


Figura 3.7: MOBILEIRON Costos promedio por usuario, Escenario 1.

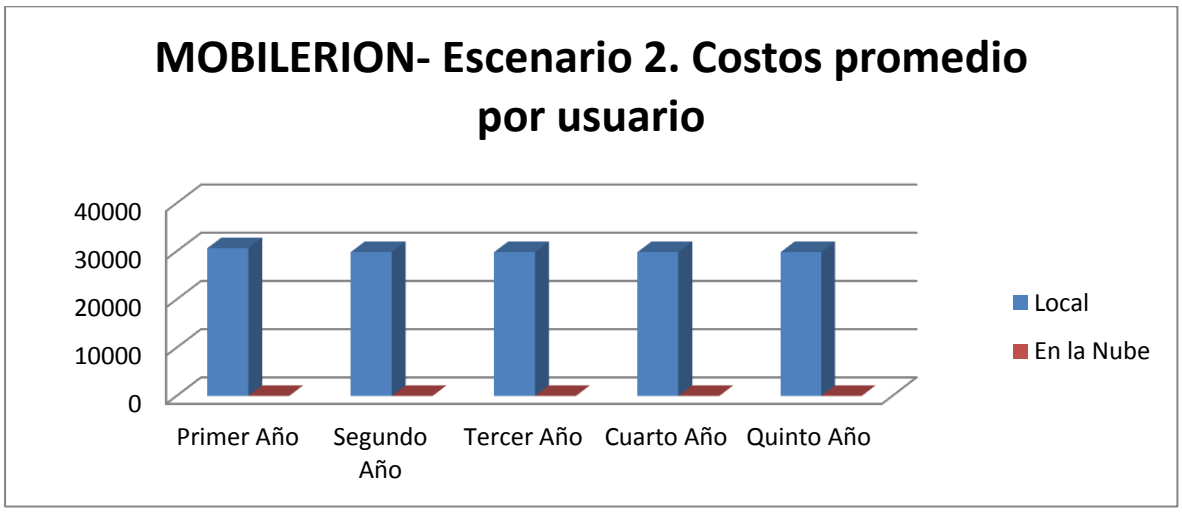


Figura 3.8: MOBILEIRON Costos promedio por usuario, Escenario 2.

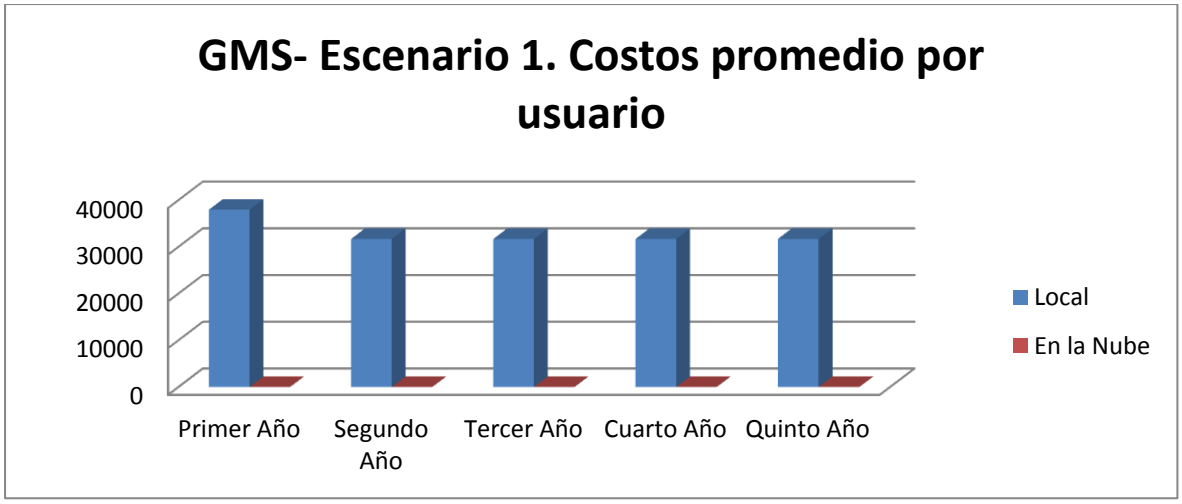


Figura 3.9: GMS Costos promedio por usuario, Escenario 1.

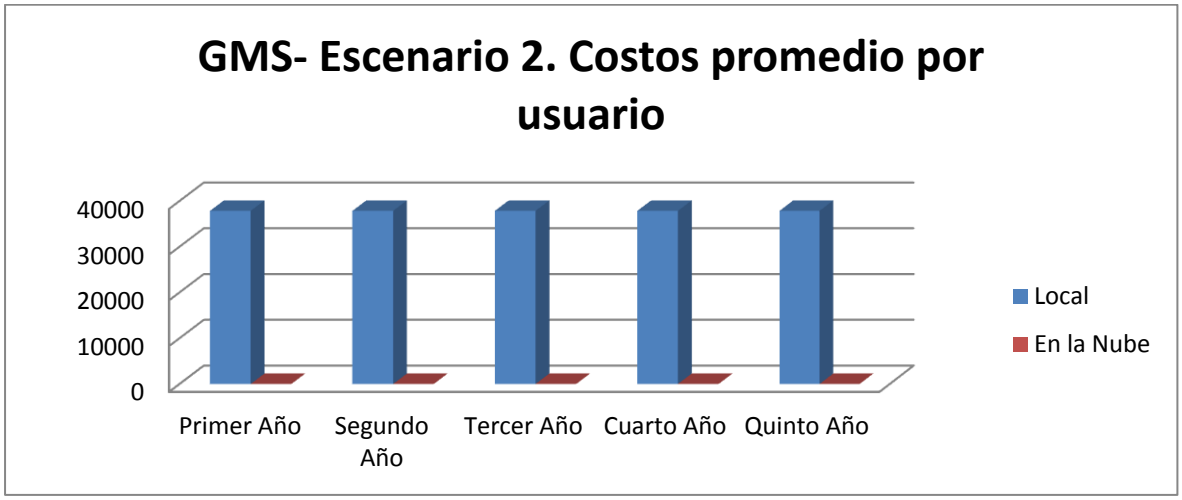


Figura 3.10: GMS Costos promedio por usuario, Escenario 2.

3.5.3.2. *COSTOS Y BENEFICIOS ACUMULADOS.*

Los costos y los beneficios acumulados representan los valores que tendrán que ser pagados por la ARCOTEL a las empresas de gestión de datos a través de los años. En otras palabras, los costos y los beneficios para el segundo año será la suma de los costes y beneficios de un año más los costos y beneficios de dos años y así sucesivamente.

Los costos acumulados y beneficios para las empresas se obtuvieron restando el valor de las prestaciones del valor de los costos, de acuerdo con la siguiente ecuación.

$$C\&B = Cost - Benefits$$

Ecuación 3.3: Costos versus Beneficios.

$$Acum\ C\&B_{x+1} = C\&B_{x+1} + C\&B_x$$

Ecuación 3.4: Costos versus Beneficios Acumulados.

Donde C & B es el valor de los costos menos los beneficios, y la ecuación anterior muestra que el coste acumulativo y el beneficio (Cum C & B) del año 2 es igual a la suma de C & B para el año 2 y C & B para el año 1.

Las siguientes figuras muestran los costos acumulativos obtenidos para los tres proveedores de soluciones MDM y la situación actual.

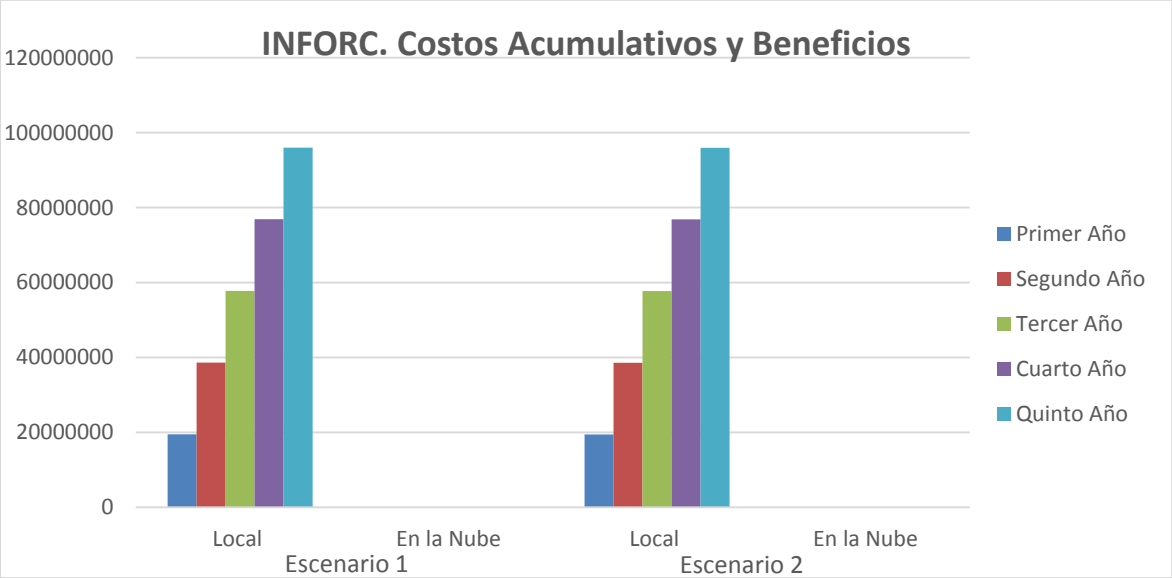


Figura 3.11: INFORC Costos Acumulados y Beneficios.

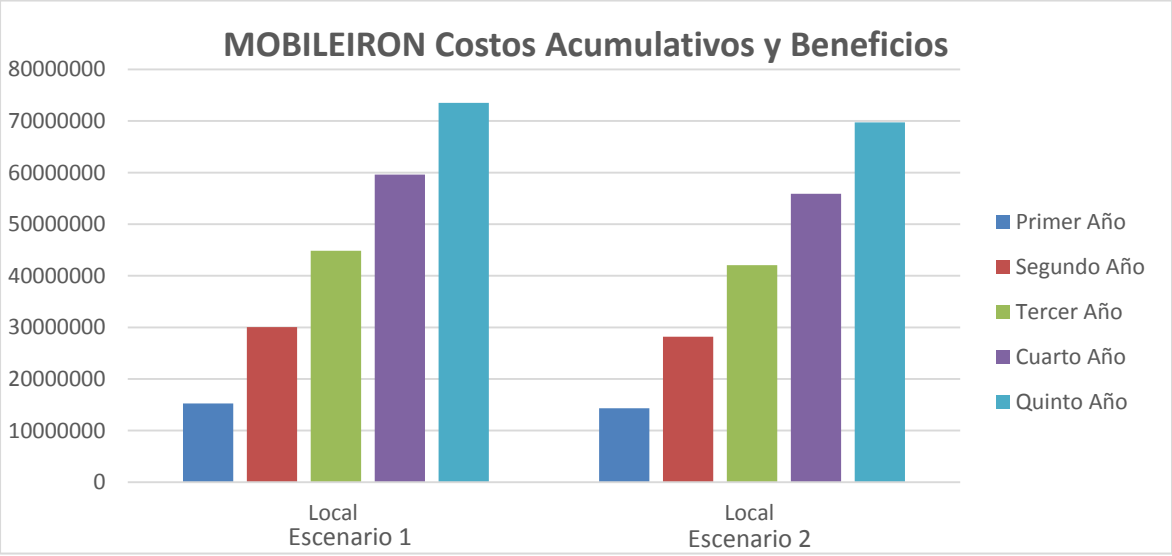


Figura 3.12: MOBILLEIRON Costos Acumulados y Beneficios.

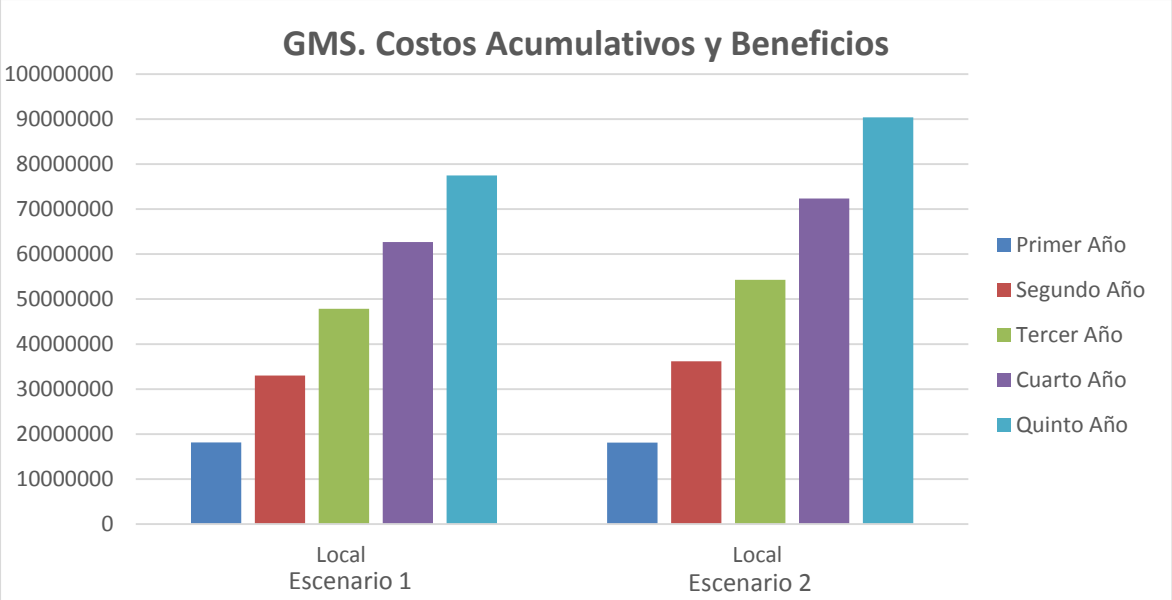


Figura 3.13: GMS Costos Acumulados y Beneficios.

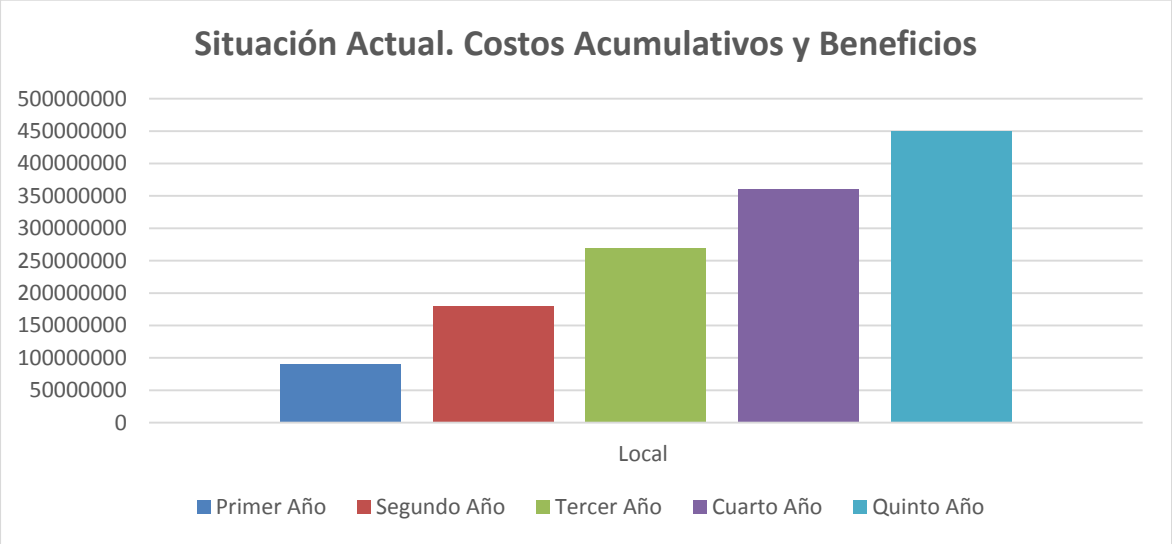


Figura 3.14: Situación Actual Costos Acumulados y Beneficios.

3.5.4. PRODUCTIVIDAD DEL SISTEMA

Uno de los mayores beneficios que se pueden obtener al implementar una solución MDM, es el aumento de la productividad de los funcionarios. La productividad se puede mejorar ya que los funcionarios pueden tener acceso a la información corporativa y llevar a cabo actividades relacionadas con su puesto de trabajo sin la necesidad de estar en la oficina y también pueden trabajar después de su jornada de trabajo. Por ejemplo, pueden trabajar desde sus hogares o fuera de horarios de oficina.

En el modelo del costo original, se consideró que los funcionarios mejoran su productividad una hora por mes. En el análisis de sensibilidad de este número se duplicó a dos horas al mes y los nuevos valores de retorno de la inversión se muestra en la siguientes figuras.

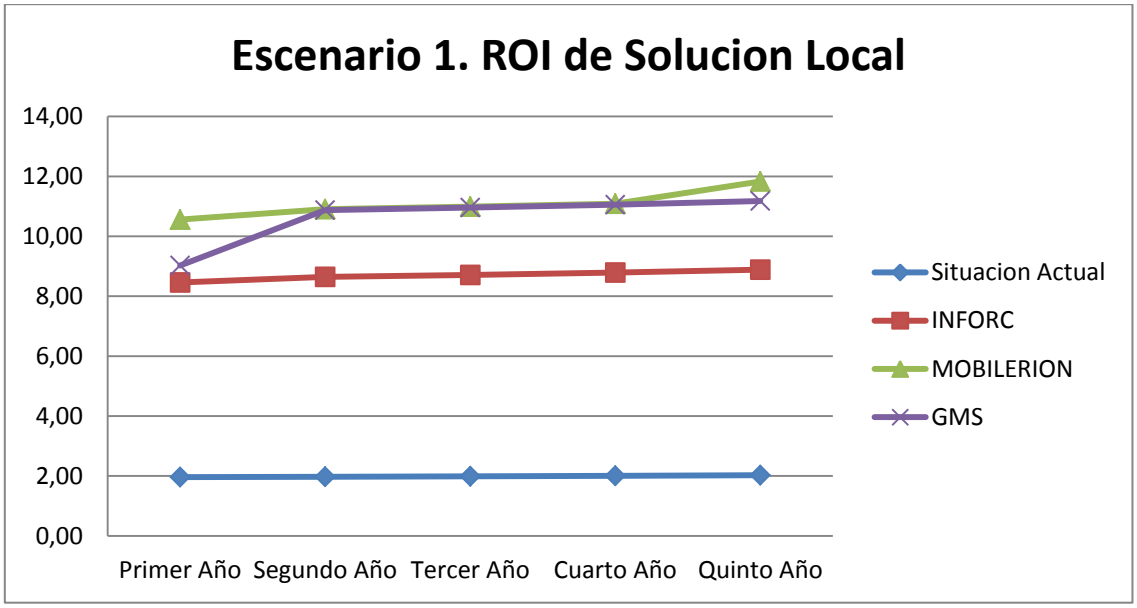


Figura 3.15: Retorno de la Inversión en la Solución Local escenario 1.

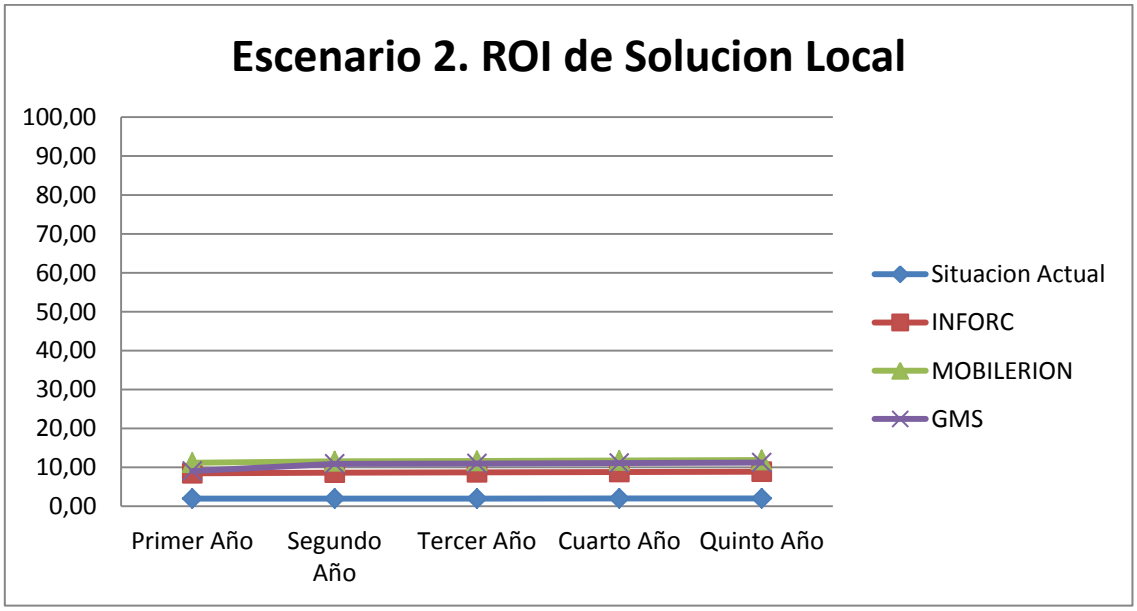


Figura 3.16: Retorno de la Inversión en la Solución Local escenario 2.

Cuando se aumenta el número de horas de mayor productividad, los valores de retorno de la inversión también aumentan en todos los casos. La comparación de los valores de retorno de la inversión entre el parámetro original de la productividad (izquierda) y cuando se incrementa el parámetro (a la derecha) se puede ver en la siguiente figura.

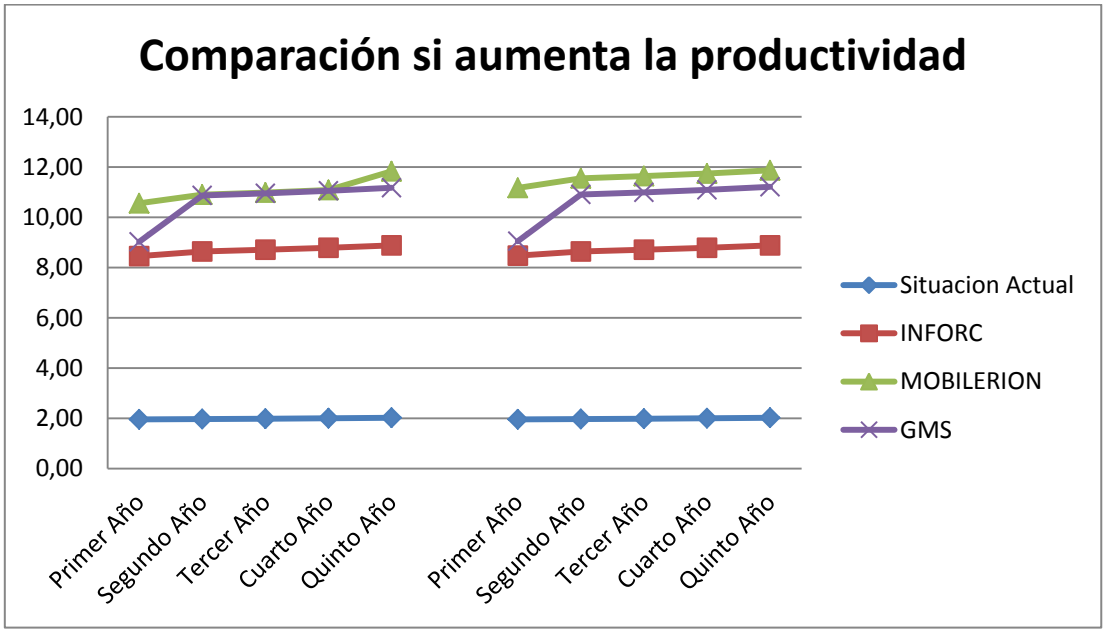


Figura 3.17: Comparación si aumentamos la productividad.

Cuando se aumenta la productividad, el valor de retorno de la inversión se incrementó también. De hecho, en el año 5 del retorno de la inversión supera el 100 %, lo que significa que los beneficios recibidos por la implementación de un sistema MDM son más altos que los costos que tienen que pagar por su adopción.

Los valores totales de los costos y el valor total de los beneficios no se pueden utilizar para determinar si es o no es una buena idea adoptar un sistema MDM.

Debido a las características del problema que se plantea resolver y por estar implicada la implementación de tecnología, la mejor métrica para determinar una decisión es calcular el retorno de la inversión (ROI) para todos los casos.

En el retorno de la inversión se comparan los beneficios a los costos y expresar el resultado en porcentaje utilizando la siguiente Ecuación:

$$ROI = \frac{Beneficios}{Costos}\%$$

Ecuación 3.5: Retorno de la Inversión.

Cuando se comparan dos valores de retorno de la inversión, la más alta de ellas, es la mejor opción, ya que significa que más beneficios se reciben en comparación con los costos que tienen que ser pagados.

Debido a que el retorno de la inversión es la medida clave para este modelo de costos, los gráficos de los resultados de los cálculos estarán acompañados de tablas que especifican los valores numéricos.

Los ejes de los gráficos han sido alterados para mostrar claramente los valores de retorno de la inversión, pero ya que son porcentajes, que originalmente ir de 0 a 100. Los resultados se resumen en las siguientes de tablas y correspondientemente se muestra en las siguientes figuras.

Tabla 3.5: Escenario 1 Tasa de Retorno de Capital.

Escenario 1. ROI de Solución Local					
	Primer Año	Segundo Año	Tercer Año	Cuarto Año	Quinto Año
Situación Actual	1,96	1,97	1,99	2,01	2,03
INFORC	8,46	8,65	8,71	8,79	8,89
MOBILERION	10,56	10,91	10,99	11,09	11,83
GMS	9,02	10,87	10,96	11,06	11,18

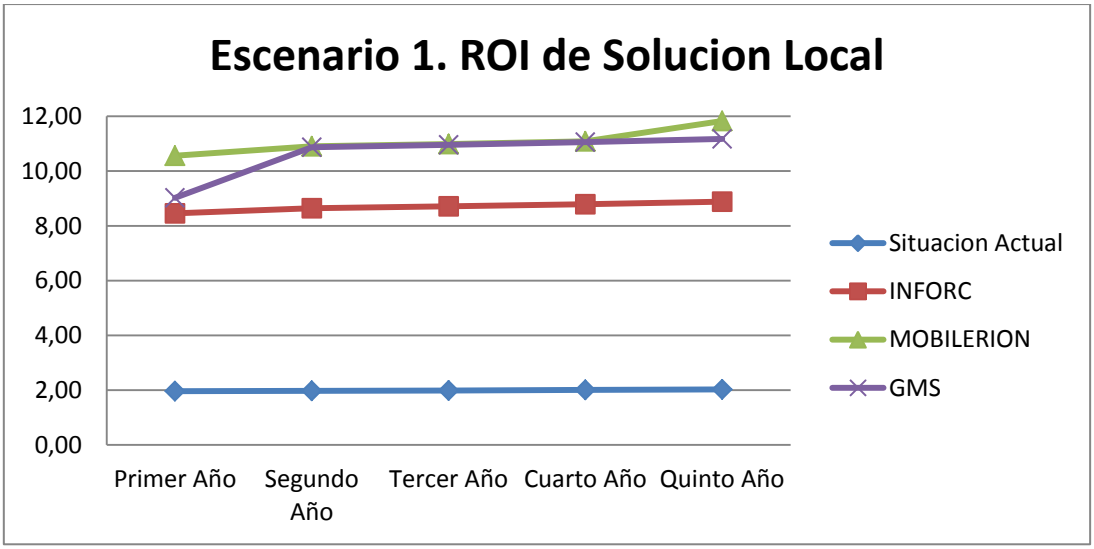


Figura 3.18: Retorno de Inversión solución Local Escenario 1.

Tabla 3.6: Escenario 2 Tasa de Retorno de Capital.

Escenario 2. ROI de Solución Local					
	Primer Año	Segundo Año	Tercer Año	Cuarto Año	Quinto Año
Situación Actual	1,96	1,97	1,99	2,01	2,03
INFORC	8,48	8,65	8,71	8,79	8,89
MOBILERION	11,17	11,55	11,64	11,75	11,87
GMS	9,05	10,91	10,99	11,09	11,21

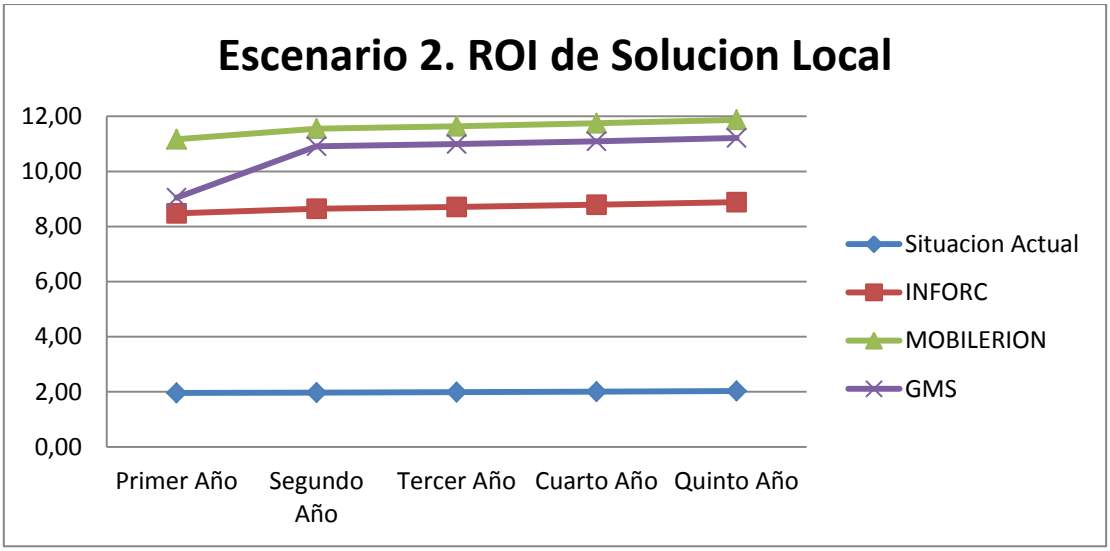


Figura 3.19: Retorno de Inversión solución Local Escenario 2.

CAPÍTULO IV.

4. PROPUESTA DE IMPLEMENTACIÓN DE LA PLATAFORMA DE ADMINISTRACIÓN DE DISPOSITIVOS MOVILES.

En este capítulo vamos a proceder a seleccionar una de las propuestas planteadas, una vez que se validó los análisis correspondientes en el capítulo anterior.

4.1. PLATAFORMA ELEGIDA PARA LA IMPLEMENTACION.

Luego del análisis realizado se ha llegado a determinar que la plataforma que le convendría elegir a la ARCOTEL, ya sea por el costo y los beneficios que esta puede ofrecer es la Propuesta presentada por la empresa MOBILERION, representada localmente por la empresa TAURUSTECH, lo relacionado a este análisis se encuentra plasmado en el capítulo anterior, donde se puede validar que se realizaron análisis de Costos, beneficios y el retorno del capital mediante las investigaciones del ROI.

4.1.1. ANÁLISIS DE LOS BENEFICIOS QUE IMPLICARÍA LA IMPLEMENTACIÓN DE LA MISMA.

Luego de la revisión de las tres ofertas presentadas se procedió a validar características técnicas, costos y beneficios que cada una tiene al momento de implementarla en la institución, es por lo cual a continuación se enlistan algunas bondades de la opción escogida.

Entre los beneficios que la oferta presentada por MOBILERION a través de su filial la empresa local TAURUSTECH son los siguientes:

EVOLUCIÓN A GESTIÓN DE MOVILIDAD EMPRESARIAL.

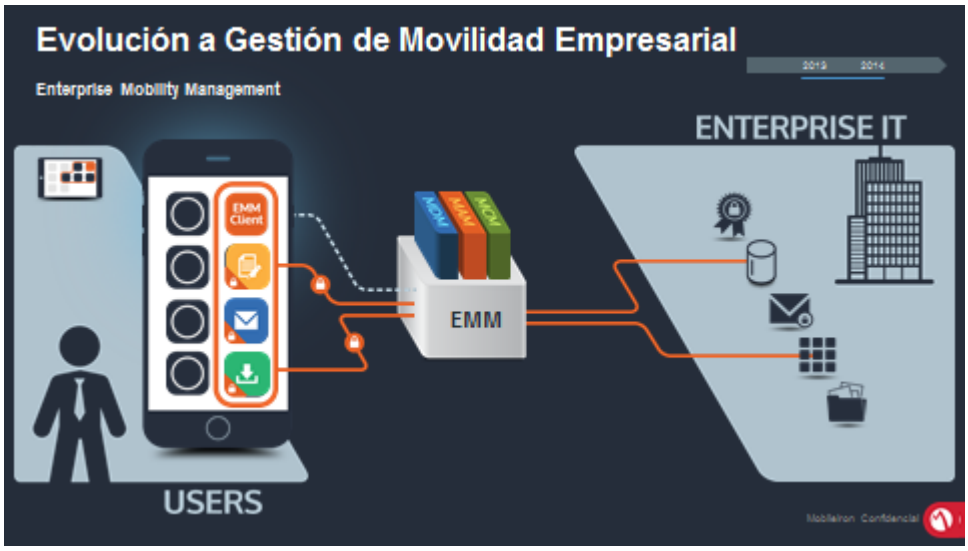


Figura 4.1: Evolución a Gestión de Movilidad Empresarial.

A partir de 2013-2014, entramos en la era de Enterprise Mobility Management (EMM), que se expandió más allá de administración de dispositivos móviles (MDM) para la Gestión de aplicaciones, (MAM) y Mobile Content Management (MCM).

MDM: Mobile administración de dispositivos (MDM) es generalmente la base de una solución moderna de gestión de movilidad empresarial (EMM) que permite a las organizaciones que sus empleados productivos en los dispositivos que les encanta usar. Una plataforma EMM debe abordar los costos, riesgos de seguridad, y los desafíos de gestión asociados a la adopción móvil que las herramientas tradicionales de TI no pueden abordar.

MAM: Luego viene la administración de aplicaciones móviles. Con la proliferación de dispositivos en la empresa, y las expectativas del usuario de utilizar aplicaciones relacionadas con el trabajo fácilmente en el dispositivo móvil, la necesidad de una gestión de aplicaciones móviles (MAM) y la seguridad también ha crecido. Una solución MAM exitosa entrega una aplicación empresarial ejemplar, con la capacidad de asegurar las aplicaciones en el dispositivo, autenticar a los usuarios finales, de negocio independiente y aplicaciones personales, y retirarse aplicaciones cuando sea necesario. MAM ayuda a la Tecnología de la

Información a gestionar todo el ciclo de vida de las aplicaciones disponibles en la App empresa, asegurar las aplicaciones en el dispositivo, la aplicación de autenticación de usuario, aislándolos de aplicaciones personales, para proceder a su amortización. Cuando el usuario se dispara a su dispositivo y se autentica, la empresa se puede instalar en el dispositivo en forma de una aplicación para que los usuarios finales puedan buscar e instalar las aplicaciones móviles a su disposición. También, dependiendo de la función del usuario final en la organización, la solución MAM instala automáticamente las aplicaciones móviles que han sido asignados a ese usuario final de forma predeterminada. Datos de la empresa sólo se pueden intercambiar entre las aplicaciones que forman parte de un contenedor seguro en el dispositivo.

MCM: Como móvil se convierte en la plataforma informática preferida, los usuarios finales esperan que el acceso a los tiempos esenciales y, a menudo, los documentos confidenciales en sus dispositivos. Para ayudar a las Tecnología de la Información a asegurar los datos corporativos sin comprometer la experiencia del usuario final, una solución eficaz MCM ofrece la posibilidad de:

- Acceso, anotar y compartir documentos de correo electrónico, Sharepoint y otros sistemas de gestión de contenidos empresariales, así como el contenido que residen en el negocio y repositorios o nube personales.
- Adjuntos de correo electrónico seguras a través de la encriptación y sólo visible mediante aplicaciones autorizadas.
- Acceso al contenido de la intranet corporativa con un navegador web seguro sin necesidad de un cliente VPN en el dispositivo.

Con una solución de gestión de contenidos móviles los usuarios finales pueden tener una forma intuitiva de acceso, anotar y compartir documentos de correo electrónico, SharePoint, y una variedad de otros sistemas de gestión de contenido empresarial. Con el

tiempo a medida que más y más usuarios finales utilizan la nube personal, como Dropbox, Box, OneDrive Pro y Office 365, las organizaciones necesitan una manera de asegurar la nube personal también. Con MCM, el administrador de la Tecnología de la Información puede establecer la prevención de pérdida de datos (DLP), controla para proteger a estos documentos de distribución no autorizada.

Los empleados pueden sacar el máximo provecho de sus dispositivos móviles para contenido empresarial seguro y colaboración. Archivos adjuntos de correo electrónico pueden ser encriptados y sólo se pueden ver con aplicaciones autorizadas que son administrados por la plataforma EMM.

REQUISITOS PARA ASEGURAR LA INFORMACIÓN EN TODAS PARTES.

Figura 4.2: Requisitos para asegurar la información.

Con el fin de cumplir con este nuevo requisito de seguridad de la información en todas partes, es necesario que existan tres elementos claves en su lugar cuando la captación y gestión de la información empresarial en un escenario móvil.

Políticas: En primer lugar, en este caso ARCOTEL debe establecer políticas que dictan las normas de seguridad y de gestión que rigen la forma en la cual los datos e información se trasladarán a los funcionarios y sus dispositivos móviles.

En esencia, un motor de seguridad y gestión puede manejar una amplia gama de sistemas operativos móviles, y se sienta entre los dispositivos de los funcionarios y los recursos de la empresa (como Directorio Activo, etc.). Este motor es el cerebro de la operación donde se definen las políticas de gestión de aplicaciones, documentos y dispositivos que determina que los usuarios pueden acceder, y con qué nivel de seguridad. Las políticas de seguridad se pueden cambiar dinámicamente en tiempo de ejecución. Es decir, el motor puede recopilar y mostrar la analítica sobre lo que ocurre al otro lado de los usuarios, dispositivos, aplicaciones y contenidos.

Aplicación: En el dispositivo, es necesario que haya un cliente seguro de que los usuarios pueden descargar de una tienda de aplicaciones empresarial.

Una vez que el cliente se instala en el dispositivo, a los usuarios se les puede pedir autenticarse. Una vez autenticado, el cliente descarga las políticas del motor de seguridad y la gestión y de esta manera empezar a hacer cumplir esas políticas de seguridad, administración y configuraciones. Así, por ejemplo, se puede empezar a configurar correo electrónico para que la empresa de correo electrónico comience a fluir en el dispositivo móvil de forma automática y segura.

También puede configurar Wifi, contraseñas y crear un contenedor seguro para que más tarde, si se añaden otras aplicaciones empresariales, que se pueden añadir a ese contenedor seguro en el dispositivo y permitir que los datos pueden compartir entre aplicaciones dentro del contenedor seguro.

Control de acceso: Esto sería lo último, debido a que debe existir una manera de gestionar y ejecutar el control de acceso a la información sensible desde el móvil. Esto se puede hacer con una puerta de enlace inteligente que gestiona el tráfico entre los dispositivos y recursos. Aquí pueden ocurrir dos cosas:

- El cifrado se despliega y la seguridad está garantizada por los datos en movimiento, etc..., y,
- La postura dispositivo se puede evaluar en tiempo real y las políticas de seguridad se implementan desde el motor de seguridad / gestión de datos en movimiento. Así, por ejemplo, si un dispositivo móvil ha caído fuera de cumplimiento, la puerta de entrada inteligente puede captar que en base a la información enviada a través del motor de seguridad y el acceso a los recursos corporativos y la información se bloquea inmediatamente.

Como se menciona anteriormente, la gran importancia de esta arquitectura general es debido a que debemos tener en cuenta el problema de la seguridad de los datos y aplicaciones a través de cualquier tipo de dispositivo, por lo tanto se debe cumplir con estos tres elementos de la arquitectura EMM, de no ser así, no es posible hacer cumplir las políticas y garantizar la seguridad en tiempo real descritas anteriormente. Sin una puerta de enlace inteligente, los datos en movimiento no se pueden asegurar y pueden existir ataques a su red. Es por eso que la administración de dispositivos móviles tiene gran importancia.

PLATAFORMA MOBILEIRON

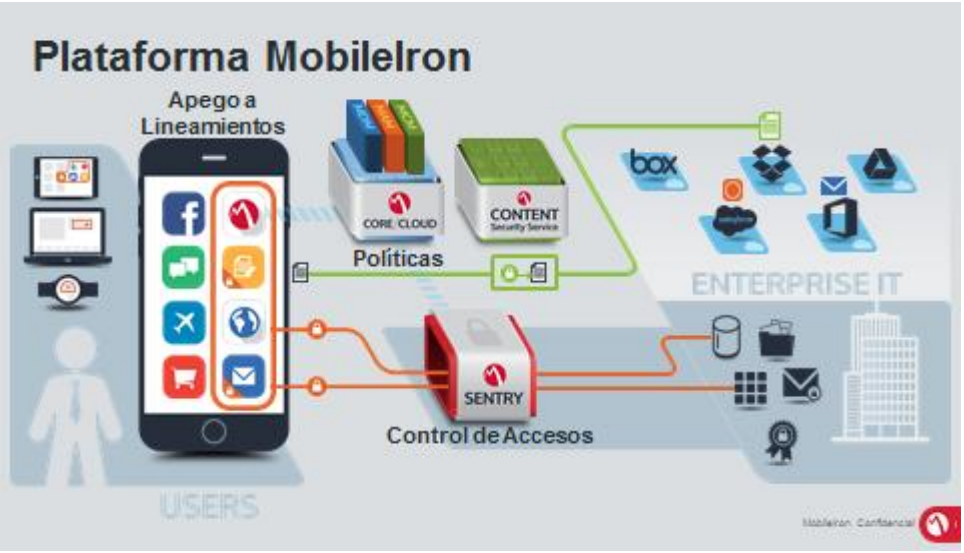


Figura 4.3: Plataforma MOBILEIRON.

Con esta arquitectura, las empresas pueden implementar EMM y Servicios de seguridad, necesarios para asegurar y administrar información de la empresa en el móvil.

Cliente MobileIron (iOS, Android o Windows Phone 8.1) permiten la aplicación en el dispositivo.

MobileIron Sentry actúa como puerta de entrada inteligente que proporciona control de acceso en tiempo seguro y verdadero.

Y MobileIron Content Security Service responde a la preocupación de la pérdida de datos (causada por los documentos de la empresa de ser colocados en servicios en la nube personales), proporcionando tanto la seguridad a nivel de documento y la estrecha integración en una plataforma EMM necesaria para proteger el contenido de la empresa a través de servicios en la nube personales comunes.

EXTENSION DE LA PLATAFORMA MOBILEIRON

Figura 4.4: Extensión de la Plataforma MOBILEIRON.

Mobileiron tiene una gran cantidad de puntos de contacto. Y sabemos que no podemos resolver todos los casos por nosotros mismos. Es por eso que hemos construido la plataforma para ser extensible en el lado del cliente. Así que ofrecemos a nuestros clientes, desarrolladores de aplicaciones móviles con SDK y un envoltorio para que puedan permitir que sus aplicaciones sean gestionadas por nosotros. Así por ejemplo, es Breezy (para

imprimir) en la App Store. Cuando se llega al dispositivo, si tenemos presente, entonces lo primero que hará es buscar el cliente MobileIron. El cliente MobileIron descargará configurar la aplicación, descargue las políticas, por ejemplo, si tiene una política de copiar y pegar, como si usted no quiere que la gente sea capaz de copiar y pegar información exterior del contenedor luego Breezy heredará que la política también. Y como los datos se mueve hacia atrás y hacia adelante entre la aplicación que se ha envuelto o construido usando nuestro SDK, entonces la información será encriptada por Sentry.

También tenemos la extensibilidad del lado del servidor. Ofrecemos API que permiten que un cliente utilice herramientas de scripting para automatizar la gestión, la integración con otras consolas de administración y cosas por el estilo, pero también damos las API para nuestros asociados que pueden utilizarlos para enriquecer sus soluciones tales como gestión de redes, herramientas de monitoreo de redes de Cisco o Juniper o Aruba o soluciones de reputación de aplicaciones. Pueden enriquecer su solución con información sobre la infraestructura móvil y ustedes, nuestros clientes y clientes potenciales proporcionar, con un valor adicional.

AMPLIO ECOSISTEMA DE PARTNERS OFRECEN ELECCIÓN

Figura 4.5: Ecosistema de Partners a Elección.

Esta es una selección de los socios que se han integrado con Mobileiron y van añadiendo el número de parejas que quieren integrarse para hacer su aplicación en el cliente empresa listo y seguro, y en el lado del servidor para que existan soluciones más móvil conscientes.

ALIANZAS CON LOS LÍDERES

Figura 4.6: Alianzas con Líderes.

MobileIron continúa asociándose con los proveedores líderes de sistemas operativos móviles para ayudar a entregar elección a las empresas sin comprometer la seguridad.

Se encuentra acelerando los despliegues empresariales con soporte para iOS 8: Con iOS 8 en 2014 formaba seguridad mejorada, una mayor gestión de dispositivos, 4.000 nuevas APIs para desarrolladores, publicación de contenidos empresariales, y las nuevas de salud y el hogar aplicaciones críticas para la vida. A fin de que las capacidades de seguridad móviles de una nueva empresa necesita una plataforma EMM como MobileIron, para hacerlo Mobileiron sigue siendo un socio muy estrechamente con Apple en estos desarrollos.

Minimizar la fragmentación con AppConnect y apoyo para Android para el Trabajo y Samsung Knox: Android para el Trabajo, es un nuevo programa de la empresa, puesto en marcha en 2015, diseñado para aumentar la adopción de Android, permitiendo la gestión de

Tecnologías de la Información uniforme y distribución de aplicaciones segura a través de un ecosistema de proveedores de EMM. Con Android para el Trabajo, que se pone de manera unificada para asegurar aplicaciones empresariales, gestionar dispositivos dispares, y el trabajo independiente y los datos personales a nivel de sistema operativo. Los trabajadores se benefician del acceso a las aplicaciones que aman, en una interfaz de usuario unificada nativa. Permite seguro, el despliegue de aplicaciones en contenedores a una gama de dispositivos Android corriendo 4.0, a Android Lollipop. Una vez más, con el fin de llevar las capacidades de AFW a la vida en la empresa, y el vendedor EMM como MobileIron se necesita, y estamos colaborando muy de cerca con Google en su iniciativa AFW (Android for Work). También apoyamos iniciativas específicas Samsung Knox para mejorar la seguridad de los dispositivos de Samsung en la empresa.

Con la llegada de Windows 10, el marco de gestión móvil será compartido a través de Windows (dispositivos - por ejemplo, un portátil) y Windows Phone (dispositivos móviles). En otras palabras, las empresas tienen una nueva manera de asegurar y administrar dispositivos de Windows. El nuevo sistema operativo tendrá una experiencia personalizada como usuario entre diferentes tamaños de pantalla - que es decir que si usted está en un dispositivo más pequeño, verá otro tipo de interfaz de usuario. El código se ejecutará en todas las categorías de dispositivos con un declarado de "Una familia de productos. Una plataforma. Una tienda". El objetivo es ofrecer valor empresarial, administración de dispositivos, la posibilidad de personalizar la tienda para el dispositivo que se encuentra, y una manera de proteger los datos. O, para decirlo con mayor precisión, habrá la capacidad de la empresa para gestionar sus dispositivos, y "personalizar" su tienda de aplicaciones, y así sucesivamente. MobileIron está trabajando estrechamente con Microsoft para apoyar estos desarrollos.

AYUDAR A LOS USUARIOS FINALES A SER PRODUCTIVOS

Figura 4.7: Ayuda a Usuarios finales a ser Productivos.

Con todas las capacidades que acabamos de discutir, de la organización de la Tecnología de la Información de la empresa, vamos a echar un vistazo al impacto en el usuario de una productividad y una perspectiva general de la experiencia.

Así que vamos a ver como un nuevo empleado puede ser configurado para ser productivo en su primer día en una empresa.

En primer lugar, este nuevo empleado va a querer asegurarse de que puede acceder a su correo electrónico y obtener todos los ajustes Wi-Fi en este dispositivo que podría traer en sí mismo en la empresa.

Después de eso, él querrá empezar a ser productivo, y además de conseguir su correo electrónico corporativo que fluye a su dispositivo, querrá tener acceso a aplicaciones clave que necesita para hacer su trabajo. Y también el contenido corporativo como documentos de fijación de precios o presentaciones de ventas.

Y, por último, si abandona la empresa, prevención de pérdida de datos se puede hacer con ella, limpiando selectivamente los datos de trabajo fuera del dispositivo como sea necesario.

El usuario es productivo y también tiene la tranquilidad de que su información personal se mantiene separada de su información profesional.

SERVICIOS DE USUARIO MOBILEIRON

Figura 4.8: Servicios de Usuario Mobileiron.

Los elementos de la izquierda (menos el elemento Borrado selectivo) son las principales cosas que los usuarios desean.

- Elección de plataformas de dispositivos.
- Quieren que sus datos privados se mantengan separados de los datos corporativos.
- Quieren continuar con una experiencia familiar, nativo de usuario que ya saben.
- Y quieren que sus dispositivos se configuren automáticamente sin que el usuario, realice una intervención manual

Lo de la derecha por lo general necesitan tener acceso a: aplicaciones empresariales, aplicaciones web, el contenido que reside en las instalaciones y repositorios nube personales de negocios y el acceso seguro al correo electrónico, todo ello con el objetivo de mejorar la productividad y la eficiencia.

Por último, la empresa de Tecnologías de la Información debe ser capaz de borrar de forma selectiva información corporativa apagar el dispositivo, en el caso de que un usuario deba abandonar la empresa.

ARQUITECTURA DE LA PLATAFORMA MOBILERION

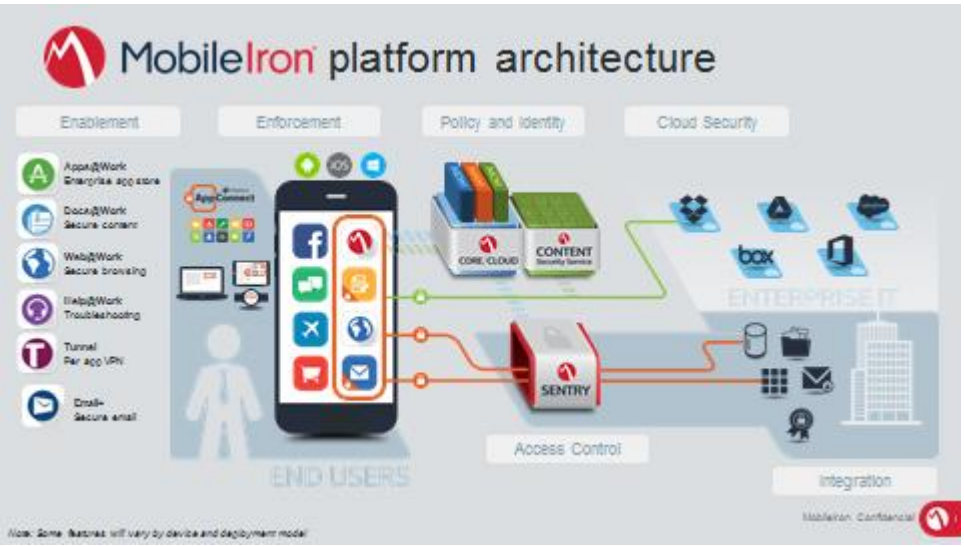


Figura 4.9: Arquitectura de la Plataforma Mobileiron.

De acuerdo a la figura anterior se muestran todas las características de la Arquitectura que ofrece la empresa MOBILEIRON, mismas que son:

- Habilitación
- Aplicación
- Políticas e Identidad
- Seguridad en la Nube
- Control de Acceso, e
- Integración.

LIDERAZGO DE MOBILEIRON EN EL MERCADO

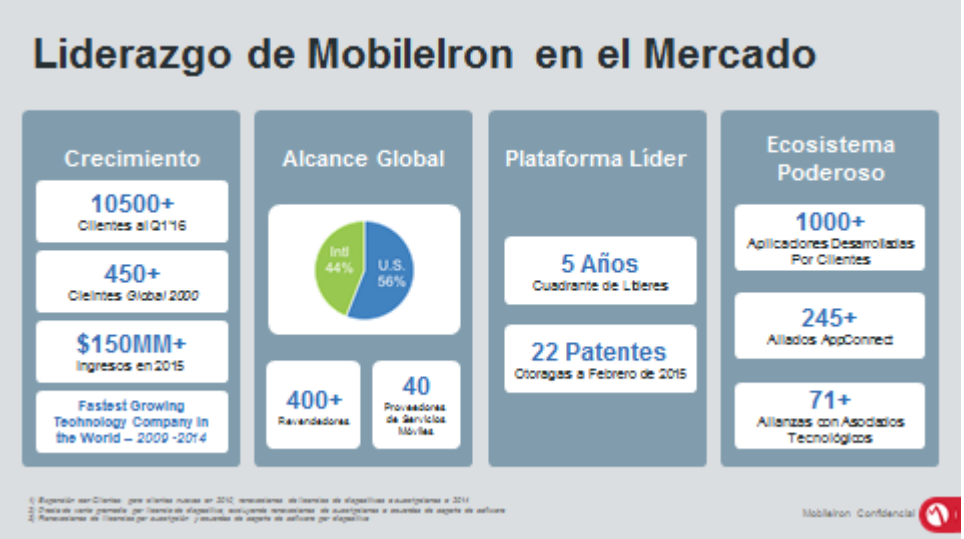


Figura 4.10: Liderazgo en el Mercado.

Como se puede ver en el grafico anterior la empresa Mobileiron ha evidenciado un gran crecimiento, un alcance global considerable, se encuentra considerada como una plataforma líder en el mercado, así como está conformada por un ecosistema poderoso.

4.1.2. EQUIPOS O DISPOSITIVOS MÓVILES QUE LA PLATAFORMA ACEPTA EN SU SISTEMA.

De acuerdo a la documentación adjunta a la oferta presentada el sistema de Administración de Dispositivos Móviles de Mobileiron, esta plataforma acepta los sistemas operativos: Android desde la versión 2.3 y superiores, La plataforma de servicios Mobileiron, IOS 5 y superiores, Windows Phone 8.1 y Windows Phone 8.1 PC, mismo que se muestra en la siguiente figura.

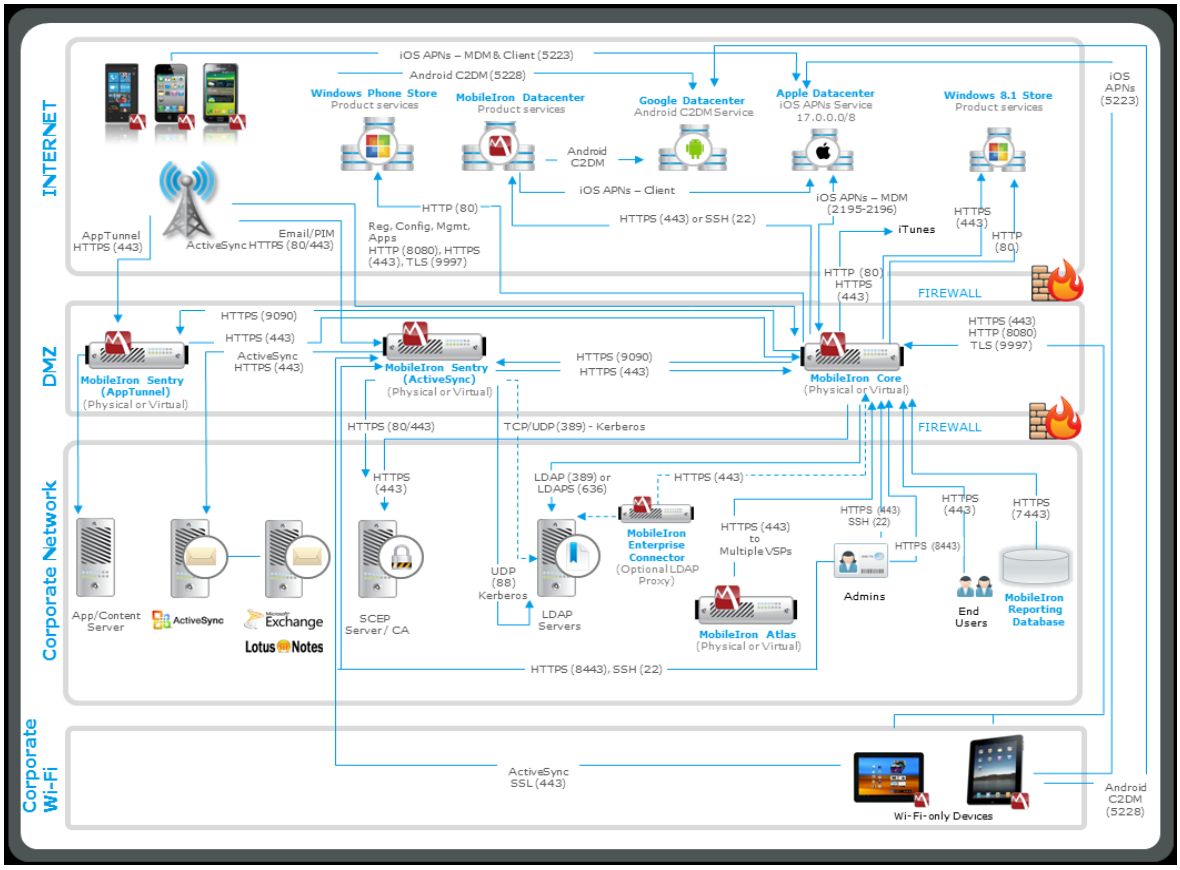


Figura 4.11: Descripción grafica de sistemas Operativos y descripción de la plataforma.

En relación a los dispositivos que la plataforma acepta, estarían inmersos todos los equipos Smartphone, tabletas y laptops que dispongan de los sistemas operativos mencionados anteriormente.

4.2. DESCRIPCIÓN DEL SOFTWARE Y/O APLICACIONES QUE CADA ÁREA TENDRÍA ACCESO.

De acuerdo al software que la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL dispone, estos se detallan en el Anexo 4, con la descripción de cada uno de ellos.

4.2.1. CREACIÓN DE PERFILES DE CADA ÁREA.

Para la creación de un determinado perfil, se debe considerar primeramente las actividades que realiza cada funcionario y en qué área se encuentra desempeñando las

mismas, de aquí partimos con la lista de aplicaciones que este va a necesitar para el buen desempeño de sus tareas.

Una vez que tenemos la lista de aplicaciones procedemos a crear grupos de funcionarios con un determinado perfil, por ejemplo la Coordinación General Administrativa Financiera tendrá acceso a las siguientes aplicaciones: Activos Fijos, E – SIGEF, QUIPUX, Planillaje, Rol de pagos, OnBase, CORREO ELECTRÓNICO.

De esta forma la ARCOTEL podrá tener mayor control sobre la asignación de funciones y privilegios a varios funcionarios al mismo tiempo, pues cuando realice un mantenimiento sobre un perfil, es decir, adicione cuentas, modifique topes u otras operaciones, éstas se ejecutarán sobre todos los usuarios que tienen asignado el perfil.

A continuación se detalla los pasos básicos para la creación de un perfil:

- Debe existir un campo Nombre de perfil en el cual se digitará el nombre que desee que lleve el perfil que se va a crear.
- Debe existir campos de fecha de inicio y final aquí se definirá un rango de fechas dentro del cual aplican los privilegios definidos aquí.
- Posterior a esto debe existir diferentes opciones del perfil de usuario que desee crear y aquí se procede a habilitar los privilegios que se le desee dar al mismo, ya sea de un usuario común o con ciertos privilegios.
- No se debe olvidar el ingreso de los datos personales de cada funcionario.

4.2.2. LISTA DE SOFTWARE Y/O APLICACIONES QUE TENDRÍA ACCESO CADA ÁREA.

De acuerdo a los requerimientos de cada área de trabajo de la ARCOTEL, cada funcionario de estas deberá tener acceso al menos a las aplicaciones que se detallan en la tabla indicada en el Anexo 4.

4.3. IMPLEMENTACIÓN DE LA PLATAFORMA ESCOGIDA MEDIANTE EL USO DE UNA SOLUCIÓN DEMO.

En esta sección se procedió a realizar una prueba de concepto mediante el uso de un ambiente creado por MOBILEIRON exclusivamente para la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, para lo cual se nos proporcionó una usuario y una clave para su instalación, a continuación se presentan las capturas de pantalla de cada paso seguido, para la instalación y operación del sistema MDM elegido para la Agencia de Regulación y Control de las Telecomunicaciones.

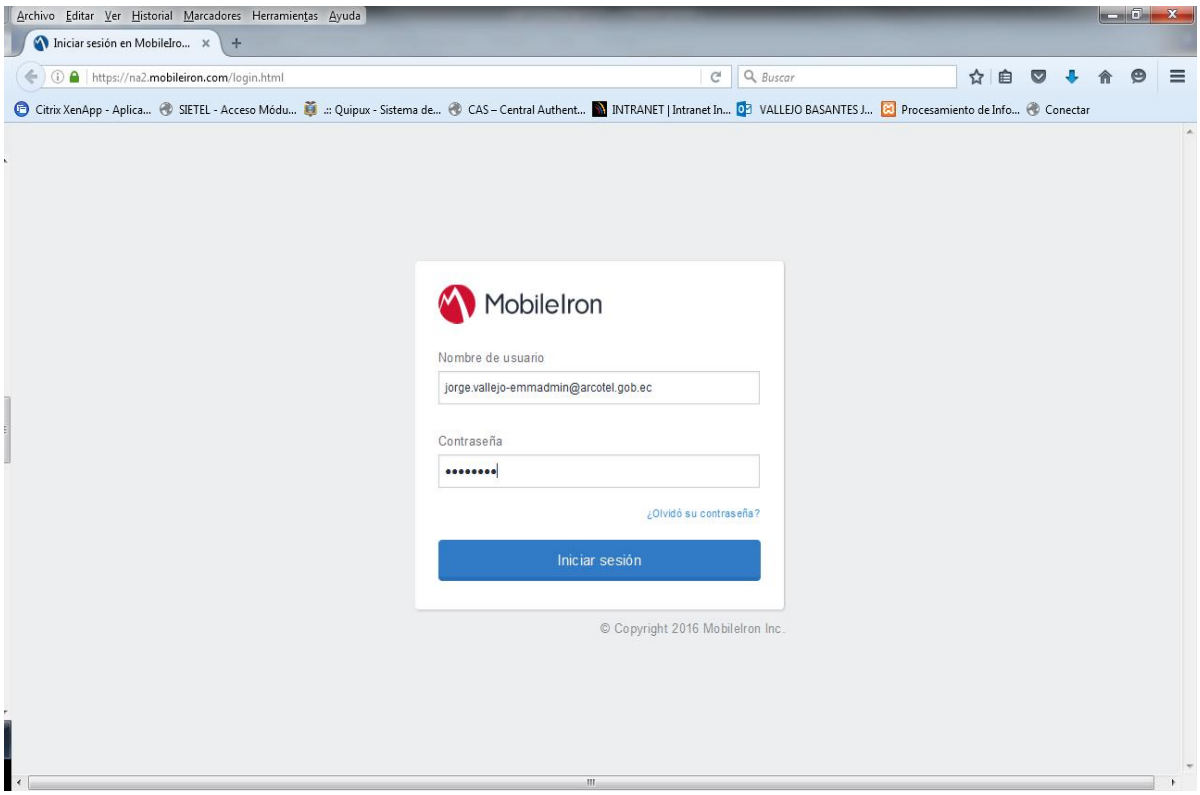


Figura 4.12: Ingreso a la plataforma creada por Mobileiron exclusivamente para ARCOTEL.

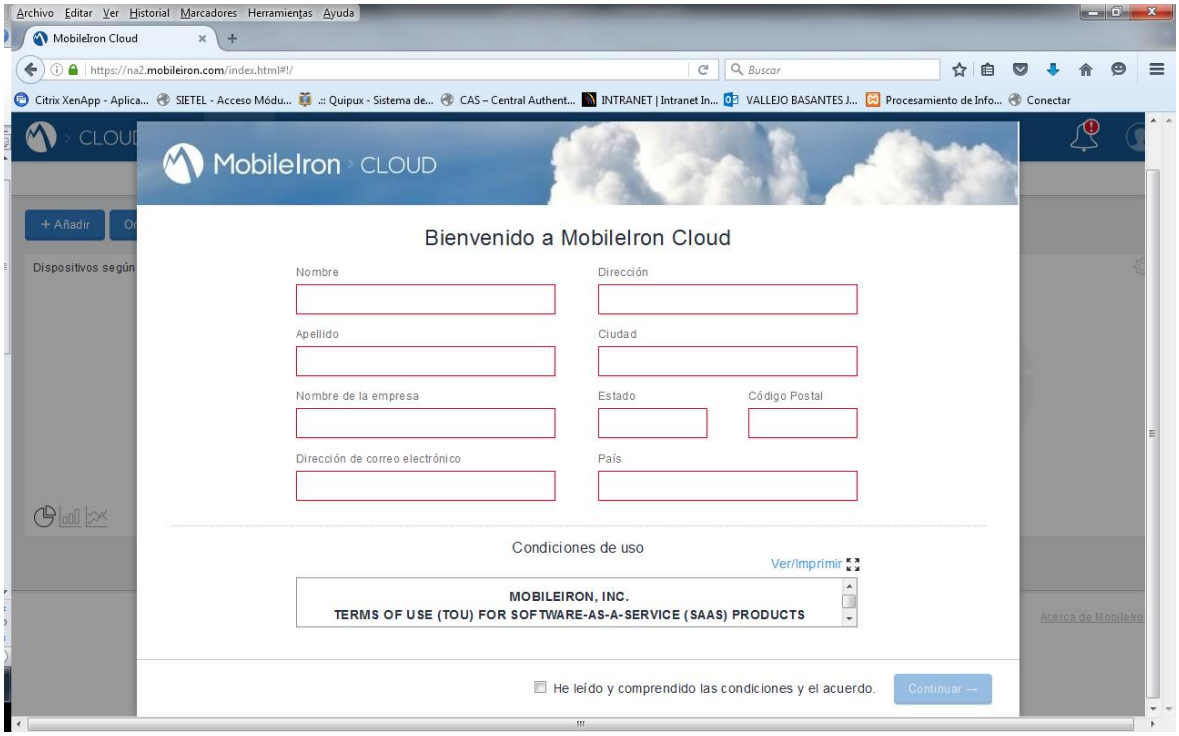


Figura 4.13: Registro y aceptación de términos y condiciones.

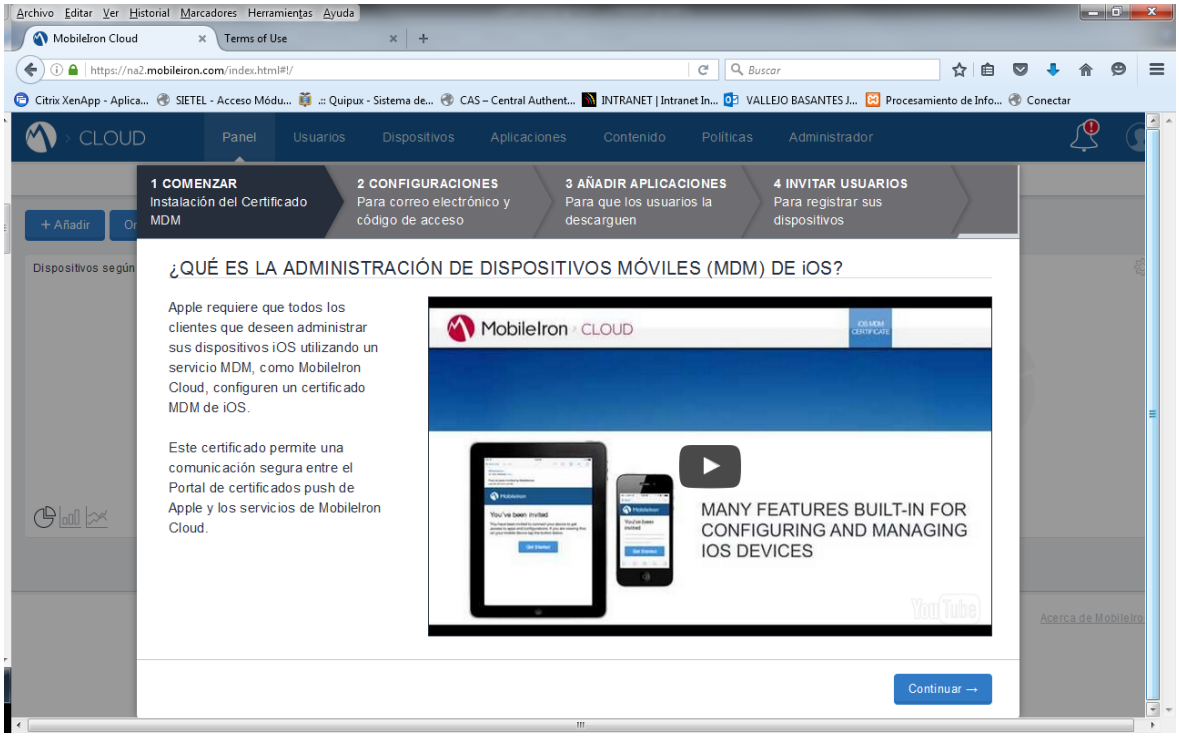


Figura 4.14: Instalación de Certificados para la operación.

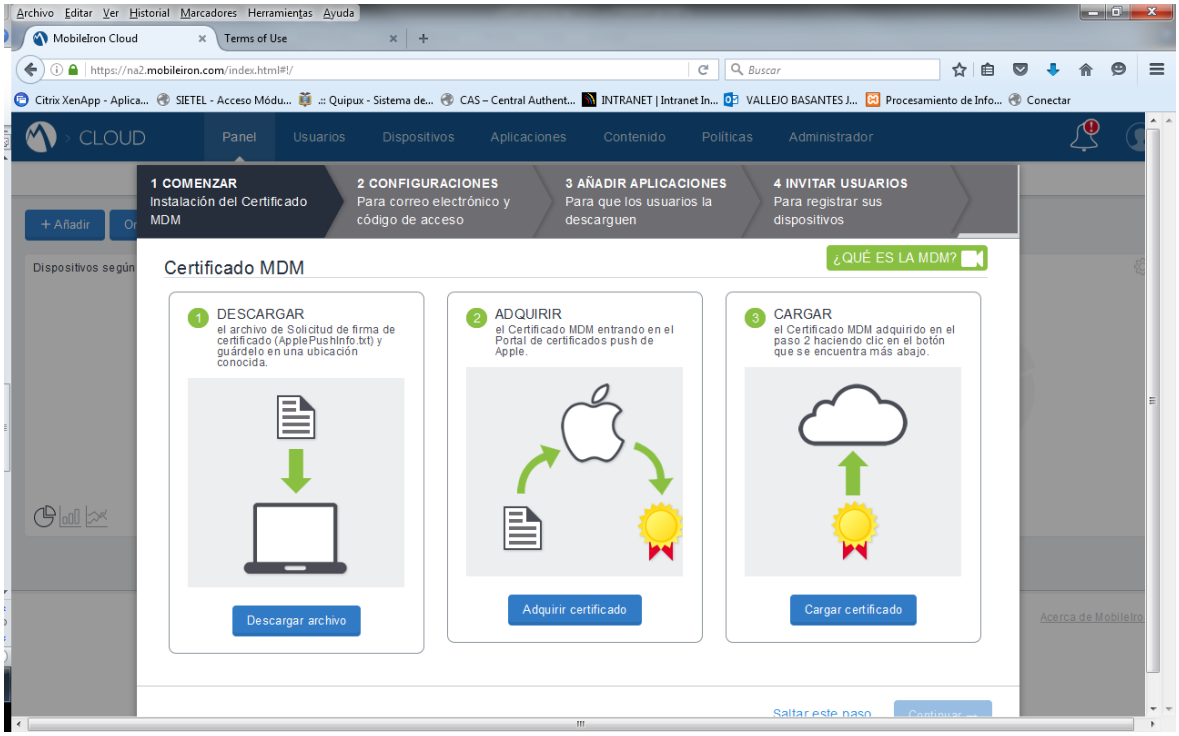


Figura 4.15: Cargar Certificados para la operación.

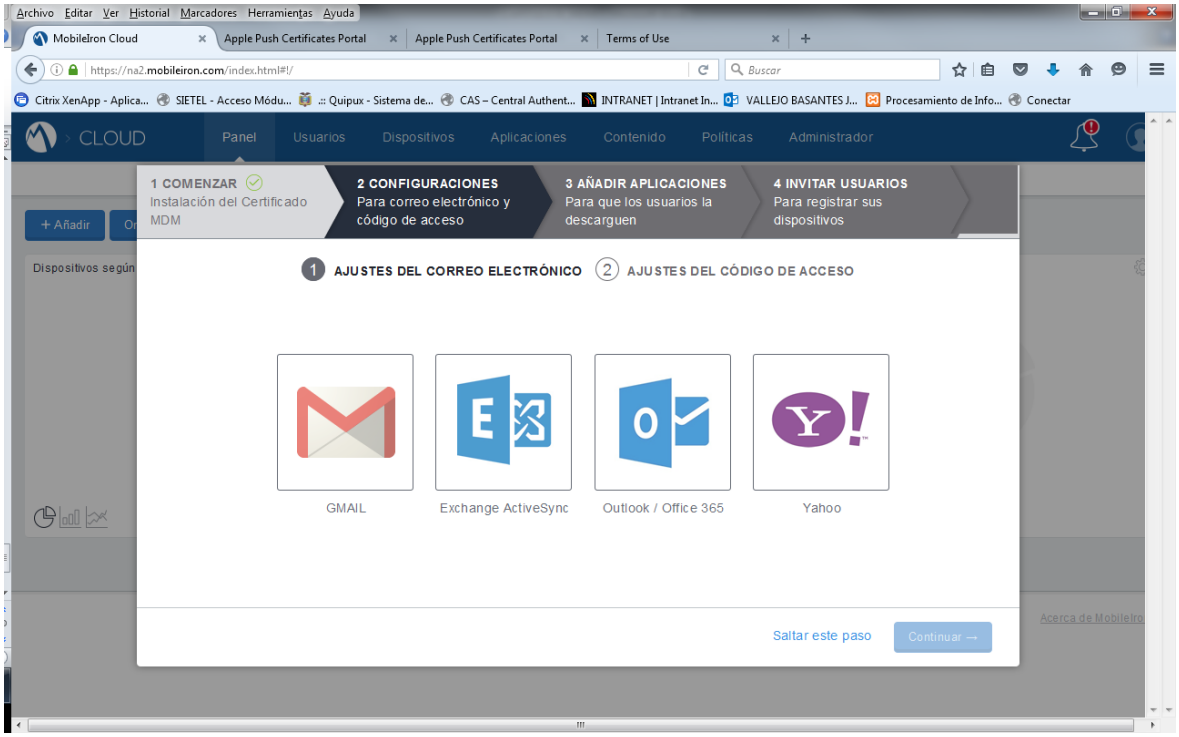


Figura 4.16: Creación y configuración de correo electrónico.

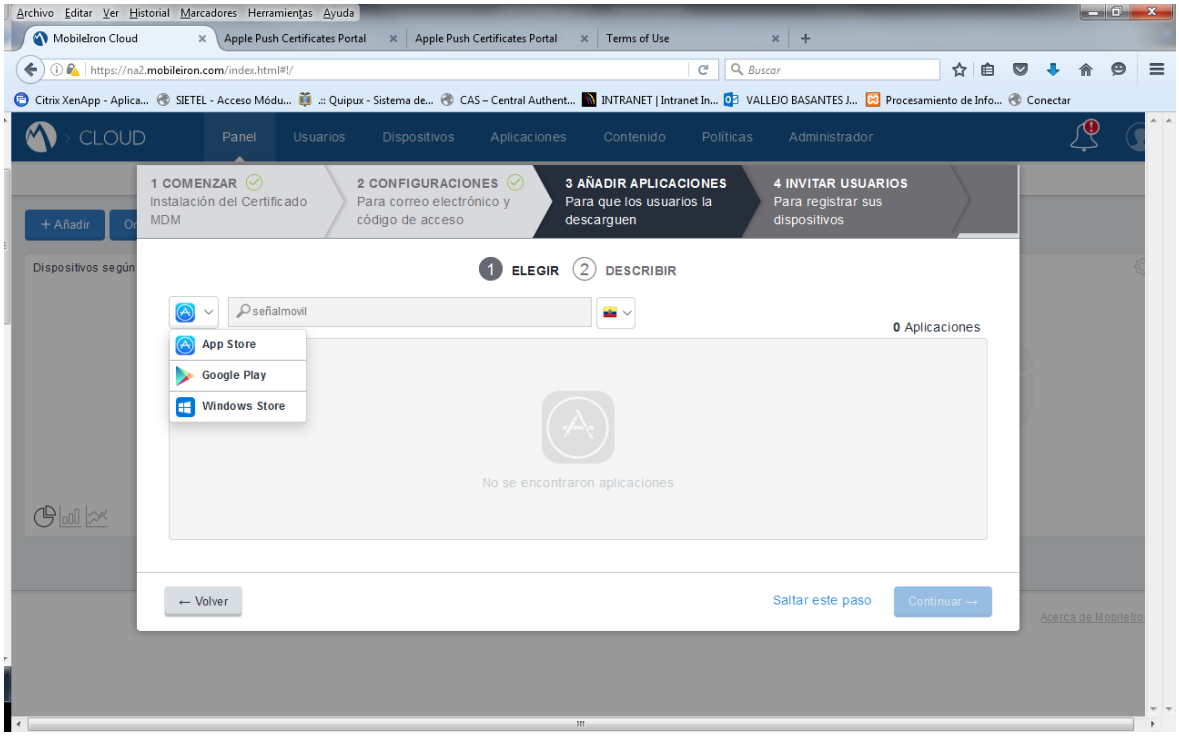


Figura 4.17: Campo para añadir aplicaciones para todos los usuarios

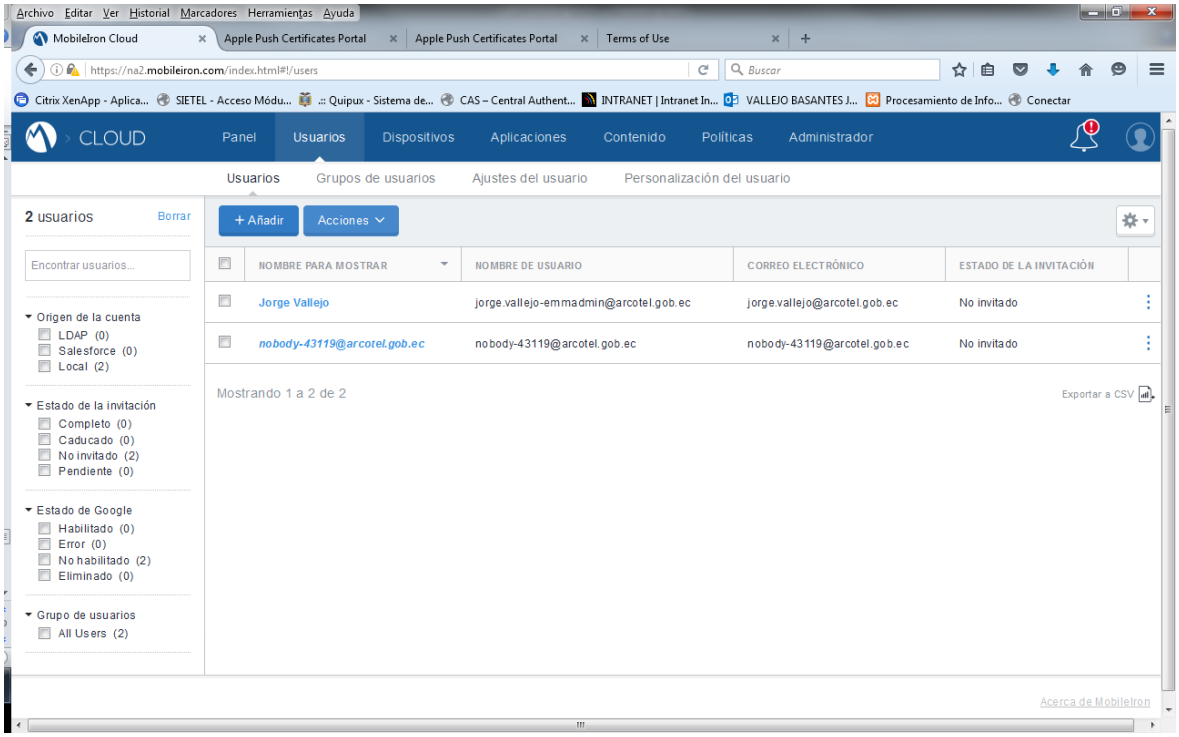


Figura 4.18: Campos de administración aquí se puede añadir, quitar usuarios y dispositivos.

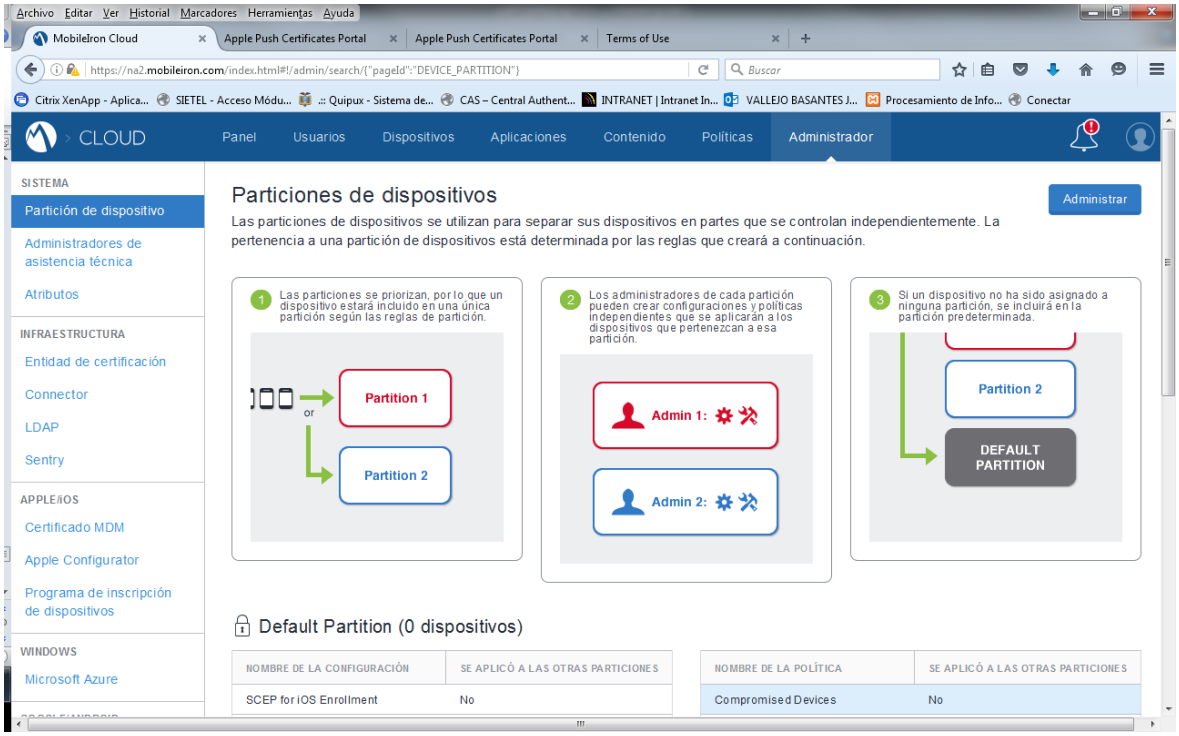


Figura 4.19: Campos de administración aquí se puede añadir, quitar usuarios dar privilegios.

CAPITULO V

5. ANÁLISIS DE GESTIÓN DE RENDIMIENTO DE LA RED UTILIZADA EN LA ADMINISTRACIÓN DE LOS DISPOSITIVOS MÓVILES

En este capítulo se realizara un análisis de la situación actual de la red LAN y la gestión de rendimiento de la misma, que dispone la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL. Todo esto con la finalidad de preparar la red para la futura implementación, y de igual manera determinar la eficiencia de la red. El rendimiento de la misma se evalúa con indicadores como el throughput (tasa promedio en la entrega de un mensaje sobre un canal de comunicación), porcentaje de utilización, tasa de erros y tiempo de respuesta.

El estado de cualquier red puede ser monitorizado, analizando los datos de rendimiento de la misma, es así que las tendencias relacionadas con la capacidad o cuestiones de fiabilidad llegan a convertirse en servicios afectados.

El lanzamiento de alarmas es establecido en relación a los límites o umbrales de rendimiento, estas alarmas deben ser manejadas por procesos de Gestión de Fallos, las mismas que pueden variar de acuerdo a la gravedad.

5.1. UBICACIÓN DE LAS OFICINAS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

La matriz de la Agencia se encuentra en la ciudad de Quito en la Av. Diego de Almagro entre Whymper y Alpallana, adicionalmente tiene oficinas administrativas en el edificio de la Av. 9 de Octubre y Berlín, también cuenta con 6 (seis) Administraciones Regionales y 2 (dos) oficinas técnicas ubicadas en: Administraciones regionales en Quito, Guayaquil, Cuenca, Riobamba, Portoviejo y Galápagos; oficinas técnicas en Loja y Lago Agrio.

El objetivo que persigue la Agencia es “Velar por el respeto a los derechos de los usuarios en materia de servicios de telecomunicaciones.”

5.1.1. ESTRUCTURA ORGANIZACIONAL

En la siguiente figura se muestra la estructura que maneja la Agencia de Regulación y control de las Telecomunicaciones.

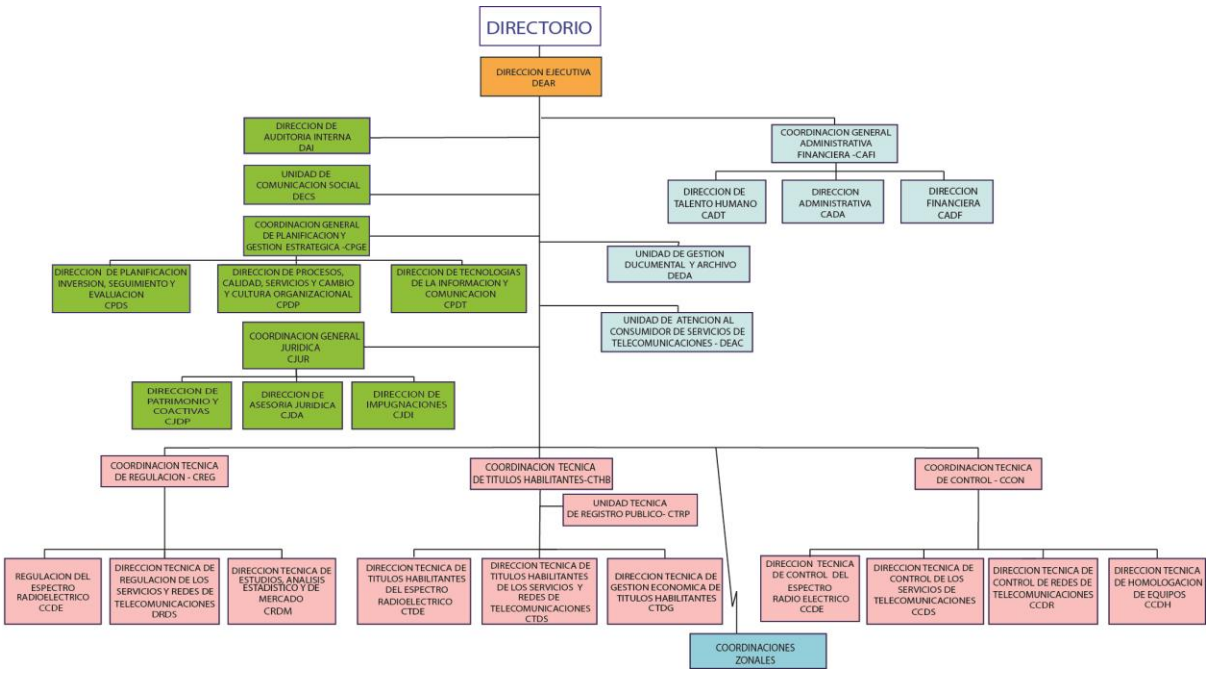


Figura 5.1: Estructura Organizacional de ARCOTEL

El departamento de tecnología de las Telecomunicaciones es el responsable del funcionamiento y operatividad de toda la red, por ende de la gestión y administración de todos los dispositivos, en este punto vamos a proceder a realizar el análisis del tráfico que cursa por la red mediante la utilización de software libre.

5.1.2. DATOS DE LA RED QUE DISPONE ACTUALMENTE LA ARCOTEL

La información detallada a continuación es el resultado de instalar un software de gestión de red y de la visita a cada edificio que dispone la Agencia en la ciudad de Quito, y las Administraciones Regionales interconectadas de Quito mediante enlaces dedicados.

Se efectuó el levantamiento de esta información, con la finalidad de conocer la situación en la que se encuentra la institución; esta información es de gran importancia

debido a que en base a esta se determinara requerimientos que existan entorno a la gestión de recursos de Red; el cual se complementara con un sondeo de tráfico de red.

Red LAN: Agencia de Regulación y Control de las Telecomunicaciones

de puntos de Acceso: 1200 aproximadamente

Back Bone: Fibra Monomodo 1 Gbps

Capacidad de Salida de Internet: 66 Mbps

Disponibilidad contratada con el ISP: 99.999%

5.1.3. DIAGRAMA DE CONEXIÓN LAN DE ARCOTEL

A continuación se adjunta un bosquejo del diagrama de conexión a internet que mantiene la Arcotel.

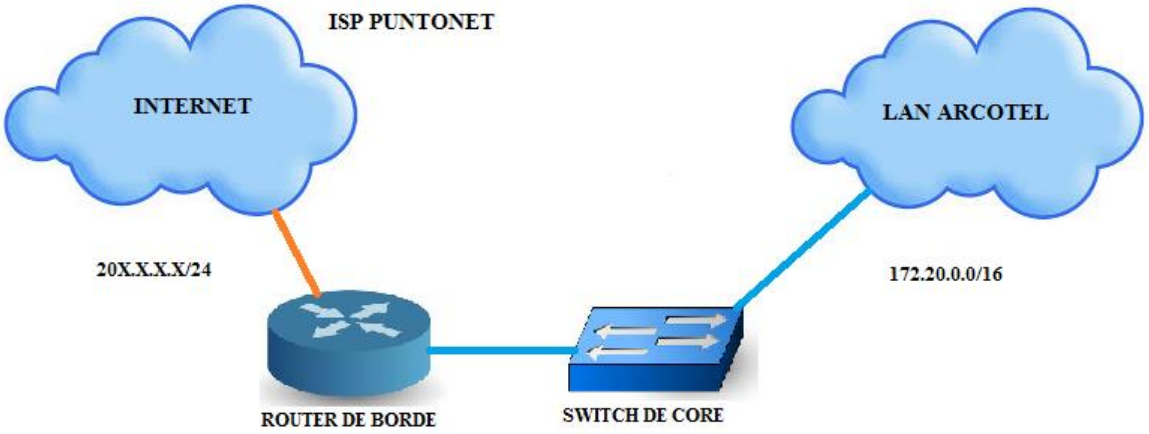


Figura 5.2. Diagrama de conexión a Internet de la ARCOTEL.

5.2. PARÁMETROS DE LA GESTIÓN

En primer lugar se debe elegir los dispositivos de los cuales se obtendrá la información necesaria para determinar el funcionamiento de la red.

También es necesario considerar un tiempo prudencial para obtener dicha información.

Es necesario balancear toda la información obtenida con la finalidad de emitir los resultados.

De aquí se parte que la Gestión del Rendimiento está basada en la evaluación de varias métricas que van a permitir analizar el comportamiento de la red.

Partiremos analizando algunas métricas que se puede obtener para la Gestión:

5.2.1. RENDIMIENTO DE LA RED

- **Utilización del Canal.** De aquí podemos determinar cuál es la capacidad realmente utilizada de la capacidad nominal. La misma que permite hacer una planificación a futuro sobre tasa de crecimiento de utilización, panificación para compra de capacidad, en que actualizaciones debo invertir, adicionalmente, ayuda a controlar y solucionar problemas de cuellos de botella, etc.
- **Retardo en la red o Jitter.** Es el tiempo transcurrido en el que un paquete llega a su destino, este puede ser producido por una aplicación, por un sistema operativo, por una tarjeta de red, etc. El mismo puede ser validado mediante el uso del comando ping.
- **Capacidad Nominal.** Esta corresponde a la máxima cantidad de bits transmitidos por cada unidad de tiempo (segundos); depende directamente de anchos de banda del medio de transmisión, Codificación del Canal y Compresión, Eficiencia de algoritmos de acceso, Capacidades de procesamiento de equipos transmisores.
- **Capacidad Efectiva del Canal.** Esta es una fracción de la Nominal y depende de Limitaciones en los dispositivos extremos, De la Carga Adicional (Overhead) de los protocolos en cada capa, Eficiencia de los algoritmos de control de flujo (TCP).
- **Errores y pérdida de paquetes.** Estos ocurren debido al hecho de generación de colas (búfers) mismas que no son infinitas, debido a que cuando un paquete

llega a una cola y esta a su vez se encuentra llena este es descartado, la perdida de paquetes también se presenta cuando un paquete tiene errores y requiere ser corregido. Adicionalmente la corrección de perdidas ejecutada mediante retransmisión puede causar aún más congestión si no se ejerce ningún tipo de control.

5.2.2. RENDIMIENTO DEL SISTEMA

- Memoria
- Procesamiento (Utilización de CPU)
- Carga (Load)
- Disponibilidad

5.2.3. RENDIMIENTO DE SERVICIOS

En relación al tráfico cursado se pueden obtener las siguientes:

- Velocidad (Bit por Segundo)
- Paquetes por segundo
- Errores
- Paquetes Descartados
- Paquetes Unicast vs No-Unicast
- Flujos por Segundo
- Tiempo de Ida y Vuelta (RTT)
- Dispersión de Retardo (Jitter)

5.3. GESTIÓN DE RENDIMIENTO EN LA RED DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

Se procederá a realizar un análisis de la red en la ciudad de Quito. La Agencia de Regulación y Control de las Telecomunicaciones se enlaza con su proveedor ISP a través de

Fibra Óptica Monomodo, con una capacidad nominal de 1 Gbps. Siendo la Capacidad efectiva del Ancho de Banda del enlace contratado con el ISP de 66 Mbps.

5.3.1. UTILIZACIÓN DEL ENLACE

Para determinar este parámetro se utilizó el software de gestión Paessler Router Traffic Grapher (PRTG), de donde se procedió a monitorear cada enlace desde el equipo móvil hacia la salida al internet, es decir todo el trayecto de la red propia de la Agencia de Regulación y Control de las Telecomunicaciones.

Trafico Entrante/Saliente Router de Borde Cisco 3845:

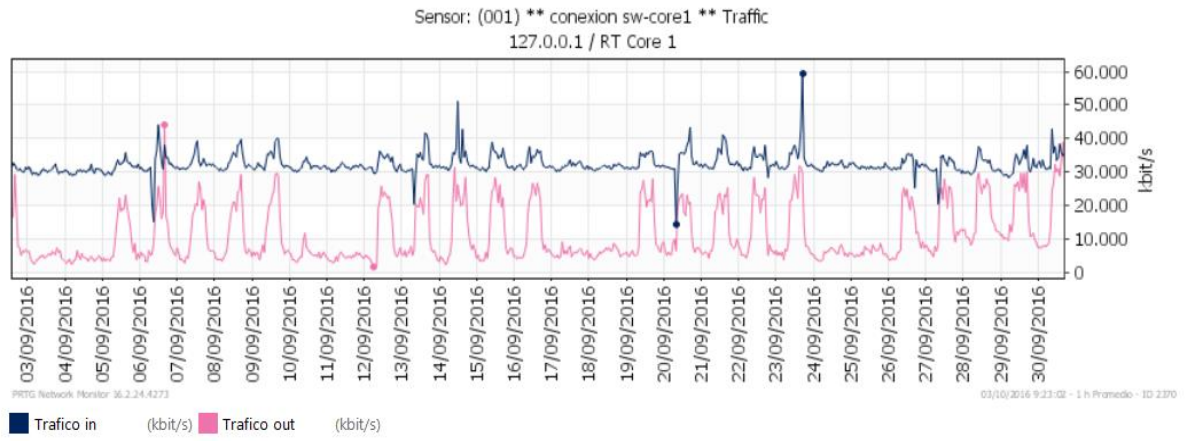


Figura 5.3. Detalle del tráfico entrante y saliente de Router de Borde del mes de Septiembre de 2016.

Este Router, es el dispositivo que permite conectar a la Agencia de Regulación y Control de las Telecomunicaciones con su proveedor de servicios de Internet (ISP). En la figura anterior se muestran datos del tráfico Entrante/Saliente correspondiente al mes de Septiembre 2016, mismo que fue considerado como muestra y se logró recabar los siguientes datos estadísticos:

Trafico Saliente

Máximo: 43.98 Mbps

Mínimo: 1.71 Mbps

Promedio: 11.07 Mbps

Trafico Entrante

Máximo: 59.20 Mbps

Mínimo: 14.53 Mbps

Promedio: 32.36 Mbps

De los datos podemos concluir que el uso del canal promedio es de 32.36 Mbps lo que corresponde a una tasa del 49.03% con respecto a la capacidad efectiva.

También podemos obtener que el máximo uso del canal es del 89.69% con respecto a la capacidad efectiva.

Adicionalmente es necesario mencionar que la salida de internet de la Agencia de Regulación y Control de las Telecomunicaciones está sujeta a restricciones en relación a contenidos no apropiados, mismos que han sido bloqueados, de esta manera se garantiza en cierto porcentaje que el ancho de banda sea utilizado en otros fines, optimizando su consumo.

Teniendo un 49.03% de uso del canal se determina que no existen cuellos de botella en la red LAN de Arcotel, así como en salida al Internet, pudiendo incrementar usuarios móviles a nivel institucional.

Trafico Entrante/Saliente Switch de Core WS-4510R-E:

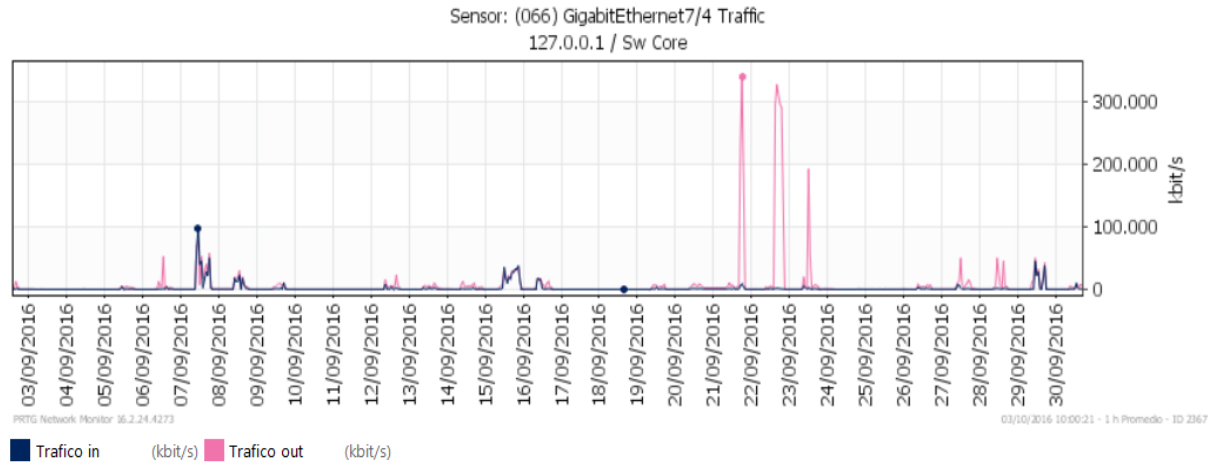


Figura 5.4. Detalle del tráfico entrante y saliente de Switch de Borde del mes de Septiembre de 2016.

Este Switch, es el dispositivo que permite conectar la Red LAN de la Agencia de Regulación y Control de las Telecomunicaciones con el Router de Borde. En la figura anterior se muestran datos del tráfico Entrante/Saliente correspondiente al mes de Septiembre 2016, mismo que fue considerado como muestra y se logró recabar los siguientes datos estadísticos:

Trafico Saliente

Máximo: 341.91 Mbps

Mínimo: 0.149 Mbps

Promedio: 7.304 Mbps

Trafico Entrante

Máximo: 98.3 Mbps

Mínimo: 0.041 Mbps

Promedio: 1.806 Mbps

De los datos podemos concluir que el uso del canal promedio es de 1.806 Mbps lo que corresponde a una tasa del 0.181% con respecto a la capacidad efectiva.

También podemos obtener que el máximo uso del canal es del 9.83% con respecto a la capacidad efectiva.

Teniendo un 0.18% de uso del canal se determina que no existen cuellos de botella en la red LAN de Arcotel, pudiendo incrementar usuarios móviles a nivel institucional.

Trafico Entrante/Saliente Switch de Piso WS-C3560G-48PS:

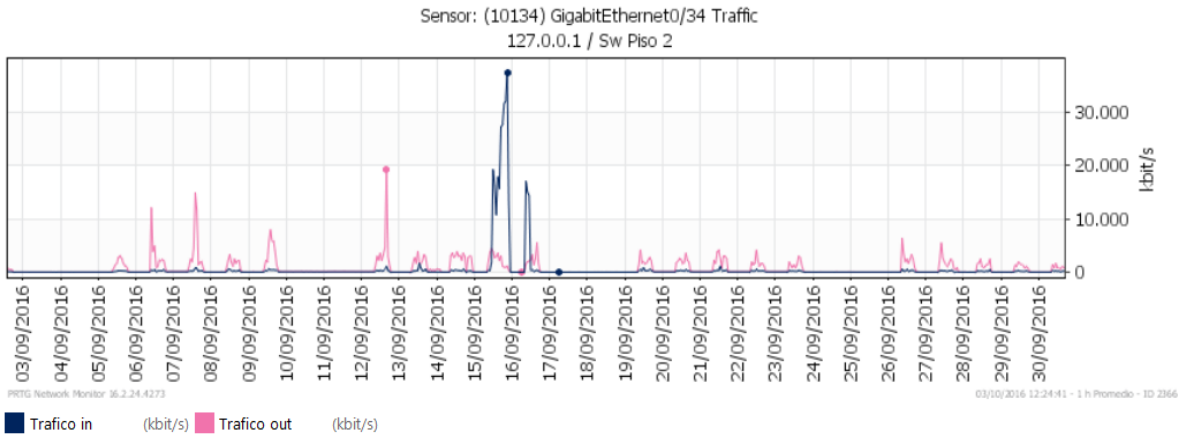


Figura 5.5. Detalle del tráfico entrante y saliente de Switch de Piso del mes de Septiembre de 2016.

Este Switch, es el dispositivo que permite conectar cada piso de la Agencia de Regulación y Control de las Telecomunicaciones se conecta con el switch de borde Y A SU VEZ CON CADA Acces Point, en la figura anterior se muestran datos del tráfico Entrante/Saliente correspondiente al mes de Septiembre 2016, mismo que fue considerado como muestra y se logró recabar los siguientes datos estadísticos:

Trafico Saliente

Máximo: 19.54 Mbps

Mínimo: 0.007 Mbps

Promedio: 0.76 Mbps

Trafico Entrante

Máximo: 37.37 Mbps

Mínimo: 0.005 Mbps

Promedio: 0.53 Mbps

De los datos obtenidos podemos concluir que el uso del canal promedio es de 0.53 Mbps lo que corresponde a una tasa del 0.053% con respecto a la capacidad efectiva.

También podemos obtener que el máximo uso del canal es del 3.74% con respecto a la capacidad efectiva.

Teniendo un 0.053% de uso del canal se determina que no existen cuellos de botella en la red LAN de Arcotel, así como en salida al Internet, pudiendo incrementar usuarios móviles a nivel institucional.

5.3.2. PERCENTIL 95

Para validar este tema se tiene los datos del mes de Septiembre del 2016, lo que resulta 676 muestras, para obtener los resultados de percentil 95, eliminaremos el 5% de los valores más altos de las 676 muestras, es decir eliminaremos los 33 valores más altos.

Trafico Entrante/Saliente Router Cisco 7604:

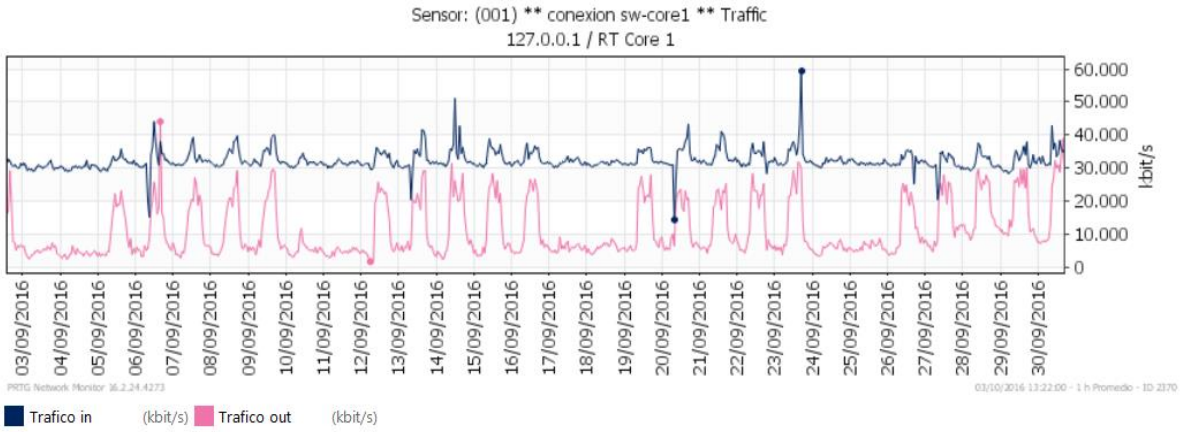


Figura 5.6. Detalle del tráfico entrante y saliente de Router de Borde del mes de Septiembre de 2016.

De los resultados que muestra la gráfica anterior el 95% del tiempo, el uso del canal es igual o menor a 37.42 Mbps.

5.3.3. RETARDO EXTREMO A EXTREMO

Con la finalidad de obtener estos resultados se utilizó herramientas de internet como medidores de velocidad confiables los mismos que permiten obtener las condiciones de retardo del enlace con respecto a sus servidores ubicados en diferentes partes del mundo.

5.3.3.1. *TIEMPO DE RESPUESTA AL INTERNET Y VELOCIDAD DE CARGA Y DESCARGA:*

El siguiente grafico muestra la velocidad de descarga y carga hacia un servidor en Guayaquil desde la ARCOTEL Quito, siendo la velocidad de descarga de 32.02Mbps, con un resultado de ping de 11 mseg tiempo que tarda en ir y regresar un paquete (round-trip-time, o RTT), esto resulta ser óptimo dentro del país.

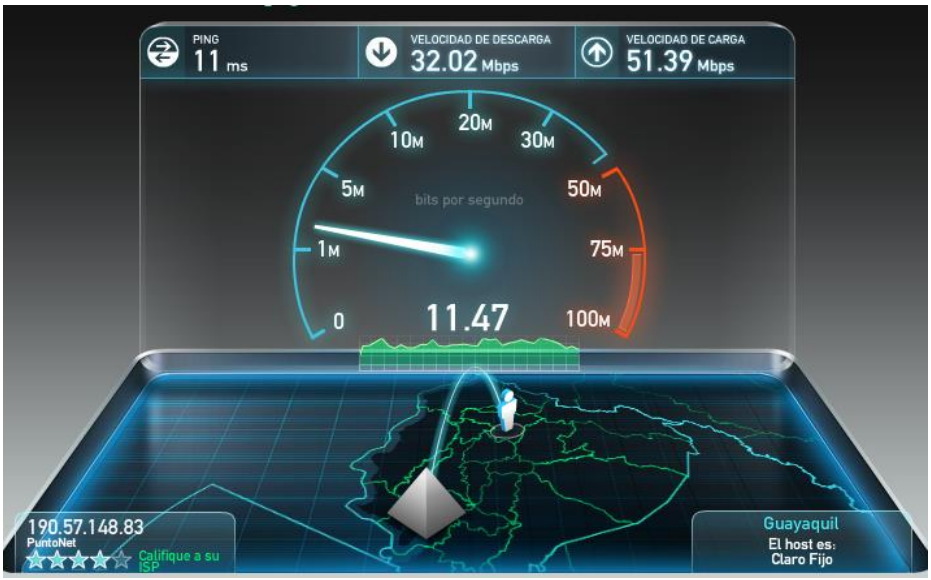


Figura 5.7. Grafica de Velocidades de Carga y descarga hacia un servidor en Guayaquil

El siguiente grafico muestra la velocidad de descarga y carga hacia un servidor en Miami desde la Arcotel Quito, siendo la velocidad de descarga de 3.86 Mbps, con un resultado de ping de 103 mseg tiempo que tarda en ir y regresar un paquete (round-trip-time, o RTT), resultados que están dentro de los parámetros aceptables.

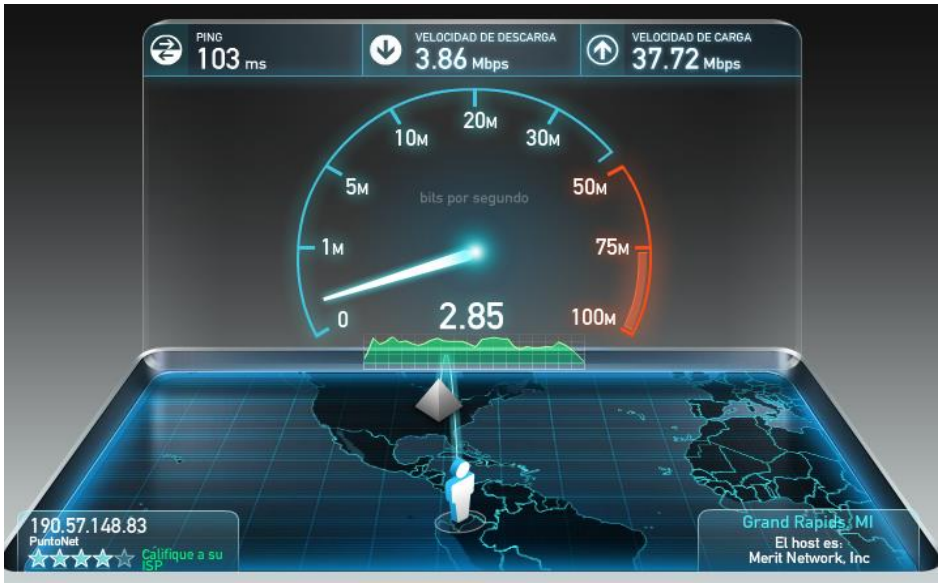


Figura 5.8. Grafica de Velocidades de Carga y descarga hacia un servidor en Miami

5.3.4. PÉRDIDA DE PAQUETES Y ERRORES

Para este análisis se usa datos recopilados en el switch de core:

Errores Transmitidos/Recibidos Switch de core Cisco WS-4510R-E:

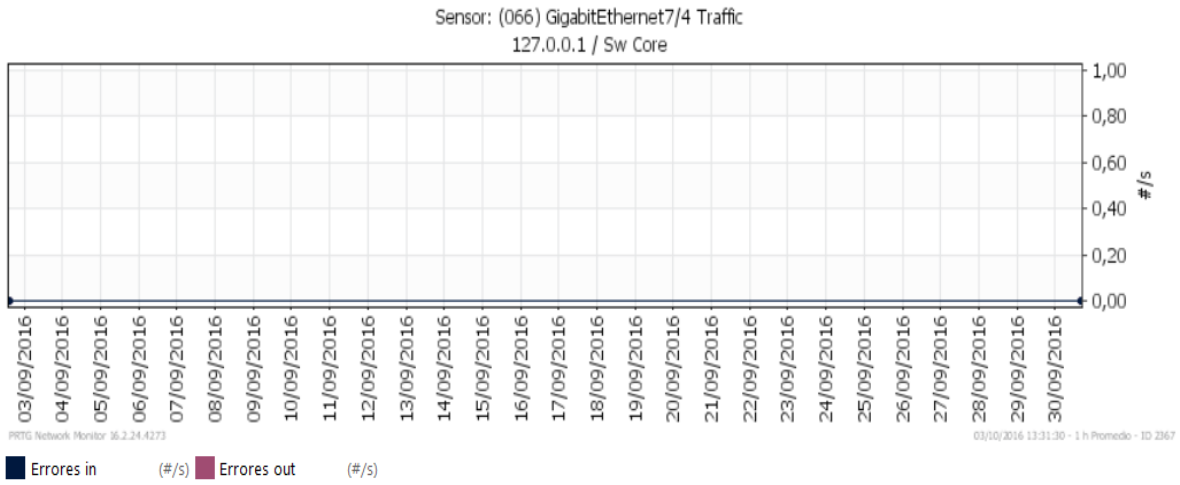


Figura 5.9. Errores In/Out mes de Septiembre 2016

La grafica anterior muestra los errores de transmisión entrante y saliente en el mes de Septiembre del 2016, por día.

De lo indicado en la gráfica anterior cuando no existen errores de transmisión, indica que no se está generando errores dentro de la intranet.

Paquetes Descartados Entrantes/Salientes Switch de core Cisco WS-4510R-E:

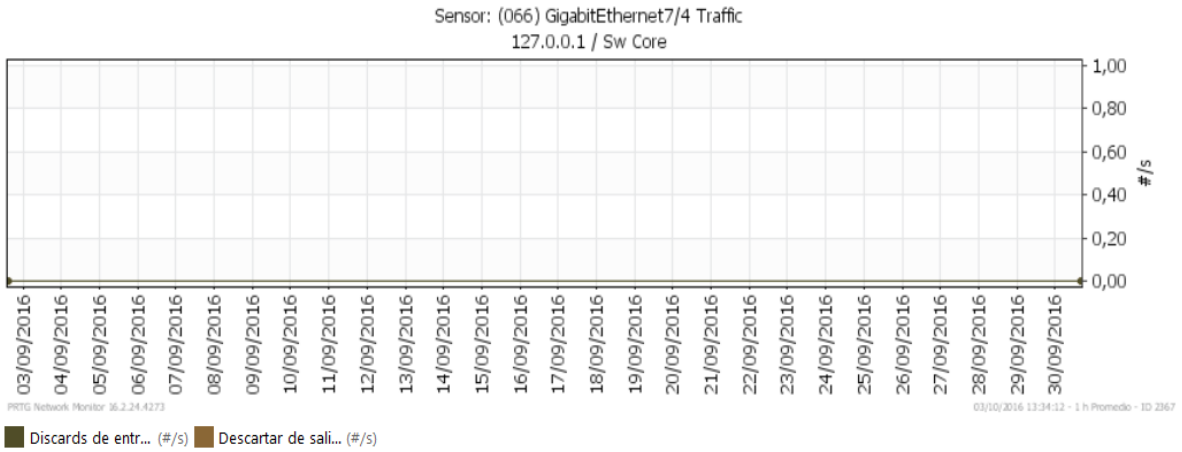


Figura 5.10. Paquetes Descartados In/Out mes de Septiembre 2016

La grafica anterior muestra el número de paquetes descartados entrantes y salientes en el mes de Septiembre del 2016, por día.

Si no existen paquetes descartados en la recepción, esto que indica que los buffers del switch no se congestionan, es decir provocando que se eliminen paquetes en la recepción, mientras que si existe un gran número de paquetes descartados en la transmisión esto indicaría que existe congestión en la Intranet.

CAPÍTULO VI.

6. CONCLUSIONES Y RECOMENDACIONES.

6.1. CONCLUSIONES.

- El modelo de costos muestra claramente que el retorno de la inversión de la solución actual que se propone utilizar en la Agencia de Regulación y Control de las Telecomunicaciones (Microsoft Exchange) es el más alto cuando se compara con el retorno de la inversión de las tres empresas analizadas en el modelo de costos. Este comportamiento es constante en los dos escenarios considerados en el modelo basado en las soluciones.
- La siguiente mejor alternativa en función de su retorno de la inversión es la empresa MOBILERION. La alternativa en las instalaciones o sea en servidores locales, produce un ROI más alto. Los resultados del rendimiento de la inversión de las otras dos empresas no están lejos de los resultados obtenidos con MOBILERION lo que significa que sus costos y beneficios son muy similares.
- Es interesante analizar el retorno de la inversión como resultado de las tres empresas y la situación actual aumenta a medida que pasa el tiempo. Este comportamiento se explica porque los valores de los beneficios se vuelven más altos cada año. El parámetro que hace que el aumento de los beneficios es la seguridad ya que cada año las soluciones MDM tendrán que evitar que un mayor número de ataques y así ser menos vulnerables.
- El análisis de sensibilidad muestra cómo un modelo de costos puede ser alterado por el cambio de un parámetro. En el modelo del costo actual del análisis de sensibilidad incluyó la modificación de una reducción del ROI para las tres empresas analizadas.

- A continuación, el parámetro productividad fue modificado por aumentar el número de horas que los funcionarios y empleados trabajarían desde su casa usando la solución MDM. El resultado fue un incremento en los valores de retorno de la inversión para las tres empresas.
- Mediante el análisis de la gestión de rendimiento se puede evaluar el desempeño de la red, esto es mediante la utilización de métricas, almacenamiento de datos y elaboración de estadísticas para la toma de decisiones, con el claro objetivo de mejorar sus prestaciones y tomar medidas preventivas y/o correctivas que aseguren la disponibilidad de la red en el mayor porcentaje.
- Luego de realizar una gestión sobre la red de la ARCOTEL, se puede determinar que no existe cuellos de botella y/o congestionamiento en cada uno de los enlaces inmersos en las conexiones o saltos que dará cada dispositivo móvil, así como en el enlace de acceso al Internet contratado, es decir se tiene un amplio porcentaje de ancho de banda disponible.
- En el análisis de los retardos de extremo a extremo se puede establecer que los mismos se encuentran dentro de niveles aceptables, con lo cual se asegura una conexión rápida y con niveles de velocidad y descarga apropiados.
- De los datos recogidos durante el mes de septiembre de 2016, no se encuentra errores en la transmisión y/o recepción de paquetes, que indiquen que puedan presentarse problemas a nivel de capa de transporte, tamaños de ventana etc.
- El descarte de paquetes en la transmisión es mínimo, con lo cual se puedo concluir que no existe congestión a nivel de la Intranet, esto se garantiza debido a que la mayor parte de la infraestructura de la Arcotel es mediante conexiones de hasta 1 Gbps, por tal razón se garantiza que el tráfico generado por los dispositivos móviles no causaría impacto en el tráfico de la red.

6.2. RECOMENDACIONES

- Mi recomendación para la Agencia de Regulación y Control de las Telecomunicaciones es que debe seguir usando Microsoft Exchange para proporcionar cierto grado de gestión a sus dispositivos. No es el momento ni el lugar adecuado para adoptar una nueva solución. Debido a que Microsoft Exchange está cubriendo las necesidades actuales de la ARCOTEL mediante el acceso a correo electrónico corporativo y la función de borrado remoto. Sin embargo, estas necesidades van a aumentar pronto y entonces será recomendable para la ARCOTEL elegir una solución MDM. Con base en el modelo del costo, MOBILERION es una gran opción para la transición. Además, se considera que no es adecuado aun la implementación, porque si el cliente hubiera sido parte del mercado de la salud, o del sector financiero en lugar de la ARCOTEL, habría recomendado el cambio inmediato a una solución MDM debido a la característica de sensibilidad de la información que las empresas tienen que manejar.
- En el futuro, cuando la ARCOTEL disponga de asignación de presupuestos para adquisición de bienes o servicios, y, esté lista para adoptar una solución MDM, yo recomendaría que cada funcionario debería llevar su dispositivo de políticas (BYOD). BYOD va a ayuda a que la ARCOTEL tenga mejores resultados de ROI, ya que no tendría que incurrir en los gastos de adquisición de teléfonos inteligentes y tabletas, a los funcionarios que cuestan alrededor de $ 110.600 cada año.

BIBLIOGRAFIA

[1.] "Choosing an MDM platform: Where to start the conversation." Blackberry. Blackberry, p.v. Viernes. 4 Dic. 2015. <http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/blackberry-10/ChoosingAnMDMPlatform.pdf>

[2.] "MDM Architecture." Notify Technology. Notify Technology Corporation, p.v. Viernes. 4 Dic. 2015. <http://www.notifycorp.com/products/notifymdm/architecture/>

[3.] "A real MDM difference" MaaS360. Fiberlink Communications Corp., p.v. Viernes. 4 Dic. 2015. <http://www.maas360.com/why-maas360/a-real-mdm-difference/>

[4.] "Administración de Dispositivos Móviles" de la UNAD Universidad Nacional de Colombia, p.v. Viernes. 4 Dic. 2015. <http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_10_administracin_de_dispositivos_mviles.html>

[5.] "Estudio de perspectivas y estrategia de desarrollo y difusión de aplicaciones móviles en México" p.v. Viernes. 4 Dic. 2015. <http://amiti.org.mx/wp-content/uploads/2013/10/Estudio-Apps_Documental.pdf>

[6.] "Cobertura Digital en Ecuador" p.v. Viernes. 4 Dic 2015. <http://www.coberturadigital.com/2014/05/20/smartphones-en-ecuador-acceso-se-duplico-en-2-anos/>

[7.] "Notify Technology" p.v. Viernes. 4 Dic 2015. <http://www.notifycorp.com/solutions/enterprise-mobility-management>

[8.] "Set up." Device Link Mobile Device & App Management. Unwired Revolution, p.v. Viernes. 4 Dic 2015.

<http://www.unwireddevicelink.com/setup/>

[9.] "Agencia de Regulación y Control de las Telecomunicaciones", p.v. Viernes. 4 Dic 2015.

<http://www.arcotel.gob.ec/>

ANEXOS

ANEXO 1.- DISTRIBUTIVO DE PERSONAL DE ARCOTEL

Agencia de Regulación y Control de las Telecomunicaciones

Art. 7 de la Ley Orgánica de Transparencia y Acceso a la Información Pública - LOTAIP			
Literal b2) Distributivo de personal de la institución			
No.	**Unidad a la que pertenece**	**Apellidos y nombres de los servidores y servidoras**	**Puesto Institucional**
PROCESOS GOBERNANTES / NIVEL DIRECTIVO			
1	DIRECCIÓN EJECUTIVA	PROAÑO DE LA TORRE ANA VANESSA	DIRECTORA EJECUTIVA
2	DIRECCIÓN EJECUTIVA	CARVAJAL VILLAMAR GONZALO NATANAEL	ASESOR INSTITUCIONAL
3	DIRECCIÓN EJECUTIVA	MENDEZ CASTILLO DIEGO ROLANDO	ASESOR
4	DIRECCIÓN EJECUTIVA	TORRES COSTALES JUAN PABLO	ASESOR
5	COORDINACIÓN GENERAL ADMINISTRATIVA FINANCIERA	ORQUERA VILLENAS EDGAR EDMUNDO	INTENDENTE NACIONAL DE GESTIÓN - COORDINACIÓN GENERAL ADMINISTRATIVA FINANCIERA
6	COORDINACIÓN GENERAL DE ASESORÍA JURÍDICA	POVEDA CAMACHO JUAN FRANCISCO	PROCURADOR GENERAL - COORDINADOR GENERAL DE ASESORÍA JURÍDICA
7	COORDINACIÓN GENERAL DE ASESORÍA JURÍDICA - PATROCINIO JUDICIAL	PEÑAHERRERA VEJAR JOSE LUIS	COORDINADOR GENERAL
8	COORDINACIÓN GENERAL DE ASESORÍA JURÍDICA - JUZGADO NACIONAL DE COACTIVAS	YEPEZ TAMAYO ALBERTO RENE	COORDINADOR INSTITUCIONAL
9	COORDINACIÓN TÉCNICA DE CONTROL	YANEZ ULLOA FRED ANDREY	INTENDENTE NACIONAL DE CONTROL TÉCNICO - COORDINADOR TÉCNICO DE CONTROL
10	COORDINACIÓN TÉCNICA DE REGULACIÓN	AVENDAÑO MORA MARCELO ANTONIO	DIRECTOR GENERAL - COORDINADOR TÉCNICO DE REGULACIÓN
11	COORDINACIÓN ZONAL 2	JATIVA ESPINOSA MIGUEL ANGEL	INTENDENTE REGIONAL - COORDINADOR ZONAL 2
12	COORDINACIÓN ZONAL 3	GALARZA BASTIDAS MIGUEL PATRICIO	DELEGADO REGIONAL - COORDINADOR ZONAL 3
13	COORDINACIÓN ZONAL 4	HERNANDEZ LUNA ROQUE JACINTO	DELEGADO REGIONAL - COORDINADOR ZONAL 4
14	COORDINACIÓN ZONAL 5	MENDEZ CABRERA LUIS GUILLERMO	INTENDENTE REGIONAL - COORDINADOR ZONAL 5
15	COORDINACIÓN ZONAL 6	OCHOA FIGUEROA EDGAR EFRAIN	INTENDENTE REGIONAL - COORDINADOR ZONAL 6
16	DIRECCIÓN ADMINISTRATIVA	SANTIANA ALARCON PABLO ALEJANDRO	DIRECTOR GENERAL
17	DIRECCIÓN DE ATENCIÓN AL USUARIO	PAREDES MOLINA WILLIAM DAVID	DIRECTOR NACIONAL
18	AUDITORÍA INTERNA	SALVADOR JACOME FRANCISCO ALBERTO	PROFESIONAL AUDITOR 4 - DIRECTOR
19	DIRECCIÓN DE CERTIFICACIÓN DE EQUIPOS DE TELECOMUNICACIONES E INVESTIGACIÓN	AVILES BURBANO MARIA TERESA	DIRECTOR NACIONAL
20	DIRECCIÓN DE COMUNICACIÓN	BEGNINI DOMINGUEZ LUCIA FERNANDA	DIRECTOR NACIONAL
21	DIRECCIÓN DE CONTROL DE SERVICIOS DE TELECOMUNICACIONES	VALDIVIEZO BLACK ANA GABRIELA	DIRECTOR NACIONAL
22	DIRECCIÓN DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	GALLO MOYA CARLOS ANDRES	DIRECTOR NACIONAL
23	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	VITERI TORRES CATALINA DE LOS ANGELES	SECRETARIA GENERAL **(E)**
24	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	GOMEZ DE LA TORRE GOMEZ JOSE MARIA	DIRECTOR NACIONAL **(E)**
25	DIRECCIÓN DE PLANIFICACIÓN DE LAS TELECOMUNICACIONES	VALENCIA BARAHONA VIRGILIO RAMIRO	DIRECTOR GENERAL
26	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	GUERRERO LOOR HENRY PATRICIO	DIRECTOR GENERAL
27	DIRECCIÓN DE PROCESOS	LOPEZ GONZALEZ MARIAM SORAYA	DIRECTOR NACIONAL
28	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	SALAZAR SAETEROS DIEGO JAVIER	DIRECTOR GENERAL
29	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	VELASQUEZ AGUILAR JENNY GUADALUPE	DIRECTOR GENERAL
30	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	BALSECA CHAVEZ DIEGO PATRICIO	DIRECTOR NACIONAL
31	DIRECCIÓN DE TALENTO HUMANO	SUAREZ NARANJO ANGEL GERARDO	DIRECTOR NACIONAL
32	DIRECCIÓN FINANCIERA	SEGOVIA MEJIA FERNANDO EFRAÍN	DIRECTOR NACIONAL
33	DIRECCIÓN FINANCIERA	MANCERO PINOS GLADYS DEL ROCIO	COORDINADOR GENERAL
34	DIRECCIÓN JURÍDICA DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES	BURBANO ARIAS ESTEBAN SANTIAGO	DIRECTOR NACIONAL
35	DIRECCIÓN JURÍDICA DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	VASCONEZ VILLALBA AIDA ELVIA	DIRECTOR NACIONAL
36	DIRECCIÓN JURÍDICA DE REGULACIÓN	QUISHPE GONZALEZ JUDITH SALOME	DIRECTOR GENERAL **(E)**
37	OFICINA TÉCNICA GALÁPAGOS	JAYA SANCHEZ OSCAR XAVIER	DELEGADO REGIONAL **(E)**
PROCESOS AGREGADORES DE VALOR / NIVEL OPERATIVO			
38	COORDINACIÓN GENERAL DE ASESORÍA JURÍDICA	PORRAS MARGARITA GUADALUPE	AUXILIAR DE SERVICIOS
39	COORDINACIÓN GENERAL DE ASESORÍA JURÍDICA	SALCEDO ARCOS ANA ELIZABETH	ASISTENTE ADMINISTRATIVO 3
40	COORDINACIÓN TÉCNICA DE CONTROL	CHAMAZA CHICAIZA FRANCISCO XAVIER	AYUDANTE DE OFICINA
41	COORDINACIÓN TÉCNICA DE CONTROL	FLORES SARANCHI LUIS ENRIQUE	ASISTENTE PROFESIONAL 2
42	COORDINACIÓN TÉCNICA DE CONTROL	IZURIETA TORRES MONICA GRACIELA	ASISTENTE PROFESIONAL 2
43	COORDINACIÓN TÉCNICA DE CONTROL	MOSQUERA JACOME ANDREA VERONICA	ASISTENTE ADMINISTRATIVO 4
44	DIRECCIÓN DE ATENCIÓN AL USUARIO	BELTRAN VINUEZA MARCO PATRICIO	PROFESIONAL ADMINISTRADOR 3
45	DIRECCIÓN DE ATENCIÓN AL USUARIO	CASTILLO ROMERO SILBANA AMABILIA	ASISTENTE PROFESIONAL 1
46	DIRECCIÓN DE ATENCIÓN AL USUARIO	COBA ROMERO AMPARO MIREYA	ASISTENTE PROFESIONAL 4
47	DIRECCIÓN DE ATENCIÓN AL USUARIO	GUALOTUÑA PUNGACHO JOSE EDUARDO	ASISTENTE ADMINISTRATIVO 4
48	DIRECCIÓN DE ATENCIÓN AL USUARIO	MORALES HECTOR FABIAN	ASISTENTE PROFESIONAL 1
49	DIRECCIÓN DE ATENCIÓN AL USUARIO	RENGEL ALVEAR AUGUSTA XIMENA	ESPECIALISTA JEFE 1
50	DIRECCIÓN DE ATENCIÓN AL USUARIO	SALAZAR ESPIN GONZALO ALFONSO	ASISTENTE PROFESIONAL 1
51	DIRECCIÓN DE ATENCIÓN AL USUARIO	SARZOSA CARRION MONICA PATRICIA	ASISTENTE PROFESIONAL 1
52	DIRECCIÓN DE ATENCIÓN AL USUARIO	SOLANO DE LA SALA BROWN JUAN ANTONIO	ASISTENTE PROFESIONAL 3
53	DIRECCIÓN DE CERTIFICACIÓN DE EQUIPOS	BAUZ TAPIA LUIS PABLO	PROFESIONAL ADMINISTRADOR 1
54	DIRECCIÓN DE CERTIFICACIÓN DE EQUIPOS	MATUTE SAVICKAS RAFAEL	PROFESIONAL TECNICO 2
55	DIRECCIÓN DE CERTIFICACIÓN DE EQUIPOS	MIRANDA CASTELLANOS CESAR IVAN	PROFESIONAL TECNICO 1
56	DIRECCIÓN DE CERTIFICACIÓN DE EQUIPOS	MOLINA GAVILANEZ LUIS FERNANDO	SERVIDOR PUBLICO 5
57	DIRECCIÓN DE CERTIFICACIÓN DE EQUIPOS	NORIEGA MORA RAMIRO SANTIAGO	PROFESIONAL TECNICO 1
58	DIRECCIÓN DE CERTIFICACIÓN DE EQUIPOS	RODRIGUEZ ACOSTA GERMANIA MARIA	ASISTENTE PROFESIONAL 1
59	DIRECCIÓN DE CERTIFICACIÓN DE EQUIPOS	SALAZAR MARIANA DE LOURDES	AUXILIAR DE SERVICIOS
60	DIRECCIÓN DE CERTIFICACIÓN DE EQUIPOS	VINUEZA VINUEZA LUIS ALFREDO	PROFESIONAL TECNICO 2
61	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	AGUIRRE CHECA MELBA SOLIMAR	PROFESIONAL INFORMATICO 2
62	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	ARCE VERA CRISTIAN FERNANDO	PROFESIONAL TECNICO 1
63	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	AVILA ROSAS AMANDA PAULINA	SERVIDOR PUBLICO 6
64	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	BAUTISTA DUEÑAS CHARLIE EDUARDO	PROFESIONAL TECNICO 1
65	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	CARTAGENA ANDRADE MARLON JHOVANNY	PROFESIONAL TECNICO 1
66	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	CHAVEZ CEVALLOS GIOVANINA ISABEL	ASISTENTE PROFESIONAL 2
67	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	CRESPO GOMEZ WILMA ROMELIA	PROFESIONAL FINANCIERO 1
68	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	DIAZ TACO CRYSTIAN NELSON	PROFESIONAL TECNICO 1
69	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	GAGLIARDO HERNANDEZ GINA SOFIA	PROFESIONAL ADMINISTRADOR 1
70	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	GILER EGUEZ CARLOS ALEJANDRO	PROFESIONAL TECNICO 1
71	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	GUAYGUA TOAPANTA DAVID EMILIO	PROFESIONAL TECNICO 1
72	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	NAZAMUES QUENGUAN ANA LUCIA	PROFESIONAL TECNICO 1
73	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	PEREZ VACA EDISON RAFAEL	PROFESIONAL TECNICO 1
74	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	PUMA CONSTANTE LUIS ANDRES	SERVIDOR PUBLICO 6
75	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	RUIZ OCAMPO PAHOLA ANDREA	PROFESIONAL TECNICO 2
76	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	SUAREZ CALDERON LUIS HERNAN	PROFESIONAL TECNICO 1
77	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	TORRES VEINTIMILLA ISAAC OLIVERIO	ASISTENTE ADMINISTRATIVO 1
78	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	ULLOA CAMPOS DAYSI PATRICIA	SERVIDOR PUBLICO 6
79	DIRECCIÓN DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	VARELA BURBANO FABIAN ANDRES	SERVIDOR PUBLICO 5
80	DIRECCIÓN DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	ESCOBAR CAIZA VERONICA PATRICIA	PROFESIONAL TECNICO 1
81	DIRECCIÓN DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	LINCANGO PACHA ANIBAL GILBERTO	AUXILIAR DE SERVICIOS
82	DIRECCIÓN DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	MARTINEZ VILLACRESES JUAN CARLOS	PROFESIONAL TECNICO 2
83	DIRECCIÓN DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	MORENO SUAREZ MARITZA DEL PILAR	ASISTENTE PROFESIONAL 1
84	DIRECCIÓN DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	PANCHI HERRERA EDWIN GONZALO	PROFESIONAL TECNICO 3
85	DIRECCIÓN DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	RODRIGUEZ COBA JHONNY HOMERO	ASISTENTE PROFESIONAL 2
86	DIRECCIÓN DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	YEPEZ CROW HUGO SANTIAGO	PROFESIONAL TECNICO 1
87	DIRECCIÓN DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	ZAMBONINO RUBIO FRANKLIN MARCELO	PROFESIONAL TECNICO 3
88	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	ALVAREZ SEGURA FRANKLIN RAMIRO	ASISTENTE PROFESIONAL 3
89	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	CONDOR MAIGUALCA FRANKLIN EDMUNDO	PROFESIONAL TECNICO 4
90	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	GUACHO MOROCHO DIEGO DAVID	SERVIDOR PUBLICO 6
91	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	JACOME TORRES ANA LORENA	PROFESIONAL TECNICO 1
92	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	NARVAEZ MORILLO EDWIN ARMANDO	PROFESIONAL TECNICO 1
93	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	NEGRETE ESPINOSA MARIA FERNANDA	ASISTENTE PROFESIONAL 1
94	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	NOBOA YANEZ DIEGO ANDRES	SERVIDOR PUBLICO 5
95	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	PEREZ LUDEÑA LUIS ANIBAL	CONDUCTOR DE AUTOMOTOR 1
96	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	PEREZ VILLARREAL DARWIN ROBERTO	ASISTENTE PROFESIONAL 3
97	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	RIVADENEIRA FUENTES MARCO DAVID	SERVIDOR PUBLICO 7

98	DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	URIBE NOGALES DIEGO MAURICIO	PROFESIONAL TECNICO 2
99	DIRECCIÓN DE PLANIFICACIÓN DE LAS TELECOMUNICACIONES	ESTRELLA PEREZ DANIELA ALEJANDRA	JEFE DE AREA 2
100	DIRECCIÓN DE PLANIFICACIÓN DE LAS TELECOMUNICACIONES	HERNANDEZ SILVA ROSA JIMENA	SERVIDOR PUBLICO 4
101	DIRECCIÓN DE PLANIFICACIÓN DE LAS TELECOMUNICACIONES	RIVADENEIRA NARANJO FANNY ELENA	JEFE DE AREA 2
102	DIRECCIÓN DE PLANIFICACIÓN DE LAS TELECOMUNICACIONES	RUIZ RUANO LOURDES CONSUELO	SERVIDOR PUBLICO 5
103	DIRECCIÓN DE PLANIFICACIÓN DE LAS TELECOMUNICACIONES	SEGURA RIOS ALLISON NICOLE	SERVIDOR PUBLICO DE APOYO 4
104	DIRECCIÓN DE PLANIFICACIÓN DE LAS TELECOMUNICACIONES	SUASNAVAS FLORES MARIA ISABEL	ESPECIALISTA JEFE 1
105	DIRECCIÓN DE PLANIFICACIÓN DE LAS TELECOMUNICACIONES	TORRES LOZADA GLORIA EVANGELINA	JEFE DE AREA 1
106	DIRECCIÓN DE PLANIFICACIÓN DE LAS TELECOMUNICACIONES	VASQUEZ CASTRO BRYAN SEBASTIAN	SERVIDOR PUBLICO 7
107	DIRECCIÓN DE PLANIFICACIÓN DE LAS TELECOMUNICACIONES	VITERI VAYAS PATRICIO ANDRES	SERVIDOR PUBLICO 1
108	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	ANDRADE CHACON IVAN JOSE	SERVIDOR PUBLICO 1
109	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	ASTUDILLO TORRES MARIA FERNANDA	OFICINISTA
110	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	DIAZ VILLACIS LUIS EFREN	PROFESIONAL TECNICO 4
111	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	FLORES CASTILLO RITA DEL CARMEN	ASISTENTE
112	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	FUERTES MARTINEZ MIREYA CRISTINA	SERVIDOR PUBLICO 6
113	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	JACOME ALTAMIRANO MARCO LEOPOLDO	SUBDIRECTOR GENERAL
114	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	JARAMILLO RIVADENEIRA HERNAN RAMIRO	PROFESIONAL TECNICO 3
115	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	MONTUFAR FELIX PAOLA FATIMA	ESPECIALISTA DE PLANIFICACIÓN INSTITUCIONAL
116	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	REYES REYES LUIS ALCIDES	PROFESIONAL ADMINISTRADOR 3
117	DIRECCIÓN DE PLANIFICACIÓN Y PROYECTOS	RON SANCHEZ KARLA BELEN	SERVIDOR PUBLICO 1
118	DIRECCIÓN DE PROCESOS	AGUILAR AREVALO BLANCA MARIBEL	ASISTENTE PROFESIONAL 3
119	DIRECCIÓN DE PROCESOS	CALVACHE BANDA GUILLERMO AUGUSTO	PROFESIONAL TECNICO 2
120	DIRECCIÓN DE PROCESOS	QUINTEROS VACA ANDRES FERNANDO	PROFESIONAL ADMINISTRADOR 1
121	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	ABARCA TORRES ADRIANA DEL PILAR	OFICIAL ADMINISTRATIVO 2
122	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	AGUILAR SANCHEZ GIOVANNI DANILO	SUBDIRECTOR GENERAL
123	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	ARELLANO PINEDA LIBIA ANABEL	SERVIDOR PUBLICO 5
124	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	AREVALO WASHIMA ROBERTO XAVIER	SERVIDOR PUBLICO 5
125	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	ARIAS PINEDA SANDRA MARGOTH	ANALISTA DE GESTIÓN DE SERVICIOS DE TELECOMUNICACIÓN, RADIODIFUSIÓN Y TELEVISIÓN
126	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	ASQUI ARROBA ADOLFO OTTOMAR	ESPECIALISTA JEFE 1
127	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	CRUZ BAÑO MAYRA ALEXANDRA	ANALISTA DE GESTIÓN DE SERVICIOS DE TELECOMUNICACIÓN, RADIODIFUSIÓN Y TELEVISIÓN
128	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	FLORES HERRERA ALEJANDRO DARIO	SERVIDOR PUBLICO 1
129	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	FUERTES GUANGA MARIBEL GEOVANNA	SERVIDOR PUBLICO 5
130	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	GARZON PEÑAFIEL SILVANA ELIZABETH	ANALISTA DE GESTIÓN DE SERVICIOS DE TELECOMUNICACIÓN, RADIODIFUSIÓN Y TELEVISIÓN
131	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	GARZON PERUGACHI JOHAN FABIAN	JEFE DE DIVISION
132	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	GUAMIALAMA PAZMIÑO GIOVANNY SANTIAGO	SERVIDOR PUBLICO 7
133	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	LOPEZ PIEDRA PABLO IVAN	SUBDIRECTOR GENERAL
134	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	MACHADO SARZOSA SANTIAGO ANDRES	SERVIDOR PUBLICO 2
135	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	MARTINEZ CHICANGO HECTOR STALIN	ANALISTA EN GESTIÓN TÉCNICA
136	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	MERINO MALDONADO JAVIER ALEJANDRO	SERVIDOR PUBLICO 6
137	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	NUÑEZ PERALVO DANIEL ALEJANDRO	JEFE DE DIVISION
138	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	PAREDES TERAN ANA CAROLINA	SERVIDOR PUBLICO 3
139	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	PERUGACHI BETANCOURT MARIA LUISA	JEFE DE DIVISION
140	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	SALAZAR ZAPATA VICTOR HUGO	ESPECIALISTA JEFE 1
141	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	SARANGO VERA WILSON ALONSO	SERVIDOR PUBLICO 5
142	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	TEJADA GUARNIZO DAVID ARMANDO	SERVIDOR PUBLICO 5
143	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	VALDIVIESO NOLIVOS MARIBEL ALEJANDRA	ASISTENTE DE GESTIÓN DE SERVICIOS DE TELECOMUNICACIONES, RADIODIFUSIÓN Y TELEVISIÓN
144	DIRECCIÓN DE REGULACIÓN DE SERVICIOS DE TELECOMUNICACIONES	VIZUETE LOPEZ MARCOS MESIAS	SERVIDOR PUBLICO 7
145	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	ACOSTA VACA DIEGO FABIAN	ESPECIALISTA JEFE 2
146	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	AGUILAR GONZAGA OSCAR VICENTE	ESPECIALISTA JEFE 1
147	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	ANDRADE TITO RAMIRO FRANCISCO	SERVIDOR PÚBLICO 5
148	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	ANGULO CRUZ DORIAN ALEXANDER	ESPECIALISTA JEFE 1
149	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	BAYAS PALACIOS EDGAR GUILLERMO	ANALISTA DE GESTIÓN EN ESPECTRO RADIOELÉCTRICO
150	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	CARRILLO AUQUILLA JENNY BELEN	JEFE DE DIVISIÓN
151	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	CHICANGO RAMIREZ NANCY MARIA	SERVIDOR PÚBLICO 5
152	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	GARAY OLIVO DELCIA VANESSA	ESPECIALISTA JEFE 1
153	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	GUAYAQUIL VILLARROEL SILVANA CLEMENTINA	SERVIDOR PÚBLICO 2
154	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	IBUJES FACTOS LENIN MAURICIO	JEFE DE ÁREA 1
155	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	JACOME ALZAMORA DELIA MARGARITA	JEFE DE ÁREA 1
156	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	MARTINEZ TORRES IBETH ELISA	ESPECIALISTA JEFE 1
157	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	MENDEZ GRUEZO GIOVANA JOSEFINA	SERVIDOR PÚBLICO 7
158	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	MERINO CADENA DIEGO ARMANDO	ESPECIALISTA JEFE 1
159	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	MIRANDA GRIJALVA HAROLD ESTUARDO	SERVIDOR PÚBLICO 2
160	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	PALATE CRIOLLO FRANKLIN BOLIVAR	ASISTENTE DE GESTIÓN EN ESPECTRO RADIOELÉCTRICO
161	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	POZO FELIX SONIA ELIZABETH	SERVIDOR PÚBLICO 6
162	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	QUEL HERMOSA EDWIN GUILLERMO	OFICIAL ADMINISTRATIVO 2
163	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	RAMIREZ YANEZ KATTY ALEXANDRA	SERVIDOR PÚBLICO 2
164	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	RIOFRIO AGUIRRE MONICA PATRICIA	SERVIDOR PÚBLICO 2
165	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	RODRIGUEZ CAICEDO HENRY VINICIO	ANALISISTA DE GESTIÓN EN ESPECTRO RADIOELECTRICO
166	DIRECCIÓN DE REGULACIÓN DEL ESPECTRO RADIOELÉCTRICO	ZHUNIO CIFUENTES JENNY PAULINA	ESPECIALISTA JEFE 1
167	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	ALMEIDA TORRES ILICH ALEXANDER	SERVIDOR PUBLICO 6
168	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	ARACIL JACOME IVAN ORLANDO	PROFESIONAL INFORMATICO 1
169	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	BALLADARES ENRIQUEZ CARLOS ALBERTO	PROFESIONAL INFORMATICO 1
170	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	CEDEÑO ZAMBRANO MARIA ELIZABETH	SERVIDOR PUBLICO 6
171	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	DÍAZ LOACHAMIN JOSE JACINTO	SERVIDOR PUBLICO 6
172	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	GARCES VITERI CARLOS ALBERTO	JEFE DE AREA 1
173	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	IBARRA REYES LUIS EDUARDO	ESPECIALISTA JEFE 1
174	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	JURADO BUITRON GABRIELA EDITH	PROFESIONAL INFORMATICO 1
175	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	MALES CEVALLOS GIOVANNY MARCELO	SERVIDOR PUBLICO 7
176	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	MEJIA SALAZAR ALEXANDRA DEL ROCIO	ESPECIALISTA JEFE 1
177	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	MONTOYA ROSALES LENIN BLADIMIR	ASISTENTE ADMINISTRATIVO 1
178	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	MUÑOZ MERA ROSA ALEXANDRA	SERVIDOR PUBLICO DE APOYO 3
179	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	PAREDES GUANANGA BOLIVAR	OFICIAL ADMINISTRATIVO 1
180	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	PINTO RAMIREZ ANDREA PATRICIA	SERVIDOR PUBLICO 1
181	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	RAMIREZ RECALDE VICTOR JULIO	ESPECIALISTA JEFE 2
182	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	SARAGURO GUAMAN MARIBEL ESPERANZA	ASISTENTE DE TECNOLOGÍAS DE LA INFORMACIÓN
183	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	VASQUEZ PILLAJO JENNY IRENE	SERVIDOR PUBLICO 6
184	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	VILLAVICENCIO CORTEZ MARIA ANGÉLICA	SERVIDOR PUBLICO DE APOYO 4
185	DIRECCIÓN DE SISTEMAS INFORMÁTICOS	ZHAMUNGUI OVIEDO CHRISTIAN XAVIER	SERVIDOR PUBLICO 5
186	DIRECCIÓN JURÍDICA DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES	CHICAIZA MORALES YOLANDA MARCELA	ASISTENTE PROFESIONAL 3
187	DIRECCIÓN JURÍDICA DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES	CHIRIBOGA PAZMIÑO VICTOR HUGO	AYUDANTE DE OFICINA
188	DIRECCIÓN JURÍDICA DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES	GUERRA GUERRA GUSTAVO RICARDO	PROFESIONAL JURIDICO 2
189	DIRECCIÓN JURÍDICA DE CONTROL DE SERVICIOS DE LAS TELECOMUNICACIONES	SEMINARIO ESPARZA JUAN RAMON	PROFESIONAL JURIDICO 2
190	DIRECCIÓN JURÍDICA DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	ARGUDO LOPEZ HAIDY IRINA	ASISTENTE PROFESIONAL 1
191	DIRECCIÓN JURÍDICA DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	BECERRA CHINGAL ALEX PATRICIO	SERVIDOR PUBLICO 1
192	DIRECCIÓN JURÍDICA DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	CABRERA BONILLA MAYRA PAOLA	SERVIDOR PUBLICO 3
193	DIRECCIÓN JURÍDICA DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	MONCAYO ROLDAN KARLA ELIZABETH	SERVIDOR PUBLICO 4
194	DIRECCIÓN JURÍDICA DE CONTROL DEL ESPECTRO RADIOELÉCTRICO	SARAVIA ALTAMIRANO ROBERTO DAVID	SERVIDOR PUBLICO 6
195	DIRECCIÓN JURÍDICA DE REGULACIÓN	BOLAÑOS MONTERO TATIANA DEL ROCIO	ESPECIALISTA JURÍDICO EN GESTIÓN DE TÍTULOS HABILITANTES
196	DIRECCIÓN JURÍDICA DE REGULACIÓN	CABEZAS REA SANDRA CATALINA	SUBDIRECTOR GENERAL
197	DIRECCIÓN JURÍDICA DE REGULACIÓN	CAJAS CASA ANDREA ELIZABETH	SERVIDOR PUBLICO 1
198	DIRECCIÓN JURÍDICA DE REGULACIÓN	CALDERON ZAPATA MAURICIO ABDON	OFICIAL ADMINISTRATIVO 3
199	DIRECCIÓN JURÍDICA DE REGULACIÓN	CARRION MORA DAVID FERNANDO	SERVIDOR PUBLICO 7
200	DIRECCIÓN JURÍDICA DE REGULACIÓN	CHICAIZA IZA MIRIAN JEANETH	SERVIDOR PUBLICO 4
201	DIRECCIÓN JURÍDICA DE REGULACIÓN	DONOSO TOBAR DAVID	ESPECIALISTA JEFE 1
202	DIRECCIÓN JURÍDICA DE REGULACIÓN	ESCOBAR BENITEZ ADRIANA CATALINA	OFICIAL ADMINISTRATIVO 2
203	DIRECCIÓN JURÍDICA DE REGULACIÓN	ESCOBAR ESCOBAR VANESSA ELIZABETH	SERVIDOR PUBLICO 5
204	DIRECCIÓN JURÍDICA DE REGULACIÓN	FLORES VACA LAURA INES	ASISTENTE PROFESIONAL 2
205	DIRECCIÓN JURÍDICA DE REGULACIÓN	GARCIA FREIRE PATRICIA MAGDALENA	ASISTENTE DE PROFESIONAL
206	DIRECCIÓN JURÍDICA DE REGULACIÓN	GUAMANI DEFAZ JADIRA ALEXANDRA	ANALISTA DE CONTRATACIÓN DE BIENES Y SERVICIOS
207	DIRECCIÓN JURÍDICA DE REGULACIÓN	GUERRERO GUERRERO VIVIANA JACQUELINE	SERVIDOR PUBLICO 1
208	DIRECCIÓN JURÍDICA DE REGULACIÓN	HUACHO RODRIGUEZ VERONICA ALEXANDRA	SERVIDOR PUBLICO 7
209	DIRECCIÓN JURÍDICA DE REGULACIÓN	LEIVA VELASQUEZ MICHELLE	SERVIDOR PUBLICO 4
210	DIRECCIÓN JURÍDICA DE REGULACIÓN	MACIAS AGUAYO NARCISA MONSERRATE	SERVIDOR PUBLICO 2
211	DIRECCIÓN JURÍDICA DE REGULACIÓN	MALDONADO PEREZ GRACIELA PIEDAD	ESPECIALISTA JEFE 1

212	DIRECCIÓN JURÍDICA DE REGULACIÓN	MARIN VALLADARES ROSA MATILDE	JUEZ NACIONAL DE COACTIVAS
213	DIRECCIÓN JURÍDICA DE REGULACIÓN	MOLINA OSORIO MARIA EUGENIA	SERVIDOR PUBLICO 5
214	DIRECCIÓN JURÍDICA DE REGULACIÓN	MORA NARVAEZ EUGENIA VANESSA	SERVIDOR PUBLICO 2
215	DIRECCIÓN JURÍDICA DE REGULACIÓN	PALIZ DAVILA HERNAN EFREN	SUBDIRECTOR GENERAL
216	DIRECCIÓN JURÍDICA DE REGULACIÓN	PEÑA TITUAÑA WILLAMS RIGOBERTO	ESPECIALISTA JURÍDICO
217	DIRECCIÓN JURÍDICA DE REGULACIÓN	PINCAY PARRALES ROMELIA JANETH	SERVIDOR PUBLICO 3
218	DIRECCIÓN JURÍDICA DE REGULACIÓN	POZO RUEDA EDISON ULPIANO	JEFE DE DIVISION
219	DIRECCIÓN JURÍDICA DE REGULACIÓN	PUGA BENALCAZAR PABLO HERNAN	SERVIDOR PUBLICO 7
220	DIRECCIÓN JURÍDICA DE REGULACIÓN	QUIJANO PEÑAFIEL GUSTAVO ALEJANDRO	SUBDIRECTOR GENERAL
221	DIRECCIÓN JURÍDICA DE REGULACIÓN	ROMAN ROMAN ROCIO DEL CARMEN	OFICIAL ADMINISTRATIVO 1
222	DIRECCIÓN JURÍDICA DE REGULACIÓN	ROSERO ERAZO ANDREA MARIBEL	SERVIDOR PUBLICO 3
223	DIRECCIÓN JURÍDICA DE REGULACIÓN	ZAMBRANO CEDEÑO YAEL MERCEDES	OFICIAL ADMINISTRATIVO 1
224	JUZGADO NACIONAL DE COACTIVAS	LOPEZ MIÑO CARLOS LUIS	ASISTENTE ADMINISTRATIVO 2
225	PATROCINIO JUDICIAL	TORRES HIDALGO JOSE MIGUEL	ASISTENTE PROFESIONAL 4
		PROCESOS DESCONCENTRADOS	
226	COORDINACIÓN ZONAL 2	BALDEON VALENCIA LUIS EFREN	ASISTENTE PROFESIONAL 4
227	COORDINACIÓN ZONAL 2	BUENO GARCES FANNY YOLANDA	ASISTENTE ADMINISTRATIVO 3
228	COORDINACIÓN ZONAL 2	CARRION PAZMIÑO JORGE EDUARDO	PROFESIONAL JURIDICO 1
229	COORDINACIÓN ZONAL 2	CRIOLLO ROMAN CHRISTIAN MAURICIO	SERVIDOR PUBLICO 7
230	COORDINACIÓN ZONAL 2	FILIAN NARVAEZ MARCELO RICARDO	PROFESIONAL TECNICO 1
231	COORDINACIÓN ZONAL 2	GAVILANES FREILE PENELOPE ROCIO	ASISTENTE PROFESIONAL 2
232	COORDINACIÓN ZONAL 2	GORDILLO ALOMIA MIGUEL IVAN	ASISTENTE PROFESIONAL 1
233	COORDINACIÓN ZONAL 2	GRANDA SOTOMAYOR GONZALO PATRICIO	ASISTENTE PROFESIONAL 1
234	COORDINACIÓN ZONAL 2	GUERRA FERNANDEZ PUBLIO FERNANDO	CONDUCTOR DE AUTOMOTOR 2
235	COORDINACIÓN ZONAL 2	GUERRERO GANAN GUALBERTO RODRIGO	CONDUCTOR DE AUTOMOTOR 1
236	COORDINACIÓN ZONAL 2	GUTIERREZ GUTIERREZ FRANCISCO XAVIER	ASISTENTE PROFESIONAL 3
237	COORDINACIÓN ZONAL 2	HALLO ORTIZ MAGNO ORLANDO	ASISTENTE PROFESIONAL 3
238	COORDINACIÓN ZONAL 2	JARAMILLO CASTILLO CARLOS ALBERTO	CONDUCTOR DE AUTOMOTOR 1
239	COORDINACIÓN ZONAL 2	LAIQUEZ MULLO EDISON VINICIO	ASISTENTE PROFESIONAL 3
240	COORDINACIÓN ZONAL 2	LASSO PLAZA PABLO FERNANDO	PROFESIONAL TECNICO 3
241	COORDINACIÓN ZONAL 2	LUNA DIAZ BOLIVAR MAURICIO	CONDUCTOR DE AUTOMOTOR 1
242	COORDINACIÓN ZONAL 2	MEJIA ENCALADA JOSE LUIS	ASISTENTE PROFESIONAL 1
243	COORDINACIÓN ZONAL 2	MEZA AYALA MARIA JOSE	PROFESIONAL TECNICO 1
244	COORDINACIÓN ZONAL 2	MONTEROS MONTENEGRO NELSON GUSTAVO	PROFESIONAL TECNICO 1
245	COORDINACIÓN ZONAL 2	NARANJO VILLACRES DIEGO RICARDO	PROFESIONAL TECNICO 1
246	COORDINACIÓN ZONAL 2	ORDOÑEZ TALBOT JAIME RODRIGO	PROFESIONAL JURIDICO 3
247	COORDINACIÓN ZONAL 2	PAEZ VASQUEZ XAVIER SANTIAGO	ASISTENTE PROFESIONAL 3
248	COORDINACIÓN ZONAL 2	ROSERO CRESPO LORENA PATRICIA	ASISTENTE ADMINISTRATIVO 2
249	COORDINACIÓN ZONAL 2	SALAS MONTIEL GIOVANNY AGUSTIN	CONDUCTOR DE AUTOMOTOR 1
250	COORDINACIÓN ZONAL 2	SANCHEZ GUEVARA FAUSTO ERNESTO	ASISTENTE PROFESIONAL 4
251	COORDINACIÓN ZONAL 2	SUAREZ FABARA IVAN RODRIGO	ASISTENTE PROFESIONAL 4
252	COORDINACIÓN ZONAL 2	TERAN BRAVO JULIO CESAR	CONDUCTOR DE AUTOMOTOR 1
253	COORDINACIÓN ZONAL 2	VALLE BUSTAMANTE CARMIÑA IVETH	SERVIDOR PUBLICO 5
254	COORDINACIÓN ZONAL 2	VALLEJO BASANTES JORGE RAMIRO	PROFESIONAL TECNICO 2
255	COORDINACIÓN ZONAL 2	VELASCO ESPINOSA JOSE MARIA	ASISTENTE PROFESIONAL 1
256	COORDINACIÓN ZONAL 2	VILLAGOMEZ QUIJANO LUIS GONZAGA	ASISTENTE PROFESIONAL 4
257	COORDINACIÓN ZONAL 2	FRANCO MONTES JOHN JOSE	AYUDANTE DE OFICINA
258	OFICINA TÉCNICA SUCUMBÍOS	MALAN MURILLO GABRIELA KATERINE	ASISTENTE ADMINISTRATIVO 1
259	OFICINA TÉCNICA SUCUMBÍOS	ORELLANA GARCIA JOSE ISRAEL	PROFESIONAL TECNICO 1
260	COORDINACIÓN ZONAL 3	ALVAREZ RUILOVA ANA CRISTINA	SERVIDOR PUBLICO DE APOYO 4
261	COORDINACIÓN ZONAL 3	ARIZAGA MOREIRA RAFAEL ASDRUBAL	CONDUCTOR DE AUTOMOTOR 1
262	COORDINACIÓN ZONAL 3	BENITEZ PEREZ MARY FERNANDA	ASISTENTE PROFESIONAL 4
263	COORDINACIÓN ZONAL 3	BUENO SILVA BYRON FERNANDO	CONDUCTOR DE AUTOMOTOR 2
264	COORDINACIÓN ZONAL 3	CAJAS SANCHEZ EDISON BENITO	SERVIDOR PUBLICO 1
265	COORDINACIÓN ZONAL 3	CALVOPIÑA HINOJOSA WILLIAM LEOPOLDO	PROFESIONAL TECNICO 1
266	COORDINACIÓN ZONAL 3	COLOMA VERA VANESSA CAROLINA	SERVIDOR PUBLICO 3
267	COORDINACIÓN ZONAL 3	GONZALEZ ARROBA FERNANDO JOSE	ASISTENTE ADMINISTRATIVO 4
268	COORDINACIÓN ZONAL 3	JIMENEZ ROMERO JORGE EDUARDO	PROFESIONAL TECNICO 1
269	COORDINACIÓN ZONAL 3	LARA CASTELO ANGEL GONZALO	AUXILIAR DE SERVICIOS
270	COORDINACIÓN ZONAL 3	LOPEZ MARTINEZ BERTHA ELIZABETH	ASISTENTE PROFESIONAL 1
271	COORDINACIÓN ZONAL 3	LOZANO RODRIGUEZ MARCO VINICIO	SERVIDOR PUBLICO 6
272	COORDINACIÓN ZONAL 3	MACHUCA PERALTA LINA NARCISA	PROFESIONAL FINANCIERO 1
273	COORDINACIÓN ZONAL 3	RICAURTE COSTALES VICENTE JAVIER	PROFESIONAL FINANCIERO 1
274	COORDINACIÓN ZONAL 3	RODRIGUEZ PACHECO EDWIN FERNANDO	SERVIDOR PUBLICO 6
275	COORDINACIÓN ZONAL 3	TOALOMBO MONTERO ARCADIO MAURICIO	PROFESIONAL TECNICO 1
276	COORDINACIÓN ZONAL 3	TROYA ALDAZ ALEX JOHNINE	PROFESIONAL TECNICO 2
277	COORDINACIÓN ZONAL 3	VELASCO JARA ANGEL HERNAN	PROFESIONAL TECNICO 3
278	COORDINACIÓN ZONAL 3	ZUÑIGA LEMA FRANKLIN GEOVANNY	CONDUCTOR DE AUTOMOTOR 1
279	COORDINACIÓN ZONAL 4	ALONZO GARCIA JAIRO AGUSTIN	AUXILIAR DE SERVICIOS
280	COORDINACIÓN ZONAL 4	BALLADARES FLORES JORGE HUMBERTO	PROFESIONAL TECNICO 1
281	COORDINACIÓN ZONAL 4	BRAVO GARCIA MIGUEL ANGEL	SERVIDOR PUBLICO 5
282	COORDINACIÓN ZONAL 4	CAMPOVERDE GANCHALA JUAN CARLOS	PROFESIONAL TECNICO 1
283	COORDINACIÓN ZONAL 4	CEDEÑO MENDOZA JACOB ADALBERTO	PROFESIONAL TECNICO 1
284	COORDINACIÓN ZONAL 4	INTRIAGO MOREIRA LUIS GUILLERMO	CONDUCTOR DE AUTOMOTOR 1
285	COORDINACIÓN ZONAL 4	MANTUANO LOOR IRENE ELIZABETH	ASISTENTE ADMINISTRATIVO 1
286	COORDINACIÓN ZONAL 4	ORTEGA PINTADO CESAR FERNANDO	SERVIDOR PUBLICO 6
287	COORDINACIÓN ZONAL 4	PEREZ ZAMBRANO ROSANNA KARINA	ASISTENTE PROFESIONAL 3
288	COORDINACIÓN ZONAL 4	SOLORZANO ORMAZA MARIANA DEL JESUS	PROFESIONAL ADMINISTRADOR 1
289	COORDINACIÓN ZONAL 4	SORNOZA GARCIA IGNACIO RODULFO	CONDUCTOR DE AUTOMOTOR 1
290	COORDINACIÓN ZONAL 4	SORNOZA GARCIA WASHINGTON FABIAN	CONDUCTOR DE AUTOMOTOR 1
291	COORDINACIÓN ZONAL 4	VIZUETA SILVA IVAN MIKE	SERVIDOR PUBLICO 7
292	COORDINACIÓN ZONAL 5	AGUIRRE FERNANDEZ ANDREA VIVIANA	SERVIDOR PUBLICO 3
293	COORDINACIÓN ZONAL 5	ALBAN ROBLEDO CLEOFE LORENZO	ASISTENTE PROFESIONAL 1
294	COORDINACIÓN ZONAL 5	ALFONZO GUZMAN MILTON IVAN	SERVIDOR PUBLICO 6
295	COORDINACIÓN ZONAL 5	BALBIN MANTILLA MERY ANTONIETA	RECAUDADOR
296	COORDINACIÓN ZONAL 5	BARROS VEGA MARIANA DE JESUS	ESPECIALISTA JEFE 1
297	COORDINACIÓN ZONAL 5	BENITEZ ENRIQUEZ JAIME ALFREDO	PROFESIONAL TECNICO 3
298	COORDINACIÓN ZONAL 5	BORJA LUNA ROMMEL FEDERICO	ASISTENTE TECNICO 4
299	COORDINACIÓN ZONAL 5	CARDENAS COQUE FRANKLIN MEDARDO	CONDUCTOR DE AUTOMOTOR 2
300	COORDINACIÓN ZONAL 5	CARLOSAMA SUAREZ DALTON BERLIZ	SERVIDOR PUBLICO 3
301	COORDINACIÓN ZONAL 5	CHAVEZ MENDEZ WILBER ANTONIO	CONDUCTOR DE AUTOMOTOR 2
302	COORDINACIÓN ZONAL 5	CHUQUICUSMA VILLACRES JOSE ANTONIO	CONDUCTOR DE AUTOMOTOR 1
303	COORDINACIÓN ZONAL 5	COELLAR SOLORZANO JOSE EDUARDO	PROFESIONAL TECNICO 1
304	COORDINACIÓN ZONAL 5	COELLO BELTRAN GUILLERMO ELIEZER	SERVIDOR PUBLICO 1
305	COORDINACIÓN ZONAL 5	CORDERO GUATUMILLO RAUL CARLOS	PROFESIONAL JURIDICO 2
306	COORDINACIÓN ZONAL 5	CORDOVA ARTEAGA SILVIA CRISTINA	SERVIDOR PUBLICO 4
307	COORDINACIÓN ZONAL 5	DELUGO QUINTO HELGA YAMILE	JEFE DE AREA 2
308	COORDINACIÓN ZONAL 5	FABRE BONILLA CARLOS ALBERTO	ASISTENTE PROFESIONAL 1
309	COORDINACIÓN ZONAL 5	FIGUEROA ROCA PEDRO BISMAR	CONDUCTOR DE AUTOMOTOR 1
310	COORDINACIÓN ZONAL 5	FLORES CASTILLO FAUSTO BOLIVAR	ASISTENTE PROFESIONAL 2
311	COORDINACIÓN ZONAL 5	FREIRE GUERRA GINA ISABEL	PROFESIONAL TECNICO 3
312	COORDINACIÓN ZONAL 5	GALLEGOS SANCHEZ MARIA FERNANDA	ASISTENTE ADMINISTRATIVO 4
313	COORDINACIÓN ZONAL 5	GAME NARVAEZ ROSA MARIA	ASISTENTE ADMINISTRATIVO 2
314	COORDINACIÓN ZONAL 5	GARCES GARCES NEYSER ANTONIO	AUXILIAR DE SERVICIOS
315	COORDINACIÓN ZONAL 5	GARCIA CAMPOS JAIME RAUL	ASISTENTE ADMINISTRATIVO 4
316	COORDINACIÓN ZONAL 5	GONZALEZ LOOR MERCEDES MARITZA	ASISTENTE ADMINISTRATIVO 1
317	COORDINACIÓN ZONAL 5	GUZMAN MIRANDA CARLOS ALBERTO	PROFESIONAL TECNICO 2
318	COORDINACIÓN ZONAL 5	INTRIAGO MACIAS LILA MIRELLA	ASISTENTE PROFESIONAL 1
319	COORDINACIÓN ZONAL 5	IPERTY MUÑOZ GLANDIA YECENIA	ASISTENTE DE PROFESIONAL
320	COORDINACIÓN ZONAL 5	JIMENEZ MOYA RICARDO RONY	ASISTENTE PROFESIONAL 3
321	COORDINACIÓN ZONAL 5	JIMENEZ ROMERO ALBA DANNY	ASISTENTE PROFESIONAL 1
322	COORDINACIÓN ZONAL 5	LARREA VERGARA MELINA NATHALIA	SERVIDOR PUBLICO 5
323	COORDINACIÓN ZONAL 5	LOOR PALLASHCO ZENNIA MARGARITA	SERVIDOR PUBLICO 5
324	COORDINACIÓN ZONAL 5	MAGGI SILVA WALTER OCTAVIO	ESPECIALISTA DE GESTIÓN DEL ESPECTRO RADIOELÉCTRICO Y SERVICOS DE TELECOMUNICACIONES
325	COORDINACIÓN ZONAL 5	MANOSALVAS ROBLES MARIA SISSI	JEFE DE AREA 1
326	COORDINACIÓN ZONAL 5	MATAMOROS CAMPOSANO CARLOS MIGUEL	PROFESIONAL TECNICO 2

327	COORDINACIÓN ZONAL 5	MEDINA MORENO ERICK ADOLFO	SERVIDOR PUBLICO 5
328	COORDINACIÓN ZONAL 5	MORA BARAHONA ISMAEL DANIEL	AUXILIAR DE SERVICIOS
329	COORDINACIÓN ZONAL 5	NEIRA SAONA FRANCISCO CELSO	ASISTENTE PROFESIONAL 4
330	COORDINACIÓN ZONAL 5	PARRALES ESPINOZA ISIDRO BIENVENIDO	CONDUCTOR DE AUTOMOTOR 1
331	COORDINACIÓN ZONAL 5	PIMENTEL VULGARIN ISABEL TERESA	SERVIDOR PUBLICO 6
332	COORDINACIÓN ZONAL 5	PINO YEROVI ANDRES EDUARDO	SERVIDOR PUBLICO 1
333	COORDINACIÓN ZONAL 5	PUMAYUGRA SERNAQUE CHRISTIAN ANTONIO	SERVIDOR PUBLICO 6
334	COORDINACIÓN ZONAL 5	QUINTANA ARMIJO ANGELICA SUSANA	ASISTENTE PROFESIONAL 4
335	COORDINACIÓN ZONAL 5	RUILOVA AGUIRRE MARIA LUZMILA	PROFESIONAL TECNICO 2
336	COORDINACIÓN ZONAL 5	VALLEJO RAMOS CARLOS IVAN	OFICIAL ADMINISTRATIVO 1
337	COORDINACIÓN ZONAL 5	VARGAS ASANZA JANNETH ALEXANDRA	SERVIDOR PUBLICO 7
338	COORDINACIÓN ZONAL 5	VERA AGUILAR JOSE GUILLERMO	CONDUCTOR DE AUTOMOTOR 1
339	COORDINACIÓN ZONAL 5	VERA SOLIS VANESSA FERNANDA	ASISTENTE ADMINISTRATIVO 3
340	COORDINACIÓN ZONAL 5	ZAMBRANO BRAVO TONY JACINTO	CONDUCTOR
341	COORDINACIÓN ZONAL 5	ZAMBRANO MENDIETA JENNIFER ALEXANDRA	SERVIDOR PUBLICO DE APOYO 2
342	COORDINACIÓN ZONAL 5	ZURITA VERGARA JOSE DAVID	PROFESIONAL FINANCIERO 1
343	COORDINACIÓN ZONAL 6	ANDRADE GUERRERO ESTEBAN ANDRES	PROFESIONAL TECNICO 1
344	COORDINACIÓN ZONAL 6	ARCENTALES NIVELO JHON ARTURO	ASISTENTE PROFESIONAL 3
345	COORDINACIÓN ZONAL 6	CHULDE FUENTES ARMANDO DANIEL	PROFESIONAL TECNICO 1
346	COORDINACIÓN ZONAL 6	COELLO MORA ESTEBAN DAMIAN	PROFESIONAL TECNICO 1
347	COORDINACIÓN ZONAL 6	CORONEL VALDIVIEZO CARLOS PATRICIO	CONDUCTOR DE AUTOMOTOR 2
348	COORDINACIÓN ZONAL 6	FIGUEROA TORRES SANTIAGO FERNANDO	SERVIDOR PUBLICO 2
349	COORDINACIÓN ZONAL 6	HURTADO FIGUEROA EDEY RAMIRO	PROFESIONAL TECNICO 1
350	COORDINACIÓN ZONAL 6	JARA PESANTEZ EDWIN GILBERTO	CONDUCTOR
351	COORDINACIÓN ZONAL 6	LEON VELEZ MARCELO JAVIER	ASISTENTE ADMINISTRATIVO 2
352	COORDINACIÓN ZONAL 6	LOPEZ MERCHAN OSWALDO EDUARDO	PROFESIONAL TECNICO 1
353	COORDINACIÓN ZONAL 6	LOPEZ SANMARTIN MARCELO JAVIER	SERVIDOR PUBLICO 2
354	COORDINACIÓN ZONAL 6	LUZURIAGA REYES MAYRA CECILIA	PROFESIONAL JURIDICO 1
355	COORDINACIÓN ZONAL 6	MERINO BERMEO DIANA LUCIA	SERVIDOR PUBLICO 5
356	COORDINACIÓN ZONAL 6	MOGROVEJO QUEZADA FERNANDO VICENTE	CONDUCTOR DE AUTOMOTOR 1
357	COORDINACIÓN ZONAL 6	MOLINA HURTADO VANESSA VERONICA	ASISTENTE ADMINISTRATIVO 2
358	COORDINACIÓN ZONAL 6	MORA ORTIZ FLOR CECILIA	PROFESIONAL TECNICO 1
359	COORDINACIÓN ZONAL 6	MUÑOZ AMOROSO CARLOS PETRONIO	ASISTENTE PROFESIONAL 2
360	COORDINACIÓN ZONAL 6	ORTIZ MENDIETA CARMEN SOLEDAD	PROFESIONAL FINANCIERO 2
361	COORDINACIÓN ZONAL 6	PALOMINO MUÑOZ JORGE EDUARDO	CONDUCTOR DE AUTOMOTOR 1
362	COORDINACIÓN ZONAL 6	PELAEZ ARIAS GIOVANNY MARTIN	CONDUCTOR DE AUTOMOTOR 2
363	COORDINACIÓN ZONAL 6	PEÑAFIEL PALACIOS WILSON FABIAN	PROFESIONAL TECNICO 3
364	COORDINACIÓN ZONAL 6	PEÑAHERRERA CALLE LEOPOLDO MIGUEL	PROFESIONAL TECNICO 3
365	COORDINACIÓN ZONAL 6	PERALTA SANCHEZ GLADIS LUSMILA	SERVIDOR PUBLICO DE APOYO 4
366	COORDINACIÓN ZONAL 6	PIEDRA CARPIO ANA CECILIA	ESPECIALISTA JEFE 1
367	COORDINACIÓN ZONAL 6	RIOS COELLO NANCY YOLANDA DE LOS DOLORES	JEFE DE AREA 1
368	COORDINACIÓN ZONAL 6	ROBLES OCHOA JORGE ARTEMIO	AUXILIAR DE SERVICIOS
369	COORDINACIÓN ZONAL 6	SANCHEZ MORA LORENA ELISABETH	ASISTENTE PROFESIONAL 4
370	COORDINACIÓN ZONAL 6	SANCHEZ PINOS DIEGO MAURICIO	PROFESIONAL TECNICO 1
371	COORDINACIÓN ZONAL 6	SEGARRA PACHECO MARIA KATERINE	ANALISTA DE GESTIÓN DE APOYO
372	COORDINACIÓN ZONAL 6	SIAVICHAY ARIAS CESAR AUGUSTO	PROFESIONAL ADMINISTRADOR 1
373	COORDINACIÓN ZONAL 6	VASQUEZ ALARCON VIVIANA GABRIELA	ANALISTA DE GESTIÓN DEL ESPECTRO RADIOELÉCTRICO Y SERVICIOS DE TELECOMUNICACIONES
374	COORDINACIÓN ZONAL 6	VELASQUEZ RAMIREZ WALTER RODOLFO	ESPECIALISTA JEFE 1
375	COORDINACIÓN ZONAL 6	VELEZ ARIZAGA LORENA DEL CARMEN	OFICIAL ADMINISTRATIVO 1
376	COORDINACIÓN ZONAL 6	ZUMBA ARICHAVALA FELIPE ENRIQUE	PROFESIONAL TECNICO 1
377	OFICINA TÉCNICA DE LOJA	IÑIGUEZ PINEDA CESAR FERNANDO	PROFESIONAL TÉCNICO 1
378	OFICINA TÉCNICA DE LOJA	SARANGO TANDAZO ZOILA PAULINA	ASISTENTE ADMINISTRATIVO 2
379	OFICINA TÉCNICA GALÁPAGOS	CRIOLLO CUEVA SILVANA DE LOS ANGELES	PROFESIONAL TECNICO 1
380	OFICINA TÉCNICA GALÁPAGOS	INSUASTI INGA JANHELLA LILIBETH	ASISTENTE ADMINISTRATIVO 1
381	OFICINA TÉCNICA GALÁPAGOS	JAYA GUACHIMBOZA DANY DANIEL	AYUDANTE DE OFICINA
382	OFICINA TÉCNICA GALÁPAGOS	LOPEZ TUMBACO WASHINGTON RAMON	CONDUCTOR DE AUTOMOTOR 1
383	OFICINA TÉCNICA GALÁPAGOS	MARQUEZ CARPIO ERNESTO EDUARDO	PROFESIONAL ADMINISTRADOR 1
384	OFICINA TÉCNICA GALÁPAGOS	VALDERRAMA LOPEZ GABRIELA GEOVANNA	PROFESIONAL JURIDICO 1
		ASESORÍAS / NIVEL DE APOYO	
385	COORDINACIÓN GENERAL ADMINISTRATIVA FINANCIERA	AVILES FREIRE LAURA VIVIANA	ASISTENTE PROFESIONAL 2
386	COORDINACIÓN GENERAL ADMINISTRATIVA FINANCIERA	GAVILANES ULLOA EDGAR JAVIER	ASISTENTE PROFESIONAL 2
387	DIRECCIÓN ADMINISTRATIVA	AGUILAR MONTENEGRO GEOVANNA DAYANARA	AUXILIAR DE SERVICIOS
388	DIRECCIÓN ADMINISTRATIVA	AMAGUA TACO LUIS PATRICIO	AUXILIAR DE SERVICIOS
389	DIRECCIÓN ADMINISTRATIVA	AÑAZCO ROJAS EDGAR MARCELO	CONDUCTOR
390	DIRECCIÓN ADMINISTRATIVA	BARAHONA LOPEZ JUAN CARLOS	PROFESIONAL ADMINISTRADOR 3
391	DIRECCIÓN ADMINISTRATIVA	CABEZAS PEREZ CHRISTIAN DAVID	SERVIDOR PUBLICO DE APOYO 4
392	DIRECCIÓN ADMINISTRATIVA	CABRERA LOPEZ ERIKA ALEXANDRA	OFICIAL ADMINISTRATIVO 1
393	DIRECCIÓN ADMINISTRATIVA	CAJAS SIERRA JOSE FRANCISCO	CONDUCTOR
394	DIRECCIÓN ADMINISTRATIVA	CAMPAÑA BERMEO WILFRIDO VITERVO	AUXILIAR DE SERVICIOS
395	DIRECCIÓN ADMINISTRATIVA	CASTILLO ORDOÑEZ DIOMER IVAN	ASISTENTE PROFESIONAL 1
396	DIRECCIÓN ADMINISTRATIVA	CUENCA SANTANA VERONICA PATRICIA	SERVIDOR PUBLICO 5
397	DIRECCIÓN ADMINISTRATIVA	ESPIN SEGURA MILTON JOEL	CONDUCTOR DE AUTOMOTOR 1
398	DIRECCIÓN ADMINISTRATIVA	ESTRADA COLCHA SEGUNDO CIRILO	AUXILIAR DE SERVICIOS
399	DIRECCIÓN ADMINISTRATIVA	FLORES LEMA MIGUEL ANGEL	OFICIAL ADMINISTRATIVO 1
400	DIRECCIÓN ADMINISTRATIVA	GAIBOR ESTEVEZ JIMMY GEOVANNY	ASISTENTE ADMINISTRATIVO 3
401	DIRECCIÓN ADMINISTRATIVA	GALARZA RODRIGUEZ PABLO RENATO	ASISTENTE PROFESIONAL 3
402	DIRECCIÓN ADMINISTRATIVA	GAVELA ARIAS PAULINA ELIZABETH	ASISTENTE PROFESIONAL 2
403	DIRECCIÓN ADMINISTRATIVA	GRANJA TERAN ANGEL MAURICIO	JEFE DE DIVISION
404	DIRECCIÓN ADMINISTRATIVA	GUAMAN CHIPANTIZA ANA MARIA	AUXILIAR DE SERVICIOS
405	DIRECCIÓN ADMINISTRATIVA	JUIÑA ANAGUANO HUGO HERNAN	CONDUCTOR
406	DIRECCIÓN ADMINISTRATIVA	LARA ESPINOZA JORGE ABDON	CONDUCTOR
407	DIRECCIÓN ADMINISTRATIVA	LARA ZAPATA ALEJANDRO WLADIMIR	CONDUCTOR DE AUTOMOTOR 1
408	DIRECCIÓN ADMINISTRATIVA	LEMA JARAMILLO MAGALI CATERINE	SERVIDOR PUBLICO DE APOYO 4
409	DIRECCIÓN ADMINISTRATIVA	LEON FERNANDEZ ANTIA DEL CARMEN	PROFESIONAL FINANCIERO 3
410	DIRECCIÓN ADMINISTRATIVA	MENCIAS GAVILANES MARTHA VIRGINIA DE LA DOLOROSA	PROFESIONAL ADMINISTRADOR 4
411	DIRECCIÓN ADMINISTRATIVA	MERINO GAVILANEZ JOSE RAMIRO	OFICIAL ADMINISTRATIVO 2
412	DIRECCIÓN ADMINISTRATIVA	MEZA ORELLANA MARIO ANTONIO	CONDUCTOR DE AUTOMOTOR 1
413	DIRECCIÓN ADMINISTRATIVA	MOSQUERA PADILLA MARIA BELEN	SERVIDOR PUBLICO 5
414	DIRECCIÓN ADMINISTRATIVA	MUÑOZ CHILA LUIS ALFREDO	AUXILIAR DE SERVICIOS
415	DIRECCIÓN ADMINISTRATIVA	OBANDO BASANTES MARIO NAPOLEON	PROFESIONAL ADMINISTRADOR 2
416	DIRECCIÓN ADMINISTRATIVA	OCAMPO OCAMPO PEDRO GUALBERTO	AUXILIAR DE SERVICIOS
417	DIRECCIÓN ADMINISTRATIVA	ORTIZ CHIRIBOGA YOLANDA ELIZABETH	ASISTENTE ADMINISTRATIVO 1
418	DIRECCIÓN ADMINISTRATIVA	ORTIZ YEPEZ EDUARDO RAMIRO	SERVIDOR PUBLICO DE APOYO 4
419	DIRECCIÓN ADMINISTRATIVA	PALACIOS TERAN JUAN PABLO	ASISTENTE PROFESIONAL 4
420	DIRECCIÓN ADMINISTRATIVA	PINEDA ASANZA YONI ANIBAL	CONDUCTOR
421	DIRECCIÓN ADMINISTRATIVA	PINZON CUENCA MANUEL BENIGNO	AUXILIAR DE SERVICIOS
422	DIRECCIÓN ADMINISTRATIVA	PRIETO ROMERO JOSE ANTONIO	SERVIDOR PUBLICO DE APOYO 3
423	DIRECCIÓN ADMINISTRATIVA	QUINCHIMBLA CAIZA LUIS ERNESTO	CONDUCTOR DE AUTOMOTOR 1
424	DIRECCIÓN ADMINISTRATIVA	QUIROZ CEVALLOS CHARLES RAMON	CONDUCTOR DE AUTOMOTOR 2
425	DIRECCIÓN ADMINISTRATIVA	REDROBAN MANTILLA MARIA FERNANDA	ASISTENTE PROFESIONAL 4
426	DIRECCIÓN ADMINISTRATIVA	RIVERA CARDENAS JAIME VINICIO	CONDUCTOR
427	DIRECCIÓN ADMINISTRATIVA	RODRIGUEZ SANTANDER MYRIAN LOURDES	MENSAJERO
428	DIRECCIÓN ADMINISTRATIVA	ROMAN ARAUJO NELSON MARCELO	ASISTENTE ADMINISTRATIVO 3
429	DIRECCIÓN ADMINISTRATIVA	SANGUCHO NEGRETE EDISON WILLIAN	CONDUCTOR DE AUTOMOTOR 1
430	DIRECCIÓN ADMINISTRATIVA	TAIPICAÑA JACOME CARLOS ALBERTO	CONDUCTOR DE AUTOMOTOR 2
431	DIRECCIÓN ADMINISTRATIVA	TERAN ORBEA MANUEL BENJAMIN	CONDUCTOR DE AUTOMOTOR 1
432	DIRECCIÓN ADMINISTRATIVA	TERCERO ALBARRACIN PEDRO LUIS	OFICIAL ADMINISTRATIVO JEFE
433	DIRECCIÓN ADMINISTRATIVA	TIPAN INAQUIZA LUIS DARWIN	AUXILIAR DE SERVICIOS
434	DIRECCIÓN ADMINISTRATIVA	TORRES PAZMIÑO WILMER EDISON	AUXILIAR DE SERVICIOS
435	DIRECCIÓN ADMINISTRATIVA	VASCONEZ SEGOVIA JOSE VICENTE	PROFESIONAL ADMINISTRADOR 2
436	DIRECCIÓN ADMINISTRATIVA	VILLALVA CUEVA DIEGO REINALDO	CONDUCTOR
437	DIRECCIÓN ADMINISTRATIVA	ACOSTA BAEZ PEDRO ALEJANDRO	CONDUCTOR
438	AUDITORÍA INTERNA	ALBUJA LOPEZ SORAYA MONSERRATH	ASISTENTE PROFESIONAL 4
439	AUDITORÍA INTERNA	BONILLA VALDIVIEZO MARGOTH ALEXANDRA	PROFESIONAL AUDITOR 1
440	AUDITORÍA INTERNA	COELLO ROSERO JUAN CARLOS	ASISTENTE PROFESIONAL 4
441	AUDITORÍA INTERNA	CORREA VACA HUGO MARCELO	ESPECIALISTA JEFE 1

442	AUDITORÍA INTERNA	JACOME PONCE CARLOS ALBERTO	ASISTENTE DE PROFESIONAL
443	DIRECCIÓN DE COMUNICACIÓN	BAQUERIZO ORDOÑEZ LILIA CAROLINA	ASISTENTE PROFESIONAL 2
444	DIRECCIÓN DE COMUNICACIÓN	JARRIN COELLO MARIO FERNANDO	PROFESIONAL COMUNICADOR SOCIAL 3
445	DIRECCIÓN DE COMUNICACIÓN	NARANJO MONTALVO JOSE ANDRES	SERVIDOR PUBLICO 6
446	DIRECCIÓN DE COMUNICACIÓN	PASPUEL CALDERON JAVIER HIPOLITO	ASISTENTE PROFESIONAL 1
447	DIRECCIÓN DE COMUNICACIÓN	RODRIGUEZ LEON YANINA EULALIA	ASISTENTE ADMINISTRATIVO 3
448	DIRECCIÓN DE COMUNICACIÓN	TORRES ARGUELLO ANA VALERIA	SERVIDOR PUBLICO 1
449	DIRECCIÓN DE COMUNICACIÓN	VELASCO SUAREZ FREDY MARCELO	PROFESIONAL COMUNICADOR SOCIAL 2
450	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	ARIAS MONTALVO SEBASTIAN ALEJANDRO	SERVIDOR PUBLICO 1
451	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	CHACON ENRIQUEZ CESAR PATRICIO	SERVIDOR PUBLICO 3
452	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	DIAZ TORRES MARCO VINICIO	ASISTENTE PROFESIONAL 2
453	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	FLORES PINEDA TANYA YADIRA	TÉCNICO DE APOYO DE DOCUMENTACIÓN Y ARCHIVO
454	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	FRANCO CHILAN RAMON SEBASTIAN	JEFE DE AREA 1
455	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	GUACHI PUJOS VICTOR ELIAS	ESPECIALISTA JEFE 1
456	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	GUTMAN GUERRON IVAN RODOLFO	ASISTENTE PROFESIONAL 1
457	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	HEREDIA PACHECO JORGE ALEXIS	OFICIAL ADMINISTRATIVO 1
458	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	LAICA GUANIN DIEGO ALEJANDRO	SERVIDOR PUBLICO DE APOYO 4
459	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	LAIQUEZ GUAYAQUIL MARCO VINICIO	ASISTENTE ADMINISTRATIVO 3
460	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	LARREA AMORES MAURICIO ALEJANDRO	TÉCNICO DE APOYO DE DOCUMENTACIÓN Y ARCHIVO
461	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	LESCANO OBANDO IMELDA DULCELINA	ESPECIALISTA JEFE 1
462	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	NARANJO SAENZ MARIANA DE LOS ANGELES	ASISTENTE ADMINISTRATIVO 4
463	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	RENTERIA ANGAMARCA JIMENA ALEXANDRA	OFICIAL ADMINISTRATIVO 2
464	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	TAPIA FUEL STALIN GABRIEL	AYUDANTE DE OFICINA
465	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	TRUJILLO CARRILLO JOAQUINA VICTORIA	AYUDANTE DE OFICINA
466	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	URBINA MAYORGA SONIA CECILIA	ASISTENTE PROFESIONAL 2
467	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	VASCONEZ NAVAS MATILDE BEATRIZ	SERVIDOR PUBLICO 1
468	DIRECCIÓN DE DOCUMENTACIÓN Y ARCHIVO	VELEZ YANEZ JORGE JOSE	ESPECIALISTA JEFE 1
469	DIRECCIÓN DE TALENTO HUMANO	AGUILAR MERINO SILVIA PAOLA	SERVIDOR PUBLICO 6
470	DIRECCIÓN DE TALENTO HUMANO	APOLO CHAMBA MIRIAM DEL ROSARIO	OFICIAL ADMINISTRATIVO 1
471	DIRECCIÓN DE TALENTO HUMANO	GARZON GUAMAN CARMEN ALICIA	ASISTENTE ADMINISTRATIVO 4
472	DIRECCIÓN DE TALENTO HUMANO	HIDALGO PAGUAY LIGIA ELENA	PROFESIONAL ADMINISTRADOR 1
473	DIRECCIÓN DE TALENTO HUMANO	HILASACA YUQUILEMA MARCO VINICIO	PROFESIONAL ADMINISTRADOR 1
474	DIRECCIÓN DE TALENTO HUMANO	LEON GUIJARRO MONICA ILIANA	PROFESIONAL ADMINISTRADOR 3
475	DIRECCIÓN DE TALENTO HUMANO	LOPEZ MEJIA WILLAM ARMANDO	ASISTENTE ADMINISTRATIVO 4
476	DIRECCIÓN DE TALENTO HUMANO	MARTINEZ SOTOMAYOR GLADYS ELIZABETH	JEFE DE DIVISION
477	DIRECCIÓN DE TALENTO HUMANO	MURILLO ARROYO MARIA GABRIELA	SERVIDOR PUBLICO 6
478	DIRECCIÓN DE TALENTO HUMANO	NOROÑA NARANJO LUIS BOLIVAR	ESPECIALISTA JEFE 1
479	DIRECCIÓN DE TALENTO HUMANO	PORRAS BRAGANZA VALERIA ALEXANDRA	SERVIDOR PUBLICO 5
480	DIRECCIÓN DE TALENTO HUMANO	SHAGÑAY PAREDES DAVID ALEJANDRO	SERVIDOR PUBLICO 7
481	DIRECCIÓN DE TALENTO HUMANO	SOSA RUALES CARLA MARIANA	OFICIAL ADMINISTRATIVO JEFE
482	DIRECCIÓN DE TALENTO HUMANO	TAPIA BEDOYA XIMENA DE LOURDES	ASISTENTE PROFESIONAL 2
483	DIRECCIÓN DE TALENTO HUMANO	TERAN ESPINOSA KARLA JIMENA	JEFE DE AREA 1
484	DIRECCIÓN DE TALENTO HUMANO	URIARTE SALVADOR LEONARDO ENRIQUE	JEFE DE ROLES
485	DIRECCIÓN DE TALENTO HUMANO	VILLAGOMEZ VARGAS CHRISTIAN DANIEL	PROFESIONAL ADMINISTRADOR 1
486	DIRECCIÓN DE TALENTO HUMANO	VINUEZA PAZMIÑO RONNAL ANTONIO	SERVIDOR PUBLICO 6
487	DIRECCIÓN EJECUTIVA	CARPIO VALDIVIEZO VERONICA ELIZABETH	SECRETARIA EJECUTIVA
488	DIRECCIÓN EJECUTIVA	COLOMA PINOS ANA PATRICIA	SERVIDOR PUBLICO 7
489	DIRECCIÓN EJECUTIVA	CUATUCUAMBA YANEZ LIGIA ELENA	ASISTENTE ADMINISTRATIVO 2
490	DIRECCIÓN EJECUTIVA	DEL VALLE MEDINA KATARINA MARICEL	OFICIAL ADMINISTRATIVO 1
491	DIRECCIÓN EJECUTIVA	JARRIN AGUAS VERONICA XIMENA	SERVIDOR PUBLICO 4
492	DIRECCIÓN EJECUTIVA	LEON CADENA FRANKLIN GIOVANNY	SERVIDOR PUBLICO 5
493	DIRECCIÓN EJECUTIVA	LOPEZ CHAVEZ CARINA JOHANNA	SERVIDOR PUBLICO 3
494	DIRECCIÓN EJECUTIVA	SALAZAR GARCES NORMA EUGENIA	ASISTENTE DE PROFESIONAL
495	DIRECCIÓN EJECUTIVA	ZAMBRANO FREIRE ANDREA CAROLINA	SERVIDOR PUBLICO 1
496	DIRECCIÓN FINANCIERA	ANDRADE ORTIZ KATIA YOMAIRA	PROFESIONAL FINANCIERO 1
497	DIRECCIÓN FINANCIERA	ARAUJO ALARCON ECUADOR	AUXILIAR DE SERVICIOS
498	DIRECCIÓN FINANCIERA	ARGUERO CUEVA SOFIA GABRIELA	ASISTENTE DE GESTIÓN DE CARTERA
499	DIRECCIÓN FINANCIERA	BERRONES CEPEDA ANGEL GUSTAVO	SERVIDOR PUBLICO 6
500	DIRECCIÓN FINANCIERA	BURBANO YANEZ ROCIO DEL CARMEN	CONTADOR GENERAL
501	DIRECCIÓN FINANCIERA	CAJAMARCA VILLA CARLOS ROBERTO	ASISTENTE ADMINISTRATIVO
502	DIRECCIÓN FINANCIERA	CARRILLO ROBAYO MONICA SOFIA	SERVIDOR PUBLICO 6
503	DIRECCIÓN FINANCIERA	CHICA SANTANA PIERINA ALEXANDRA	SERVIDOR PUBLICO 2
504	DIRECCIÓN FINANCIERA	DE LOS REYES GARCES FRANCISCO RENATO	PROFESIONAL FINANCIERO 1
505	DIRECCIÓN FINANCIERA	ECHEVERRIA MOLINA TANIA DEL CARMEN	SERVIDOR PUBLICO 5
506	DIRECCIÓN FINANCIERA	FARINANGO HERMOSA DIEGO JAVIER	PROFESIONAL FINANCIERO 1
507	DIRECCIÓN FINANCIERA	GANCHALA ASITIMBAY TERESA XIMENA	ESPECIALISTA JEFE 1
508	DIRECCIÓN FINANCIERA	IBARRA PAREDES NERLY ALEXANDRA	ASISTENTE ADMINISTRATIVO 2
509	DIRECCIÓN FINANCIERA	INTRIAGO CEDEÑO LEIDY ELENA	SERVIDOR PUBLICO 2
510	DIRECCIÓN FINANCIERA	JACOME LEON VERONICA ALEXANDRA	PROFESIONAL FINANCIERO 1
511	DIRECCIÓN FINANCIERA	JARAMILLO TORRES EDGAR FERNANDO	JEFE
512	DIRECCIÓN FINANCIERA	KUNDURY QUITO OSWALDO ISRHAELL	TÉCNICO DE ADMINISTRACIÓN DE CAJA
513	DIRECCIÓN FINANCIERA	LATORRE RODRIGUEZ BERTHA MARGOTH	ASISTENTE PROFESIONAL 4
514	DIRECCIÓN FINANCIERA	LOPEZ LLERENA CARLOS ADRIANO	CONDUCTOR DE AUTOMOTOR 2
515	DIRECCIÓN FINANCIERA	MERIZALDE PROAÑO CARLOS WILSON	SUBDIRECTOR GENERAL
516	DIRECCIÓN FINANCIERA	MEZA SAMANIEGO JANNETH ELIZABETH	ANALISTA DE GESTIÓN DE CARTERA
517	DIRECCIÓN FINANCIERA	MOLINA CARRION VANESSA CAROLINA	SERVIDOR PUBLICO DE APOYO 2
518	DIRECCIÓN FINANCIERA	MOYANO ESPIN IVONNE MADELINE	ESPECIALISTA JEFE 1
519	DIRECCIÓN FINANCIERA	MUÑOZ GUERRA ANA LUCIA	CONTADOR GENERAL
520	DIRECCIÓN FINANCIERA	NARANJO PEREZ FABIOLA CECILIA	PROFESIONAL FINANCIERO 1
521	DIRECCIÓN FINANCIERA	NARVAEZ GRIJALVA NILA LUCIA	PROFESIONAL FINANCIERO 1
522	DIRECCIÓN FINANCIERA	NIETO CONSTANTE ALFREDO RAMIRO	JEFE DE DIVISION
523	DIRECCIÓN FINANCIERA	PILATASIG OJEDA GLENDA PATRICIA	ASISTENTE DE PRESUPUESTO
524	DIRECCIÓN FINANCIERA	RON ESPINOSA SILVIA GIOVANNA	JEFE DE AREA 1
525	DIRECCIÓN FINANCIERA	SANTACRUZ HEREDIA NATALY VERONICA	SERVIDOR PUBLICO 5
526	DIRECCIÓN FINANCIERA	TORRES PORRAS EDISON FERNANDO	SERVIDOR PUBLICO 6

FECHA ACTUALIZACIÓN DE LA INFORMACIÓN:	31/12/2015
PERIODICIDAD DE ACTUALIZACIÓN DE LA INFORMACIÓN:	MENSUAL
UNIDAD POSEEDORA DE LA INFORMACION - LITERAL b2):	DIRECCIÓN DE TALENTO HUMANO
RESPONSABLE DE LA UNIDAD POSEEDORA DE LA INFORMACIÓN DEL LITERAL b2):	ING. ÁNGEL SUÁREZ NARANJO
CORREO ELECTRÓNICO DEL O LA RESPONSABLE DE LA UNIDAD POSEEDORA DE LA INFORMACIÓN:	angel.suarez@arcotel.gob.ec
NÚMERO TELEFÓNICO DEL O LA RESPONSABLE DE LA UNIDAD POSEEDORA DE LA INFORMACIÓN:	(02) 294-7800 EXTENSIÓN 2420

ANEXO 2.- LISTA DE EQUIPOS QUE DISPONE LA ARCOTEL

Unidad Administrativa	Terminal	
	Marca	Modelo
COORDINACIÓN ZONAL 2	APPLE	IPHONE 4
COORDINACIÓN ZONAL 2	APPLE	IPAD 3
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 2	APPLE	IPAD 3
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 2	APPLE	IPAD 3
COORDINACIÓN ZONAL 2	APPLE	IPAD 3
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 2	APPLE	IPHONE 4
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY ACE
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 2	APPLE	IPAD 3
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 2	APPLE	IPAD 3
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 2	APPLE	IPAD 3
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 2	APPLE	IPHONE 4
COORDINACIÓN ZONAL 2	APPLE	IPHONE 4
COORDINACIÓN ZONAL 2	APPLE	IPHONE 5
COORDINACIÓN ZONAL 2	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 2	APPLE	IPHONE 5
COORDINACIÓN ZONAL 2	APPLE	IPHONE 5
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S3
COORDINACIÓN ZONAL 3	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S3
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S3
COORDINACIÓN ZONAL 3	LG	NEXUS 5
COORDINACIÓN ZONAL 3	HUAWEI	ASCEND G7
COORDINACIÓN ZONAL 3	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S3
COORDINACIÓN ZONAL 3	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 3	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S3
COORDINACIÓN ZONAL 3	APPLE	IPAD 3
COORDINACIÓN ZONAL 3	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 3	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 3	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 3	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S3
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY ACE
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S3
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S3
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 3	HUAWEI	ASCEND G7
COORDINACIÓN ZONAL 3	HUAWEI	ASCEND G7
COORDINACIÓN ZONAL 3	SAMSUNG	GALAXY S5
COORDINACIÓN ZONAL 3	APPLE	IPAD 4
COORDINACIÓN ZONAL 3	LG	NEXUS 5
COORDINACIÓN ZONAL 4	APPLE	IPHONE 4

COORDINACIÓN ZONAL 4	APPLE	IPAD 3
COORDINACIÓN ZONAL 4	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 4	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 4	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 4	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 4	APPLE	IPHONE 5
COORDINACIÓN ZONAL 4	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 4	APPLE	IPHONE 4
COORDINACIÓN ZONAL 4	APPLE	IPHONE 4
COORDINACIÓN ZONAL 4	APPLE	IPHONE 5
COORDINACIÓN ZONAL 4	SAMSUNG	GALAXY ACE
COORDINACIÓN ZONAL 4	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 4	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 4	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 5	APPLE	IPHONE 4
COORDINACIÓN ZONAL 5	APPLE	IPAD 3
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	SAMSUNG	GALAXY ACE
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	SAMSUNG	GALAXY TAB 3
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	SONY	XPERIA M4
COORDINACIÓN ZONAL 5	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	SAMSUNG	GALAXY S2
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	SAMSUNG	GALAXY S5
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 5	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 5	APPLE	IPHONE 5
COORDINACIÓN ZONAL 6	LG	NEXUS 5
COORDINACIÓN ZONAL 6	LG	NEXUS 5
COORDINACIÓN ZONAL 6	LG	NEXUS 5
COORDINACIÓN ZONAL 6	APPLE	IPHONE 5
COORDINACIÓN ZONAL 6	SAMSUNG	GALAXY TAB 3
COORDINACIÓN ZONAL 6	APPLE	IPHONE 5
COORDINACIÓN ZONAL 6	BLACKBERRY	TORCH 9810
COORDINACIÓN ZONAL 6	APPLE	IPHONE 5
COORDINACIÓN ZONAL 6	LG	NEXUS 5
COORDINACIÓN ZONAL 6	APPLE	IPHONE 5
COORDINACIÓN ZONAL 6	APPLE	IPAD 3
COORDINACIÓN ZONAL 6	LG	NEXUS 5
COORDINACIÓN ZONAL 6	BLACKBERRY	TORCH 9810
COORDINACIÓN ZONAL 6	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 6	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 6	APPLE	IPHONE 4
COORDINACIÓN ZONAL 6	LG	NEXUS 5
COORDINACIÓN ZONAL 6	LG	NEXUS 5
COORDINACIÓN ZONAL 6	APPLE	IPHONE 5
COORDINACIÓN ZONAL 6	NOKIA	LUMIA 830
COORDINACIÓN ZONAL 6	LG	NEXUS 5

COORDINACIÓN ZONAL 6	LG	NEXUS 5
COORDINACIÓN ZONAL 6	SAMSUNG	GALAXY S4
COORDINACIÓN ZONAL 6	APPLE	IPHONE 5
COORDINACIÓN ZONAL 6	SAMSUNG	GALAXY S4
OFICINA TÉCNICA GALÁPAGOS	APPLE	IPHONE 4
OFICINA TÉCNICA GALÁPAGOS	APPLE	IPAD 3
OFICINA TÉCNICA GALÁPAGOS	BLACKBERRY	TORCH 9810
OFICINA TÉCNICA GALÁPAGOS	BLACKBERRY	TORCH 9810
OFICINA TÉCNICA GALÁPAGOS	SAMSUNG	GALAXY ACE
OFICINA TÉCNICA GALÁPAGOS	SAMSUNG	GALAXY S2
OFICINA TÉCNICA GALÁPAGOS	SAMSUNG	GALAXY S2
OFICINA TÉCNICA GALÁPAGOS	SAMSUNG	GALAXY S4
OFICINA TÉCNICA GALÁPAGOS	SAMSUNG	GALAXY S2
OFICINA TÉCNICA GALÁPAGOS	BLACKBERRY	TORCH 9810
DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	APPLE	IPAD 3
DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	SAMSUNG	GALAXY S4
DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	SAMSUNG	GALAXY S3
DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	SONY	XPERIA M4
DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	APPLE	IPHONE 4
DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	SAMSUNG	GALAXY S4
DIRECCIÓN DE INVESTIGACIÓN ESPECIAL	SAMSUNG	GALAXY S4
DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA	SAMSUNG	GALAXY S4
DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA	SAMSUNG	GALAXY ACE
DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA	SAMSUNG	GALAXY S4
DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA	SONY	XPERIA M4
DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA	SONY	XPERIA M4
DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA	APPLE	IPAD 3
SATIX - DIE	SAMSUNG	GALAXY S3
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SAMSUNG	GALAXY S3
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
SATIX - DIE	SONY	XPERIA M4
Despacho	APPLE	IPHONE 5
Coordinación Técnica	APPLE	IPHONE 5
Coordinación Técnica	APPLE	IPAD 3
Coordinación Financiera Administrativa	APPLE	IPHONE 5
Despacho	APPLE	IPAD 3
Coordinación Técnica	APPLE	IPAD 3
Dirección Certificación Equipos	APPLE	IPAD 3

Dirección Control Espectro	APPLE	IPAD 3
Dirección Control Servicios	APPLE	IPAD 3
Dirección Control Servicios	APPLE	IPHONE 4
Dirección Control Servicios	BLACKBERRY	TORCH 9810
Dirección Control Servicios	SONY	XPERIA M4
Dirección Jurídica Espectro	APPLE	IPHONE 4
Dirección Jurídica Espectro	APPLE	IPHONE 5
Dirección Control Servicios	APPLE	IPHONE 4
Coordinación Técnica	HUAWEI	ASCEND G7
Dirección Administrativa	APPLE	IPHONE 5
Dirección Certificación Equipos	APPLE	IPHONE 4
Coordinación Técnica	APPLE	IPHONE 4
Intendencia Jurídica	SAMSUNG	GALAXY ACE
Auditoría Interna	BLACKBERRY	TORCH 9810
Dirección Control Servicios	APPLE	IPHONE 5
Dirección Jurídica de Telecomunicaciones	APPLE	IPHONE 5
Dirección Talento Humano	APPLE	IPHONE 4
Dirección Imagen y Comunic.	APPLE	IPHONE 4
Asesoría	APPLE	IPHONE 4
Dirección Planificación	APPLE	IPHONE 4
Dirección Control Servicios	APPLE	IPHONE 4
Coordinación Técnica	APPLE	IPHONE 4
Dirección Control Espectro	LG	NEXUS 5
Dirección Control Servicios	APPLE	IPHONE 5
CUSTODIA DST	SAMSUNG	S4 MINI
Dirección Control Servicios	APPLE	IPAD 3
Dirección Planificación	APPLE	IPAD 3
Dirección Control Servicios	APPLE	IPAD 3
Dirección Atención al Usuario	HUAWEI	ASCEND G7
Procuraduría General (IJE)	APPLE	IPHONE 4
Intendencia Jurídica	APPLE	IPHONE 4
Dirección Imagen y Comunic.	SAMSUNG	GALAXY S4
Dirección Control Espectro	SAMSUNG	GALAXY S4
Dirección Atención al Usuario	APPLE	IPHONE 5
Asesoría	APPLE	IPAD 3
Dirección Administrativa	APPLE	IPAD 3
Coordinación Financiera Administrativa	APPLE	IPAD 3
Dirección Imagen y Comunic.	APPLE	IPAD 3
Dirección Atención al Usuario	HUAWEI	ASCEND G7
Dirección Atención al Usuario	HUAWEI	ASCEND G7

ANEXO 3.- OFERTAS PRESENTADAS

TAURUSTECH CIA LTDA

RUC: 0190364143001
AV. ORDOÑEZ LASSO S/N Y BUGAMBILLAS. EDIFICIO. SANTA CECILIA
Telf.:+593 (07) 4102962 / 4102797 / 4048545
info@taurustech.ec
Cuenca - Ecuador

PROPUESTA VENTA
N° VENTA204

Cliente: AGENCIA DE REGULACION Y CONTROL DE LAS TELECOMUNICACIONES
Provincia: PICHINCHA Cantón: QUITO
R.U.C/C.I.: 1768181900001

Fecha emisión: CUENCA, 2016-04-13
Contacto: Jorge Vallejo

DESCRIPCIÓN	CANTIDAD	PRECIO UNIT.	TOTAL
EMM Gold Subscription License with Assurance Support Per Device Cloud	526	83.82	44089.32

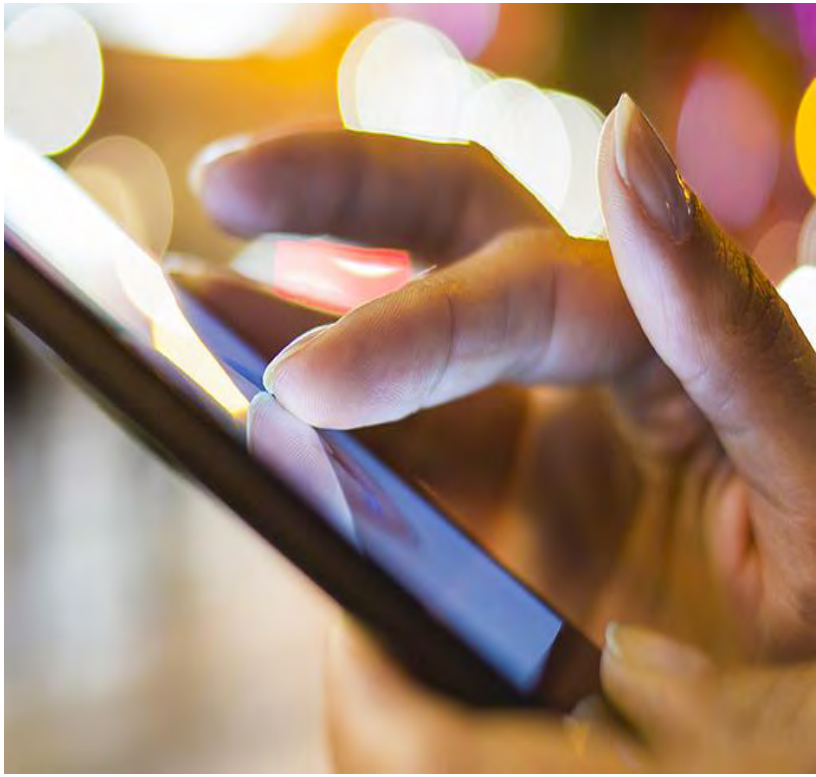
Información adicional:
Forma de Pago: -anticipo del 70% y 30% contraentrega
Tiempo de Entrega: 7 Dias
Validez de la oferta: 15 Dias
Garantía: 12 meses

SUBTOTAL $	44089.32
IVA $	5290.72
TOTAL $	**49380.04**

_____
Verónica Ronquillo Ordóñez.
TAURUSTECH

_____
Autorizado

MobileIron Architecture

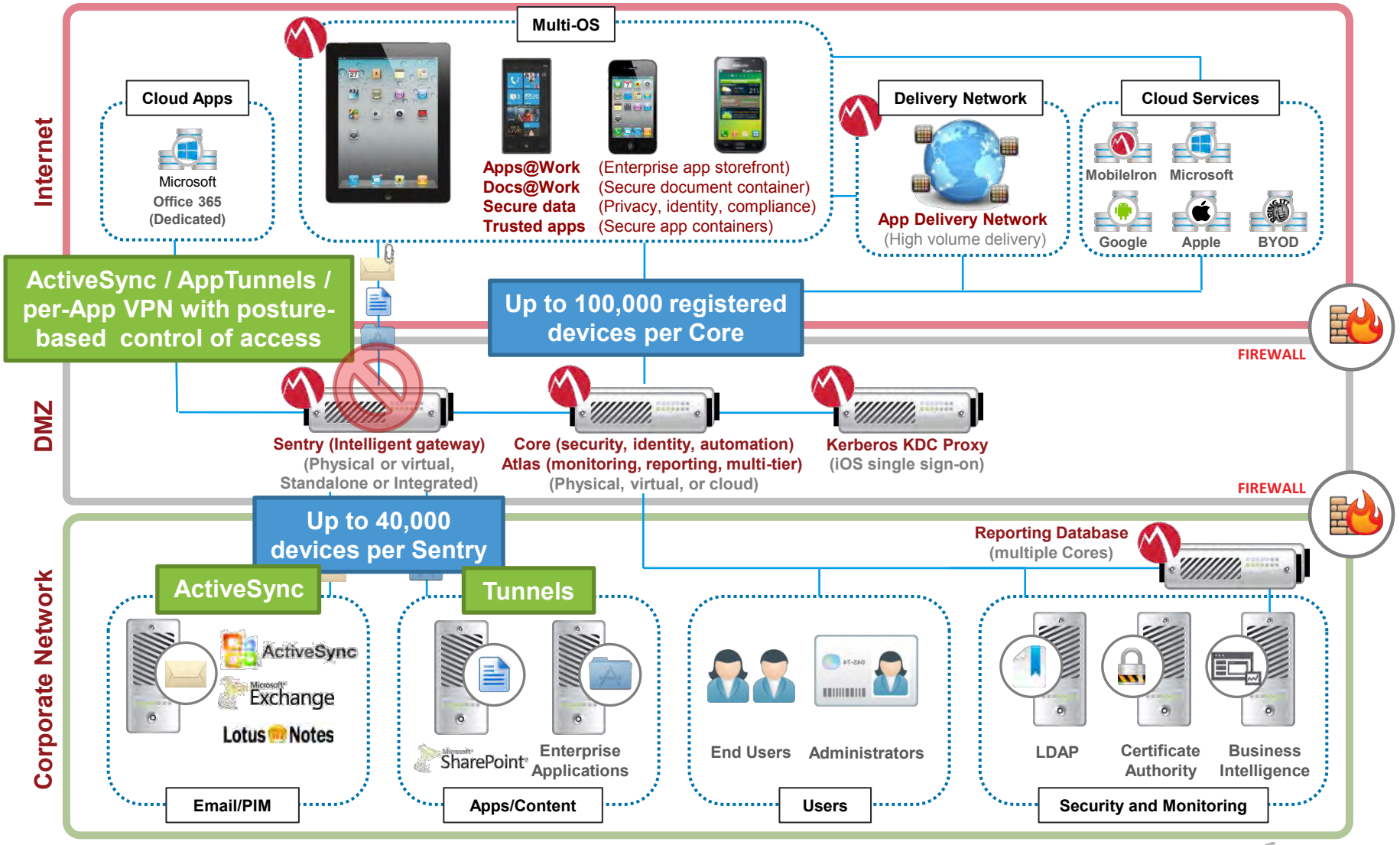


MobileIron Architecture Review

MobileIron University

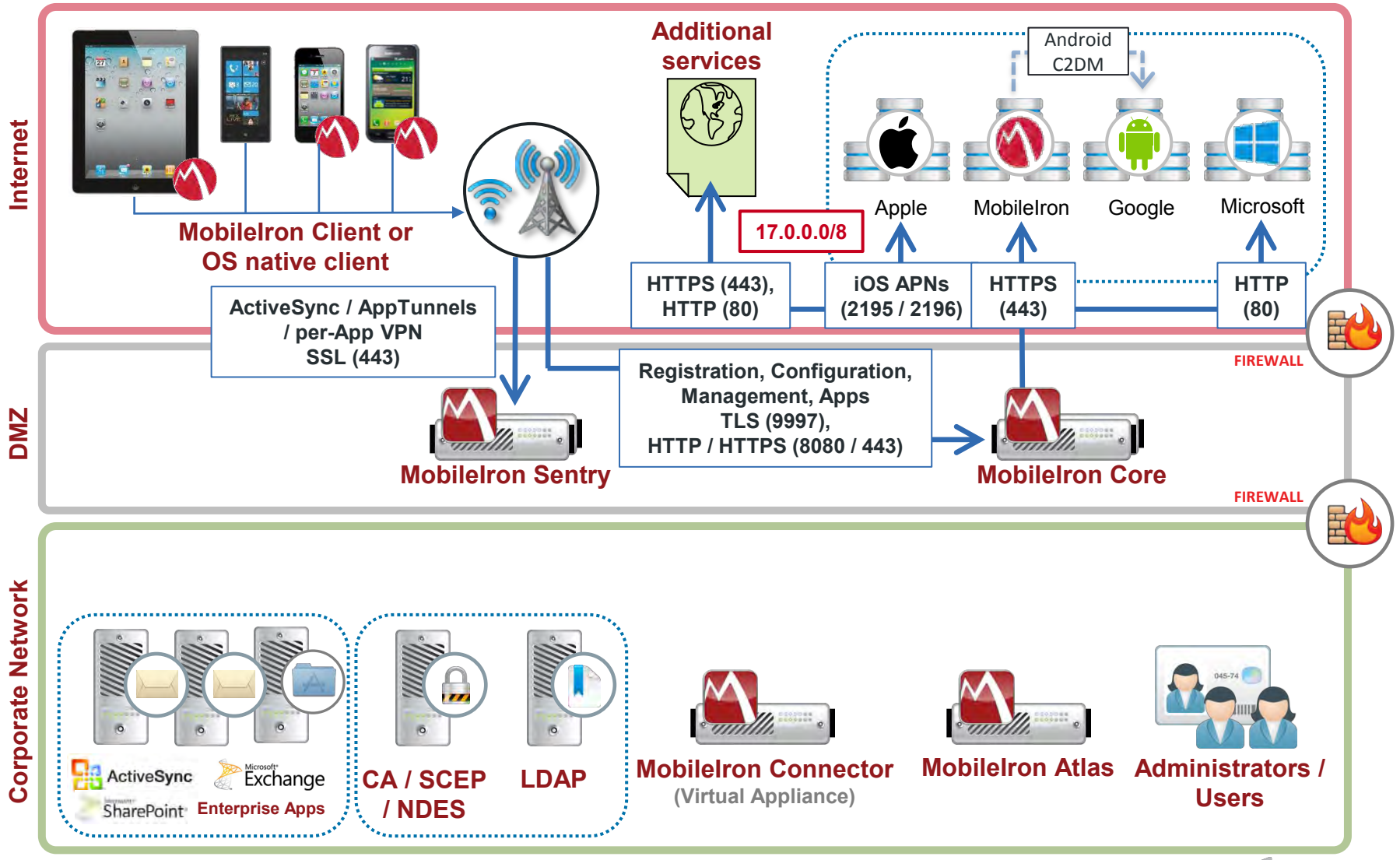
MobileIron Core Architecture

MobileIron Architecture Overview



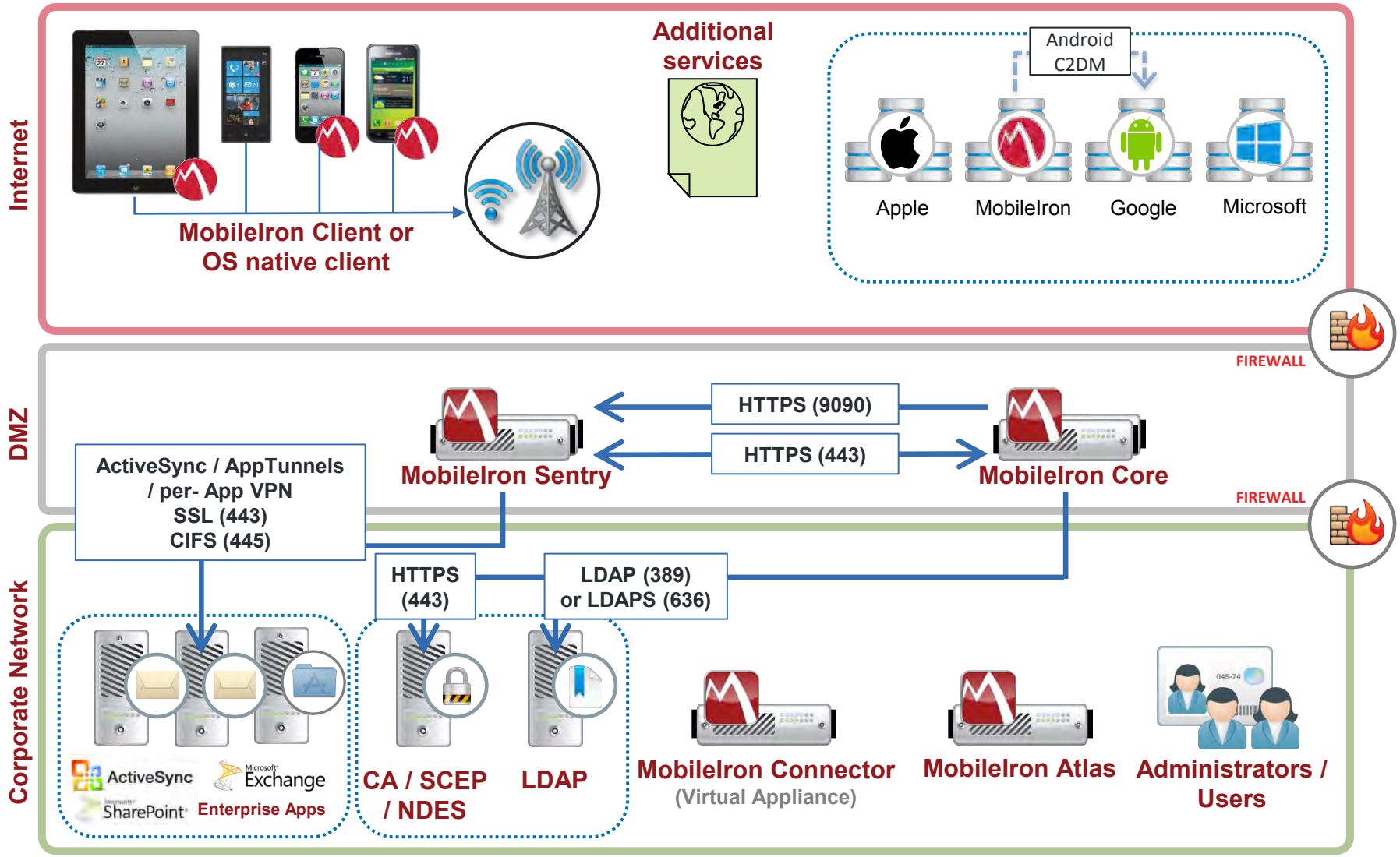
Note: *MobileIron Core, Sentry, and Atlas can be deployed behind the corporate firewall if desired*

Traffic at the Outside Firewall

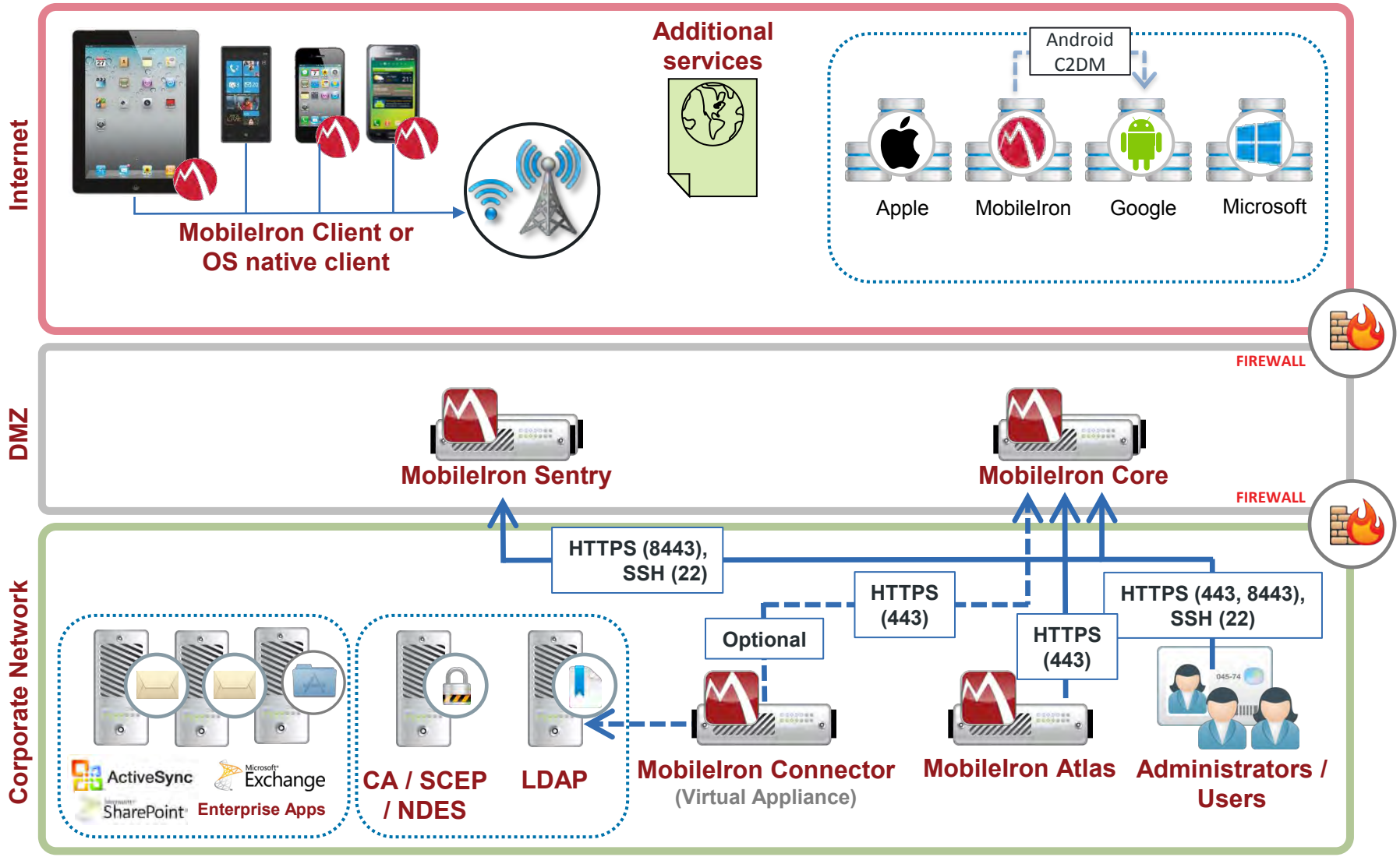


MobileIron University

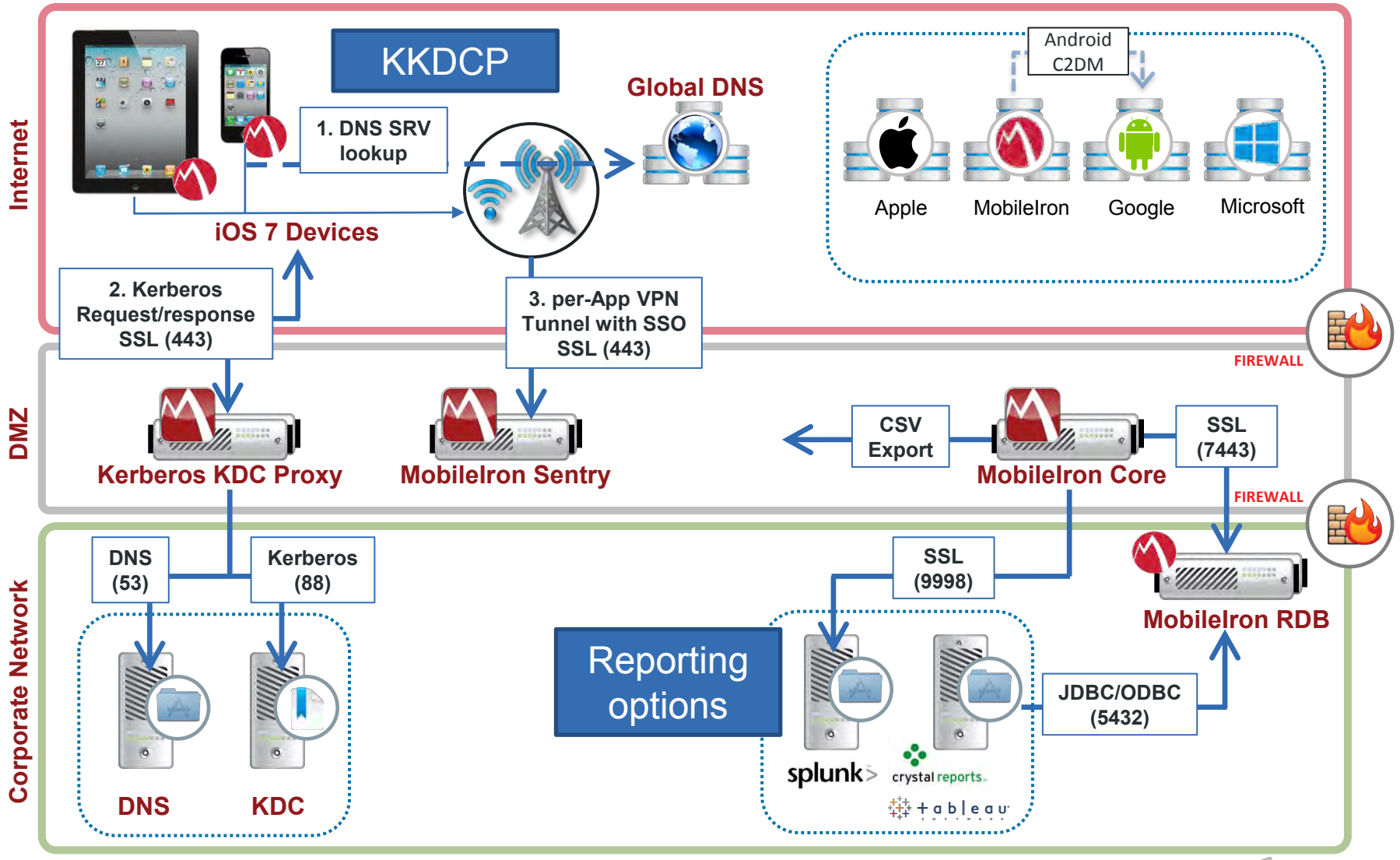
Traffic at the Inside Firewall – Inbound



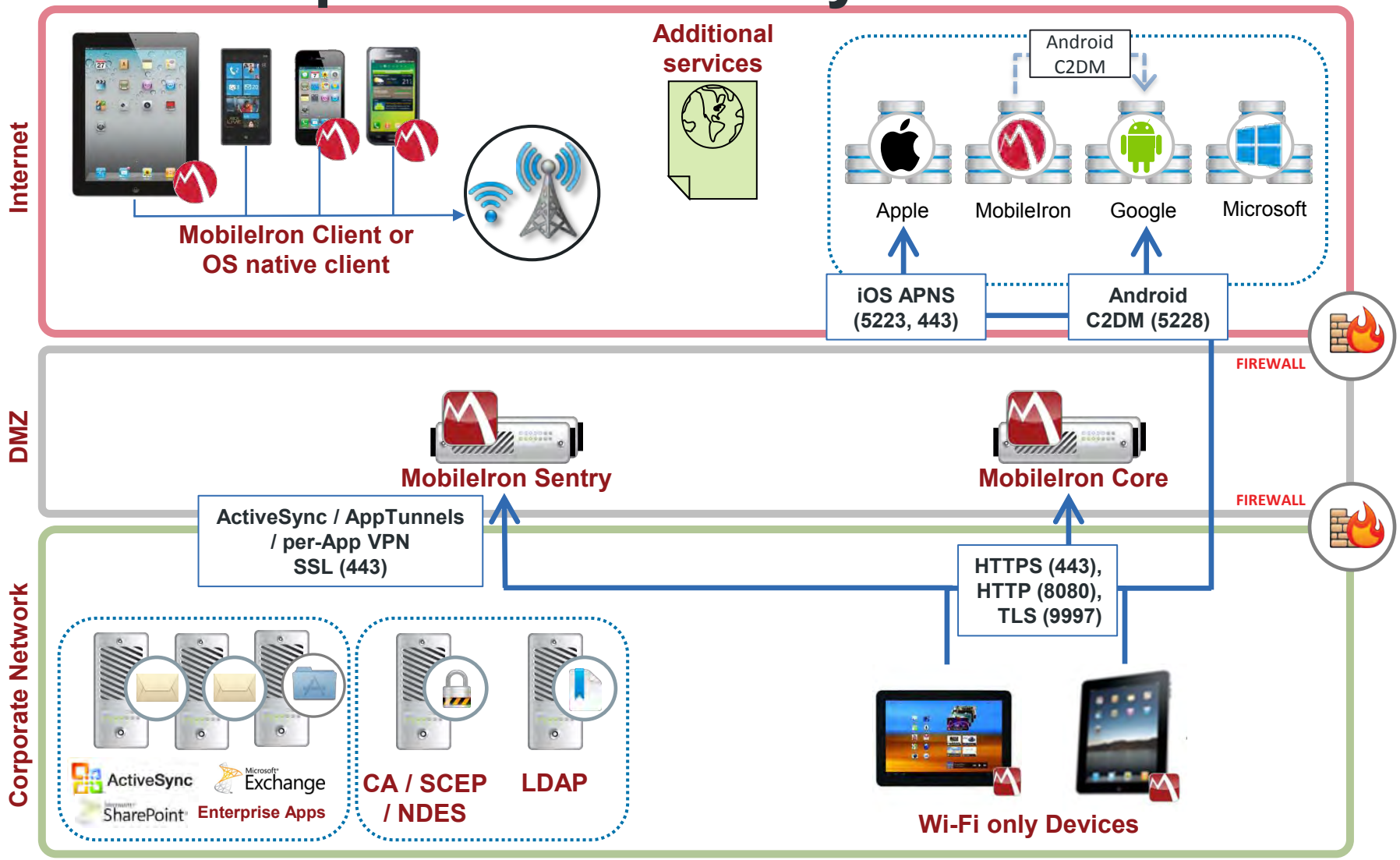
Traffic at the Inside Firewall – Outbound



Architectural Extensions

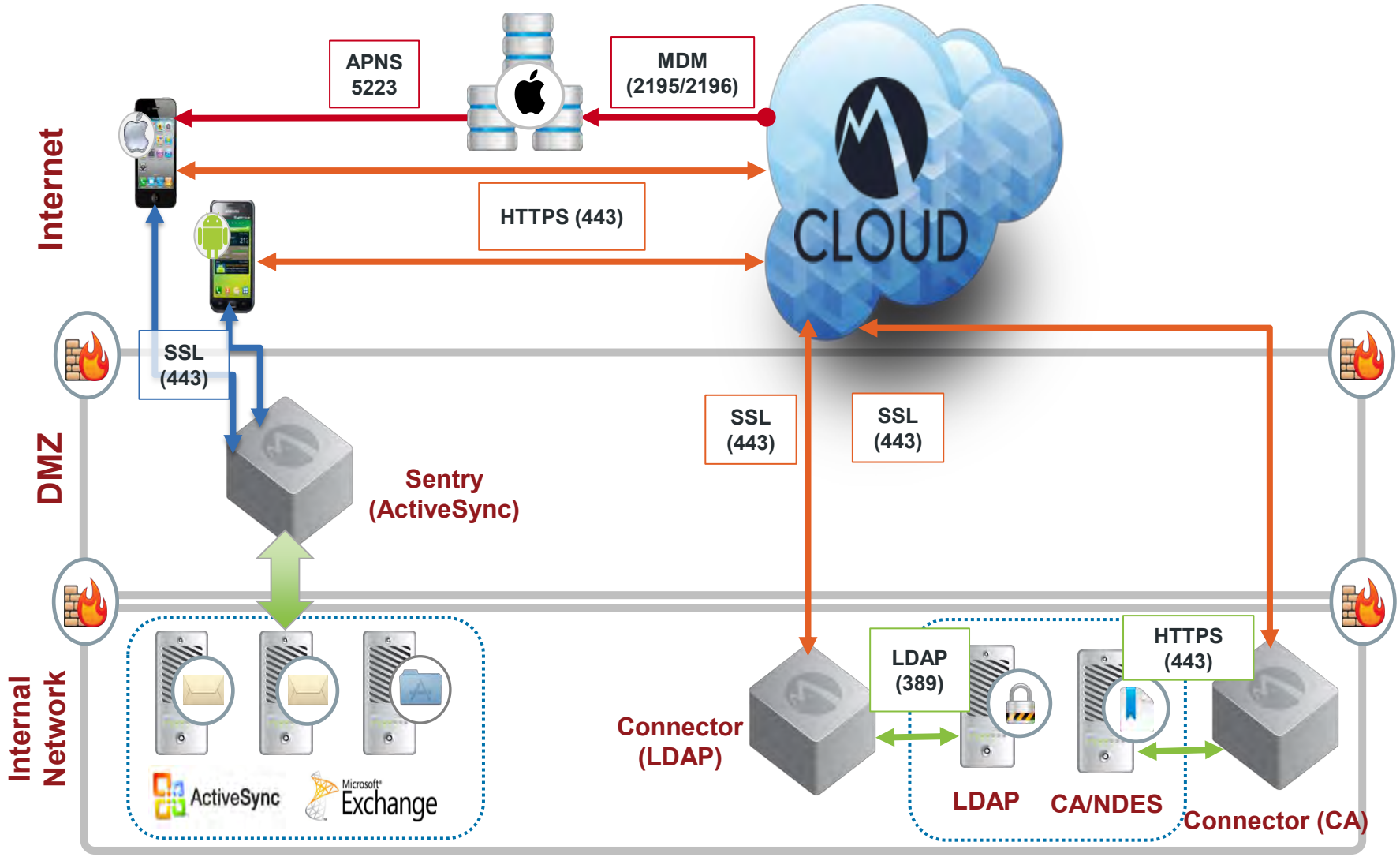


Ports: Corporate Wi-Fi Only Devices

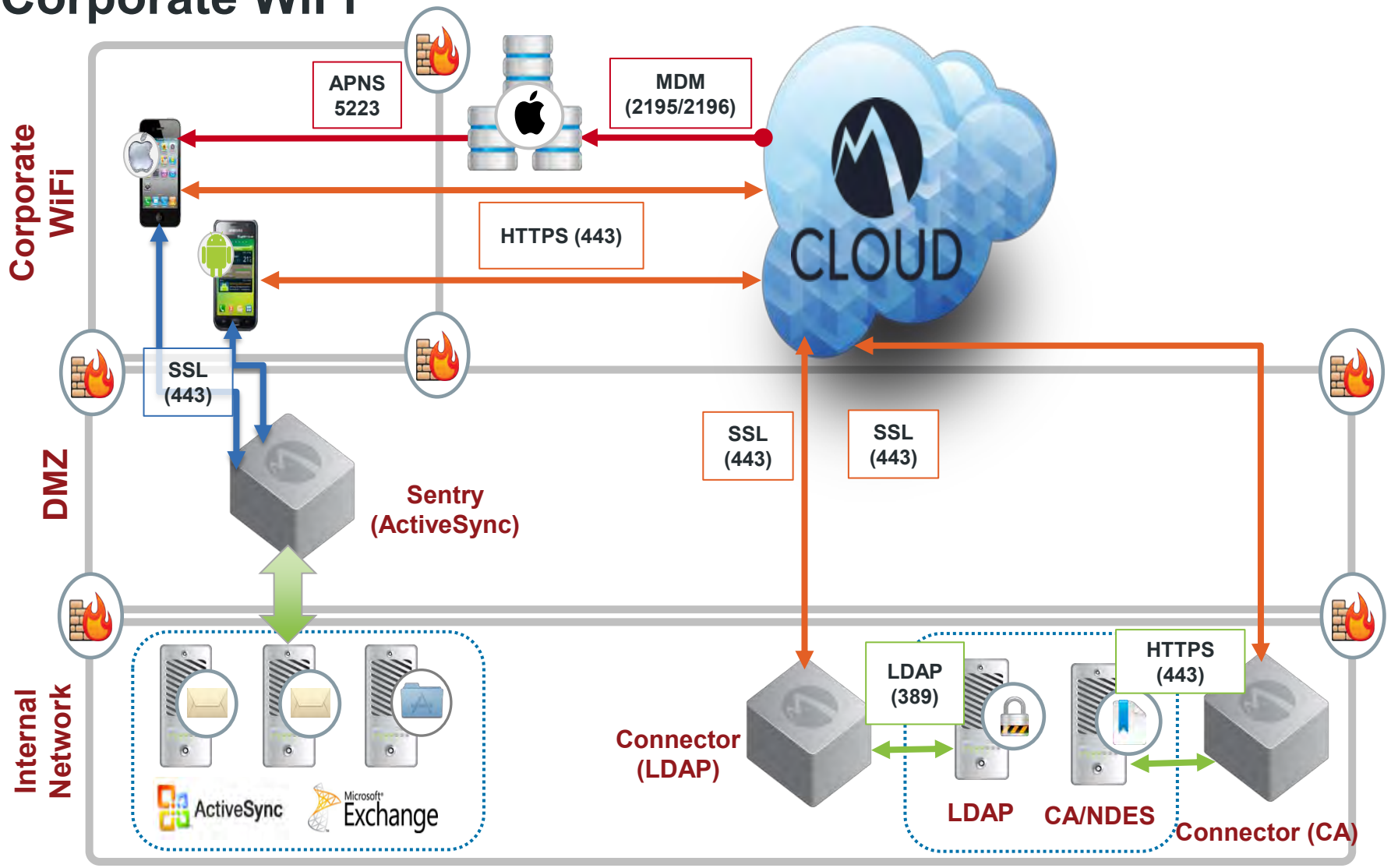


MobileIron Cloud Architecture

MobileIron Cloud Enterprise Architecture: Ports

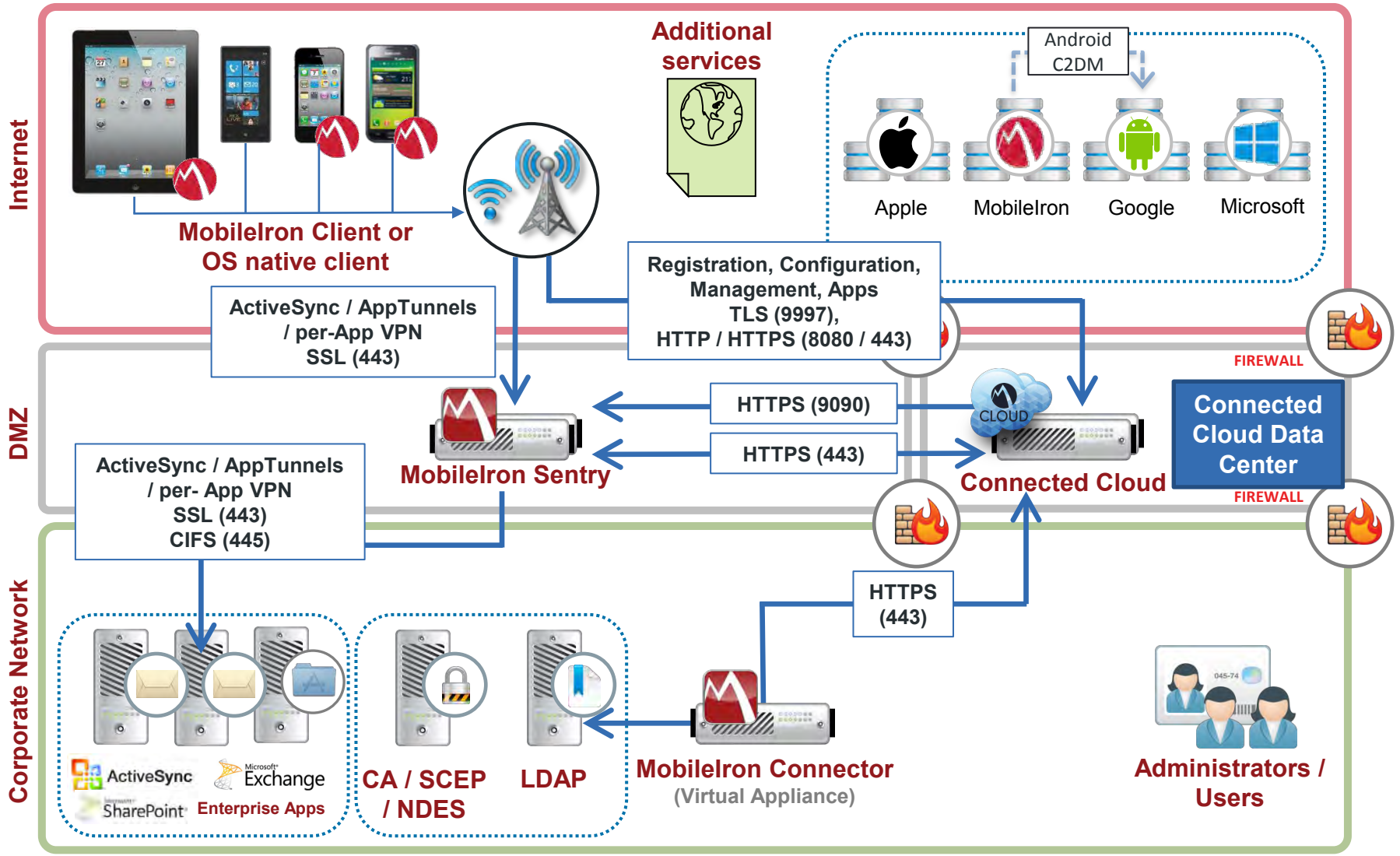


MobileIron Cloud Enterprise Architecture: Ports Corporate WiFi



MobileIron Connected Cloud

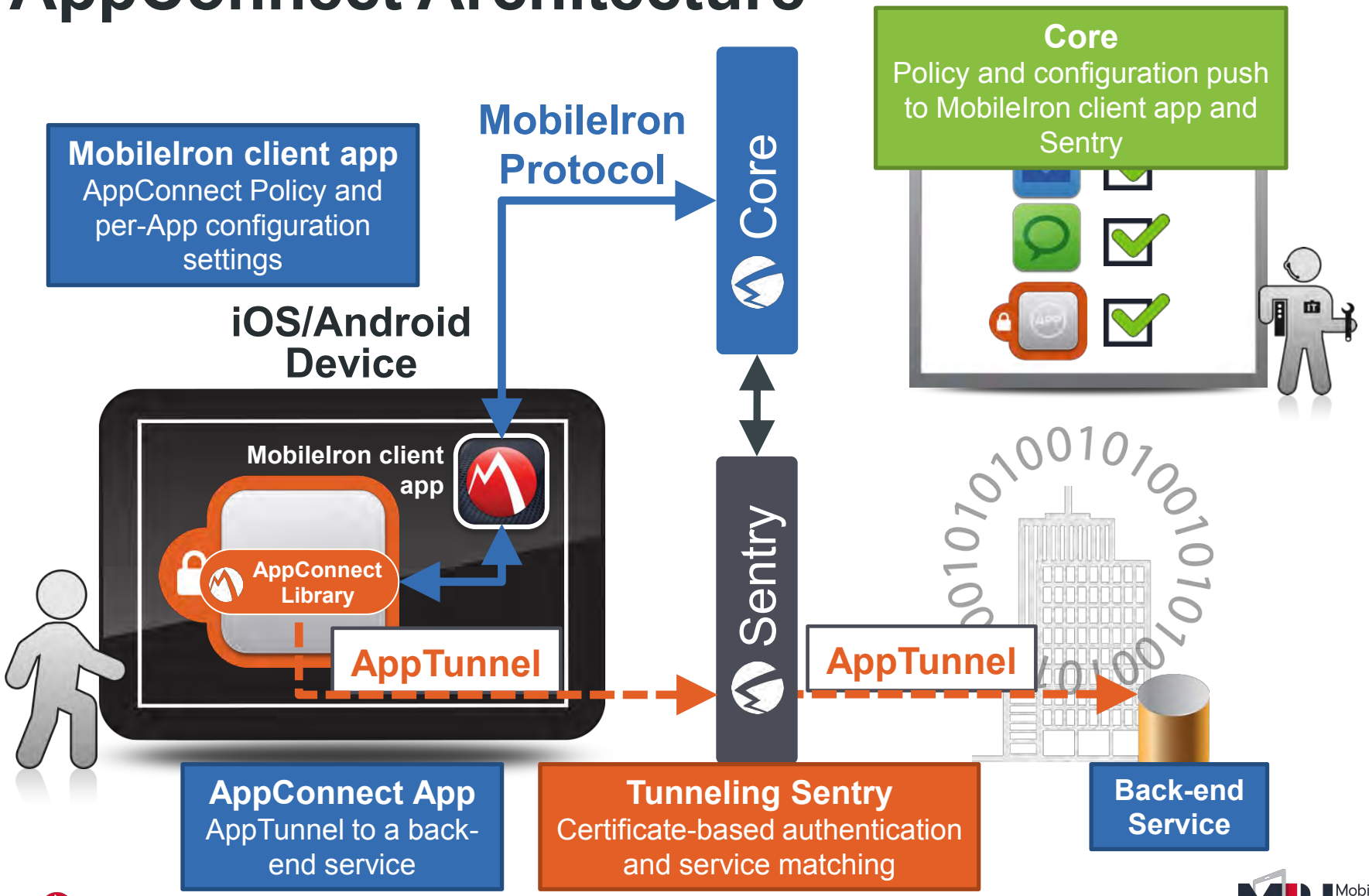
MobileIron Connected Cloud



MobileIron University

AppConnect

AppConnect Architecture



MobileIron® University

Ficha técnica - MobileIron

MobileIron

MobileIron es la plataforma móvil de tecnologías de la información (TI) especialmente diseñada para que las empresas puedan asegurar y administrar aplicaciones móviles, contenido y dispositivos, a la vez que permite a sus empleados elegir sus dispositivos, mantener la privacidad y disfrutar de una experiencia de usuario nativa.

El nuevo modelo se seguridad para empresas

Los empleados cada vez optan más por utilizar para su trabajo dispositivos móviles que cuentan con modernos sistemas operativos como Android, iOS y Windows 10, en lugar de hacerlo en equipos tradicionales y herramientas basadas en Windows. Actualmente, los datos de las empresas se alojan en aplicaciones tanto corporativas como del consumidor, así como en repositorios de almacenamiento en la nube. El reto en el ámbito de la seguridad con la tecnología móvil es muy diferente al de la era de los antiguos PC, y requiere un nuevo enfoque. Los sistemas operativos modernos solucionan muchos de los anteriores problemas de seguridad, pero generan al mismo tiempo nuevos y complejos requisitos.

Android, iOS y, ahora, Windows 10, tienen una arquitectura aislada que separa los datos a nivel de la aplicación y protege tanto el sistema de archivos como el sistema operativo de accesos no autorizados. El sistema de archivos protegidos y el núcleo protegido eliminan la amenaza del malware tradicional y la necesidad de virtualización, VPN y otras tecnologías heredadas. Sólo la administración de movilidad en el segmento empresarial ("enterprise mobility management", EMM) ofrece seguridad para las aplicaciones y datos en estos modernos sistemas operativos. Con MobileIron, las empresas disponen de un completo conjunto de funciones que mejoran la seguridad de los datos.

La plataforma MobileIron

La plataforma MobileIron se creó para asegurar y administrar sistemas operativos modernos en un mundo de dispositivos con diferentes usos. Incorpora la obligatoriedad de identidad, contexto y privacidad con el fin de establecer el nivel adecuado de acceso a los datos y servicios corporativos. MobileIron asegura los datos en reposo en el dispositivo, en las aplicaciones y el almacenamiento de la nube, además de proteger los datos en movimiento mientras se transfieren entre la red corporativa, los dispositivos y el almacenamiento en la nube. Con MobileIron, el área de informática puede asegurar la información corporativa esté donde esté, a la vez que mantiene la privacidad del empleado.

La plataforma MobileIron

La plataforma MobileIron está formada por tres componentes de software integrados y distribuidos:

MobileIron Core: un motor de políticas que permite al departamento informático definir la seguridad y las políticas de administración.

MobileIron Client: el software en el dispositivo que garantiza el cumplimiento de dichas políticas en el mismo dispositivo.

MobileIron Sentry: una puerta de enlace inteligente que asegura los datos a medida que se desplazan entre aplicaciones, dispositivos y la red corporativa.

Clientes

MobileIron ha vendido sus soluciones a más de 10 000 clientes en todo el mundo. La empresa sigue recibiendo una gran demanda de su servicio MobileIron Cloud, que fue elegido por una de las 10 mejores empresas de la lista Forbes Global 2000.

Estudios de casos recientes de clientes

Dürr: empresa de ingeniería mecánica alemana que asegura la propiedad intelectual a la vez que fomenta la productividad con miles de dispositivos Windows Phone.

Denso: este fabricante japonés de piezas de automóvil agiliza la toma de decisiones mediante un programa seguro BYOD (uso de dispositivos personales en el trabajo).

GAC-Toyota Motor: el fabricante de los conocidos automóviles Toyota permite una mejor experiencia a sus clientes al ofrecer iPads seguros en sus concesionarios.

Standard Life: esta compañía, líder en inversión, permite que sus 2000 empleados móviles accedan a documentos y archivos corporativos desde cualquier lugar.

Thomson Snell & Passmore: el despacho de abogados más antiguo del mundo permite que sus empleados trabajen desde cualquier lugar, al sustituir los dispositivos BlackBerry por iPhones y asegurar las aplicaciones personalizadas.

Ecosistema

Al finalizar el tercer trimestre, contábamos con 84 aplicaciones habilitadas para AppConnect y 58 integraciones de ServiceConnect disponibles. Se incluye aquí la integración mejorada con Splunk para proporcionar visualizaciones que se pueden utilizar en programas de cumplimiento de Payment Card Industry (PCI), Criminal Justice Information Services (CJIS) y Sarbanes-Oxley (SOX). Además, nuestros clientes han hecho uso de nuestro contenedor AppConnect para asegurar miles de aplicaciones desarrolladas internamente.

Canal

MobileIron penetra en el mercado principalmente a través de una sólida red global de socios del canal, formada por más de 500 distribuidores especializados en tecnología móvil y 40 proveedores de servicios globales.

MobileIron, Inc. Sede central:

415 East Middlefield Road
Mountain View, CA 94043, EE. UU.
650-919-8100

www.mobileiron.com

Oficinas regionales de MobileIron:

China	Italia	Singapur
Francia	Japón	Suecia
Alemania	Corea	Emiratos Árabes Unidos
Hong Kong	Holanda	Reino Unido
India	Polonia	

Historia de la empresa

Fundada en: 2007
Fundadores: Ajay Mishra y Suresh Batchu

Inversores

MobileIron cotiza en la bolsa de valores de NASDAQ

Símbolo de acciones: MOBL

Encontrará más información disponible en
investors.mobileiron.com

Datos financieros destacables del 3er trimestre de 2015:

Los ingresos brutos ascendieron a $41,1 millones, un 7 % más interanual

Los ingresos recurrentes fueron de $27,3 millones, un 35 % más interanual, y representaron el 66 % de los ingresos brutos

Los ingresos NIF fueron de $38,0 millones, un 9 % más interanual

Los ingresos ajenos a las NIF fueron de $37,7 millones, un 12 % más interanual

Los ingresos recurrentes ascendieron a $23,3 millones, un 45 % más interanual

Las pérdidas netas NIF por acción fueron de $0,30; mientras que las pérdidas netas por acción ajenas a las NIF fueron de $0,17

Ejecutivos

Bob Tinker, Presidente y director Ejecutivo

Simon Biddiscombe, Director Ejecutivo

Suresh Batchu, Cofundador, CTO y SVP de Tecnología e Ingeniería

Ajay Mishra, Cofundador y director de Servicios al Cliente

Damian Artt, Vicepresidente senior de Ventas Internacionales

Jared Lucas, Director de Recursos Humanos

Mike McCarron, Vicepresidente de Éxito del Cliente

Laurel Finch, Vicepresidenta y Asesora General

Jeff Ratzlaff, Vicepresidente de Desarrollo Empresarial

Ojas Rege, Vicepresidente de Estrategia

Vittorio Viarengo, Vicepresidente de Marketing y Productos

Empleados:

Más de 850

Logros:

Fundada en: 2007

Primer cliente: 2009

Primera patente concedida: 2011

Primer acuerdo con proveedores de servicios: 2010

Más 100 millones de dólares en ingresos
(56 % de Norteamérica y 44 % del resto del mundo): 2013

IPO: 2014

Distinciones y reconocimientos

A MobileIron le han sido concedidas 22 patentes hasta el momento

Gartner ha otorgado a MobileIron el reconocimiento de"Líder" durante cinco años consecutivos[1] en la clasificación de Magic Quadrant for Enterprise Mobility Management Suites (anteriormente denominada Magic Quadrant for Mobile Device Management Software).

Reconocida como "la empresa de tecnología de crecimiento más rápido del mundo" en la lista Technology Fast 500 de Deloitte en 2014.

Puesto 14 en la lista de "Las mejores empresas para trabajar" de los premios Employee Choice Awards de Glassdoor en 2015.

[1]Gartner, "Magic Quadrant for Enterprise Mobility Management Suites" de Terrence Cosgrove, Rob Smith, Chris Silva, John Girard, Bryan Taylor, 8 de junio de 2015.

MobileIron


MobileIron®

Propuesta Técnica y Económica

Fecha:	**08/03/2016**
Oferta Nro.:	002
Producto:	Kaspersky Mobile Device Management (MDM)
Cliente:	Agencia de Regulación y Control de las Telecomunicaciones (Arcotel)
Contacto:	Jorge Ramiro Vallejo Basantes
Ciudad:	Quito – Ecuador.

1. Sobre INFORC ECUADOR®

INFORC ECUADOR® es una empresa ecuatoriana fundada en el año 2005, con experiencia en proveer servicios y productos para la seguridad de la información, consultoría, gestión de procesos, riesgos tecnológicos y auditorias de seguridad, soportados por la experiencia de nuestros especialistas y consultores, desde hace 10 años estamos colaborando con la seguridad de la información de empresas públicas y privadas del Ecuador.

Nuestra gestión se apoya en dos premisas básicas: Búsqueda permanente de la satisfacción del Cliente y Excelencia en la provisión de productos y prestación de servicios.

Nuestro personal, en su mayoría ingenieros y técnicos, fue seleccionado teniendo en cuenta una sólida formación en telecomunicaciones e informática y una marcada vocación de servicio. De esta manera aseguramos a nuestros clientes la comprensión de sus necesidades tecnológicas y una atención dedicada y profesional.

Quienes formamos parte de INFORC ECUADOR, basados en el Sistema de la Gestión de la Calidad (*en proceso de implantación de ISO 9001:2008*) nos comprometemos a:

- Cumplir los requisitos acordados con nuestros Clientes.
- Actualizarnos permanentemente investigando nuevas tecnologías.
- Perfeccionarnos en las técnicas que aplicamos.
- Asociarnos a proveedores responsables, calificados, e innovadores.
- Lograr la más alta satisfacción de nuestros Clientes.

Apoyándonos en el mejoramiento continuo y en la eficacia de esta política, pretendemos alcanzar la excelencia de nuestros productos y servicios.

Esperamos que esta propuesta sea de su conveniencia y quedamos a su disposición para atender cualquier inquietud o comentario que pudiera surgir respecto a la misma.

Atentamente

Carlos Jumbo G.
IT Manager
INFORC ECUADOR
cjumbo@inforc.ec
Teléfonos:(593 -2) 2559067 - 2227766 – 2902045 Ext: 110
Celular: (593) 995834805
www.inforc.ec

2. Sobre Kaspersky Lab

Kaspersky Lab es una de las compañías de TI que más rápido crece en todo el mundo. En la actualidad, está firmemente posicionada como uno de los cuatro principales proveedores de software de seguridad para endpoints. Kaspersky Lab sigue incrementando su posición en el mercado, demostrando un crecimiento significativo en todas las regiones. Según los resultados financieros de la compañía correspondientes a 2013, los ingresos globales de Kaskpersky Lab crecieron un 18% con respecto al año anterior y superaron los 667 millones de dólares.

Productos corporativos
En 1999, Kaspersky Lab fue la primera compañía en introducir software antivirus integrado para estaciones de trabajo, servidores de archivos y servidores de aplicaciones que se ejecutan en sistemas operativos Linux/FreeBSD. En la actualidad, la compañía ofrece una completa gama de eficaces soluciones de seguridad corporativa para los sistemas operativos más populares específicamente diseñados para distintos tipos de empresas. La línea de productos de la compañía cubre la totalidad de los principales requisitos de seguridad de información a los que las empresas y grandes organizaciones estatales deben adherir, como excelentes niveles de protección, adaptabilidad a circunstancias cambiantes, escalabilidad, compatibilidad con diferentes plataformas, alto rendimiento, alta tolerancia a fallos, facilidad de uso y alto valor.

Una de las principales ventajas de la línea corporativa de Kaspersky Lab es la administración sencilla y centralizada suministrada por Kaspersky Security Center, que se extiende a toda la red, independientemente del número y tipo de plataformas usadas.

Kaspersky Endpoint Security for Business es una plataforma que ofrece una amplia variedad de herramientas y tecnologías para permitir que las compañías vean, controlen y protejan todos los dispositivos de endpoint. Combina sus tecnologías y herramientas en cuatro niveles, cada uno de los cuales agrega su propia capa de protección contra amenazas cibernéticas. El primer nivel, Core, contiene premiadas tecnologías antimalware. Luego vienen los niveles Select y Advanced, que ofrecen un moderno control y cifrado de endpoints. Por último, el nivel Total proporciona la mejor protección para cada área de la red, es decir, en los servidores de Internet, correo y colaboración por igual.
En cada nivel, Kaspersky Security Network ofrece a cada componente una potente protección asistida en la nube, y las herramientas de **Kaspersky Security Center** ayudan a los especialistas de TI a administrar la totalidad de las defensas de la compañía desde una única consola.

Kaspersky Endpoint Security for Business también presenta soluciones específicas que se pueden agregar a cada nivel:

- ✓ Kaspersky Security for File Servers
- ✓ **Kaspersky Security for Mobile**
- ✓ Kaspersky Systems Management
- ✓ Kaspersky Security for Virtualization
- ✓ Kaspersky Security for Storage
- ✓ Kaspersky Security for Mail
- ✓ Kaspersky Security for Internet Gateway

3. Propuesta Económica

Opción 1 – Kaspersky Mobile Device Management (MDM)

Item	Descripción	Precio Unit.	Precio Total.
526	Licencias Kaspersky Mobile Device Management (MDM).	$19.25	$10125.50
	Precio total por 1 AÑO	$19.25	$10125.50
	Precio total por 2 AÑOS	$27.90	$14675.40
	Precio total por 3 AÑOS	$35.50	$18673.00

Opción 2 - Kaspersky Mobile Device Management (MDM)

Item	Descripción	Precio Unit.	Precio Total.
223	Licencias Kaspersky Mobile Device Management (MDM).	$24.70	$5508.10
	Precio total por 1 AÑO	$24.70	$5508.10
	Precio total por 2 AÑOS	$35.50	$7916.50
	Precio total por 3 AÑOS	$46.25	$10313.75

INCLUYE:

Item	Descripción
1	▪ Licenciamiento contratado (526 o 223 dispositivos) por 12, 24 o 36 meses. ▪ Configuración, Implementación y **Capacitación** de todas las funciones de la solución MDM, entre las cuales destacan: o Protección a varios niveles. o Bloqueo de campañas de phishing y spam. o Control del uso de Internet. o Detección de liberación de dispositivos. o Protección de datos en móviles desaparecidos. o Gestión de aplicaciones móviles (MAM). o Separación de las aplicaciones y los datos corporativos y personales. o Protección de las aplicaciones y los datos almacenados en los contenedores. o Prevención del acceso a las aplicaciones y los datos por parte de antiguos empleados. o Control de aplicaciones. o Safe Browser. o Compatibilidad de MDM con diferentes plataformas. o Gestión inalámbrica de seguridad. o Gestión centralizada. o Control a través de un único panel centralizado. o Ayuda para que los usuarios sean autosuficientes. o División de responsabilidades entre los administradores. o Activación de la gestión remota. ▪ Recursos técnicos para realizar la instalación en sitio del software

	antivirus en el sitio. • Tiempos de respuesta frente a eventos infecciosos no mayor a 2 horas, incluso menor, de acuerdo a la criticidad del evento reportado. • Visitas semestrales para revisión de seguridad. Incluye también la entrega de la siguiente documentación: • Manuales de instalación y configuración. • Claves/Códigos de licenciamiento del software. • Certificado de licenciamiento Kaspersky.

Observaciones generales:

- Precios no incluye el 12% del IVA.
- Tiempo de entrega e implementación: **10 días**.
- Aquellos conceptos no descritos explícitamente no están incluidos en la oferta.
- **Forma de pago: Efectivo, depósito o transferencia en ventas hasta $200 (doscientos dólares) o de acuerdo al Registro RA-07.**
- Validez de la oferta: **30 días.**
- **Jornadas de Awareness (concienciación) a usuarios finales sobre seguridad de la información.**

4. Otros Productos

4.1. Servicios

- **Pruebas Avanzadas de Penetración y Explotación Táctica de Sistemas (Ethical Hacking).**
  - ✓ Análisis de Vulnerabilidades.
  - ✓ Test de penetración.
    - Test de Penetración de Aplicaciones Web
    - Test de Penetración de Infraestructura
  - ✓ Ingeniería Social
- **Planes de Concientización.**
- **Continuidad del Negocio BCP / DRP.**
- **Consultoría y capacitación sobre ISO 27001:2013.**
- **Implementación de SGSI ISO 27001:2013 y EGSI (Esquema Gubernamental de Seguridad de la Información).**
  - Definición del alcance
  - Análisis GAP
  - Gestión de Riesgos - ISO 27005:2008
  - Documento de Aplicabilidad (SOA)
  - Implementación de Controles de seguridad
  - ✓ Análisis de Impacto al Negocio (BIA)
  - ✓ Plan de Continuidad del Negocio (BCP)
  - ✓ Plan de Recuperación ante Desastres (DRP)
  - ✓ Implementación de Políticas de Seguridad de la Información.
  - ✓ Implementación de Procedimientos de Seguridad de la Información.
  - ✓ **ePULPO:** Plataforma (software) para la gestión integral de la seguridad de la seguridad de la información.

4.2. Protección

✓ Soluciones de Seguridad Ad-hoc:

- Antimalware, Autenticación de Doble Factor y Cifrado (**ESET**).
- Firewall NextGen (**Barracuda Networks**).
- UTM (gateprotect).
- Antifraude, Antiphishing y Monitoreo de DNS (Hispasec)
- Monitoreo de infraestructura (Pandora FMS).
- DLP - Data Loss Prevention (Endpoint Protector).
- Antispam (Spamina y Barracuda).
- Solución de correo electrónico en la nube para empresas (Parla)
- Servidores NAS (Asustor).
- Backups y Recuperación de Información (StorageCraft).
- Help Desk (ServiceTonic).
- Solución contra Amenazas Persistentes Avanzadas – APTs (Cyphort).
- Gestión global y unificada de SGSI, ISO 27001, ITIL, EGSI (ePULPO).
- Seguridad de Bases de Datos (IMPERVA).
- SIEM + Unified Security Management & Threat Intelligence (Alienvault).

ENDPOINT PROTECTOR 4

Mobile Device Management (MDM) para iOS y Android

Mobile Device Management es un módulo de Endpoint Protector 4 cubriendo especialmente las necesidades de seguridad surgidos por el uso aumentado de dispositivos móviles personales (BYOD) o perteneciendo a la compañía.
Endpoint Protector es una solución todo en uno que hace posible que los Administradores de TI implementen y gestionen una Solución Data Loss Prevention en su red cubriendo ordenadores (Windows, Mac OS x, Linux) y dispositivos móviles (iOS y Android) de una manera eficiente y económica.
En un mundo donde los dispositivos portátiles y de estilo de vida transforman la manera en que vivimos y trabajamos, Endpoint Protector 4 está diseñado para mantener la productividad y hacer el trabajo más cómodo, seguro y agradable.

Ventajas claves

- Protección para iOS y Android
- El hardware y la maquina virtual implementados en unos minutos
- Interfaz basada en la Web
- Gestión intuitiva de Endpoints
- Protección proactiva contra el robo de datos
- VMware ready

Seguridad de Endpoint Móvil

Políticas fuertes de seguridad aplicadas en los smartphones y las tabletas de la compañía garantizarán una protección proactiva de los datos críticos del negocio donde quiera y en cualquier dispositivo móvil desde que se acceden.

Soporta Dispositivos Móviles iOS y Android

Controlar y gestionar las dos más famosas y poderosas plataformas móviles en crecimiento para proteger los datos de su compañía.

Aplicación de Contraseña

Forzar cambio periódico de contraseña directamente Over-The-Air o bien con la participación del usuario.

Seguimiento y Localización

Seguir de cerca la flota de dispositivos móviles de la compañía y saber siempre donde se encuentran los datos confidenciales de su empresa. Para iOS la aplicación EPP MDM tiene que ser instalada en el dispositivo.

Borrado Remoto (Nuke) / Bloqueo remoto – Protección contra el robo

Evitar que datos confidenciales lleguen a manos equivocados por tener control Over-The-Air y aplicar Nuke Remoto del Dispositivo (borrado remoto de datos) o bloquear el dispositivo en caso de pérdida o robo.

Restricciones para iOS

Desactivar funciones tales como iCloud, FaceTime, YouTube, AppStore, Compras In-App, iTunes, Siri, Cámara si no cumplen con la política de la empresa.

Gestionar Configuración de Correo, WiFi y VPN en dispositivos iOS

Gestionar Over-The-Air la configuración del E-mail, WiFi y VPN.

Borrar Configuración de E-mail y WiFi en dispositivos iOS

Borrar de forma remota el contenido y la configuración del E-mail corporativo y la configuración del WiFi. El contenido del E-mail corporativo se puede eliminar mientras que las cuentas personales de E-mail y contenido permanecen intactas.

Localizar dispositivo por sonido (Solo Android)

Fácil detección de cualquier dispositivo móvil perdido reproduciendo una canción el tiempo justo para localizar su smartphone / tableta.

Soporte para el Modelo Bring-Your-Own-Device

Tener control total sobre los datos confidenciales de la empresa sin importar si están almacenados en dispositivos personales o de la compañía y enfocar en hacer los empleados trabajar más eficiente.

Políticas basadas en localización/ Geofencing

Definir un perímetro virtual en un área geográfica utilizando un servicio basado en la localización. Esto proporciona una mejor gestión de las políticas de MDM que se aplican sólo en un área específica.

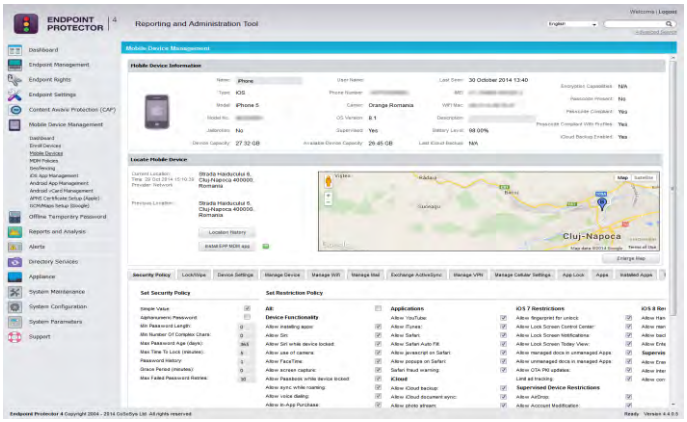
¡Las compañías tienen que definir y aplicar claramente políticas de Mobile Device Management para que se protejan!

Beneficios claves

- Imponer la política de uso de dispositivos móviles
- Proteger los datos de la compañía
- Control inmediato sobre el uso de dispositivos móviles
- Implementación Over-the-Air
- Impacto y esfuerzo mínimos para usuarios y administradores
- Cumplimiento
- Solución de seguridad BYOD

Gestión centralizada basada en Web / Panel de control

Gestione de forma centralizada el uso de dispositivos móviles. La interfaz de Administración e Informes basada en web satisface las necesidades del personal de administración y seguridad de TI y ofrece información en tiempo real sobre los dispositivos controlados en toda la empresa.



Gestión de inventario de Dispositivos Móviles

Permite el control y el inventario sobre los dispositivos móviles personales o de la compañía con registro e informes detallados de la actividad de dispositivos para auditoria posterior.

Encriptación de Dispositivo

Los iPhones y iPads vienen con encriptación hardware 256bit AES incorporada que es siempre activa y aplicada al establecer una contraseña al dispositivo.

Inscripción y Aprovisionamiento Over-The-Air

El proceso de inscripción garantizara una implementación fácil y segura de la plataforma MDM en cualquier infraestructura de TI.

Dispositivos Móviles Soportados

- iPad, iPhone, iOS 4.0, iOS 5.0, iOS 6.0, iOS 7.0, iOS 8
- Android 2.2+

Requerimientos para MDM

- Para MDM iOS se requiere una cuenta gratuita (hecha con un ID Apple) de Apple Push Notification Service (APNS)
- Para MDM Android se requiere una cuenta gratuita (hecha con una cuenta de Google) de Google Cloud Messaging para Android

Vista General de Características y Comparación para iOS y Android

Nuestro listado de características para iOS y Android se está extendiendo y sigue creciendo para cubrir siempre requerimientos de seguridad nuevos y emergentes.

Características MDM	iOS	Android
Políticas solidas de Seguridad	✔	✔
Longitud de contraseña	✔	✔
Reintentos de contraseña	✔	✔
Calidad de contraseña	✔	✔
Tiempo de bloqueo de pantalla	✔	✔
Aplicación de contraseña	✔	✔
Encriptación Forzada del	✔	✔
Seguimiento y Localización	✔(app)	✔
Localizar dispositivo perdido (sonido)		✔
Bloqueo Remoto	✔	✔
Nuke Remoto (Borrado Remoto)	✔	✔
Borrar dispositivo	✔	✔
Borrar contenido/ajustes de E- mail	✔	
Borrar Tarjeta SD		✔
Geofencing	✔	✔
Mobile Application Management	✔	✔
Restriccionar uso de cámara	✔	✔
Inscripción/Aprovisionamiento Over-The-Air	✔	✔
Inscripción por E-mail o por URL	✔	✔
Inscripción por SMS	✔	✔
Código-QR	✔	✔
Configuración de E-mail	✔	
Restringir uso de		
iTunes, iCloud, AppStore,	✔	
Compras In-App, Siri,	✔	
Cámara, FaceTime,	✔	
Forzar copia de seguridad cifrada de iTunes,	✔	
Safari, YouTube, etc.	✔	
Muchas más funciones disponibles	...	...
Versiones Soportadas	Apple iOS 4, 5, 6, 7, 8	Android 2.2+

Ciertas características de seguridad de dispositivos y de gestión no son soportados en versiones de SO antiguos y / o dispositivos.

Control de dispositivos para Windows, Mac OS X y Linux

Es otra de las características disponibles para la Prevención de Pérdida de Datos. Endpoint Protector ofrece características DLP adicionales para el control de dispositivos portátiles de almacenamiento y puertos en Windows, Mac OS X y Linux.

Protección de contenido para Endpoints (portátiles, etc.)

Protección de contenido para Windows y Mac OS X. Ofrece la posibilidad de controlar los datos sensibles que salen de la red corporativa. A través de inspección de contenido, las transferencias de documentos confidenciales de la empresa se registrarán y serán bloqueadas. Esta función evitará la fuga de datos a través de todos los posibles puntos de salida, desde dispositivos USB a aplicaciones como Microsoft Outlook, Skype, Navegadores Web, Dropbox, etc.

Endpoint Protector Hardware Appliance

Endpoint Protector Hardware Appliances son disponibles en diferentes capacidades para adaptarse a las necesidades de su negocio.

2013 MobileVillage Mobile Star Awards RISING STAR

2014 Computing Security Awards WINNER DLP Solution of the Year

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance puede ser utilizada de negocios de cualquier tamaño. Está disponible en formatos OVF, VMX, OVF, VHD, XV bis y PVM para ser compatible con las plataformas de virtualización más populares.

Utilizando el Appliance Virtual puede protegerse contra el uso no autorizado de dispositivos y pérdida de datos en su red en unos minutos.

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

Entornos Virtuales Soportados	Versión	.ovf	.vmx	.vhd	.xva	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Para los entornos marcados con *, por favor contacte nuestra línea de soporte. Otros entornos de virtualización pueden estar disponibles.

Visite www.EndpointProtector.com para una prueba gratuita.

CoSoSys Germany
E-Mail:
sales.de@cososys.com
Phone: +49-7541-978-2627-0
Fax: +49-7541-978-2627-9

CoSoSys North America
sales.us@cososys.com
+1-888-271-9349

CoSoSys Ltd.
sales@cososys.com
+40-264-593110
+40-264-593113

Contacte su socio local para más información:

COSOSYS

Creado en 12-Jun-2015

Oferta de Servicios de

Preparada para:

ARCOTEL

21 de Marzo, 2016

Contenido

Quito, 21 de marzo del 2016

Sr. Ingeniero
Jorge Vallejo
Coordinación Zonal 2
ARCOTEL
Ciudad

Apreciado Ingeniero:

GMS agradece la oportunidad de presentarle esta oferta de soluciones informáticas. Somos una empresa de Seguridad de la Información con más de 35 años de experiencia, durante los cuales hemos podido atender a muchas de las compañías más importantes de la región. Nuestras soluciones cubren las más altas exigencias de nuestros clientes, y nos caracterizamos por cumplir proyectos de alta complejidad. Asumimos el papel de socio estratégico para establecer relaciones exitosas a largo plazo.

Esperamos que esta propuesta sea de su conveniencia y quedo a su disposición para atender cualquier inquietud o comentario que pudiera surgir respecto a la misma.

Atentamente,

Ma. Elena Suquinagua
Asesor Comercial
mariaelena.suquinagua@gms.com.ec
Oficina: (593-2) 399-3000 ext. 7515
Celular: (593-9) 6799-5513
www.gms.com.ec
Quito – Guayaquil – Cuenca – Bogotá

I. Información sobre GMS

Perfil empresarial

Fundada en 1978, GMS es una de las empresas de seguridad informática de mayor trayectoria en la región. Nuestra visión es ser el líder a nivel regional de seguridad de la información que aporta de manera innovadora a la productividad de nuestros clientes.

Hemos estructurado nuestra oferta para brindar las mejores soluciones enfocadas a Seguridad de la Información, que se complementan con servicios de consultoría en estrategias, normas de TI y servicios de desarrollo de aplicaciones. Con nuestro apoyo, su empresa puede dejar en el pasado preocupaciones como incompatibilidad entre herramientas o rendición de cuentas con diversos proveedores que no logran responsabilizarse de la operación global de su red empresarial.

Datos de la Empresa:

- Razón Social: Grupo Microsistemas Jovichsa SA
- RUC: 1790590542001
- Dirección: Av. NNUU 1014 y Amazonas
- Teléfono: +593 (02) 399 3000

Sistemas de gestión

Para asegurar los niveles de servicio que requieren las empresas más exigentes, GMS opera con un sistema de gestión ITIL para el control de actividades y requerimientos. En el mismo, hemos habilitado un portal web que permite a nuestros clientes revisar el historial de los trabajos realizados para ellos, ingresar nuevas solicitudes, y hacer un seguimiento sobre el avance de las mismas. El sistema también permite registrar los niveles de satisfacción ante los soportes entregados, con lo cual mantenemos un control para asegurar un mejoramiento continuo.

Todos nuestros servicios cuentan con esquemas de escalamiento. Estos aseguran redundancia en canales de comunicación para que los clientes puedan aprovechar del soporte 7x24 ofrecido por GMS. Adicionalmente establecen tiempos de respuesta para distintos tipos de requerimientos, incluyendo los mecanismos de apoyo por parte de fabricantes internacionales, según el caso. La combinación de estos elementos permite a GMS otorgar niveles de atención y apoyo que marcan la diferencia.

Clientes destacados

Nuestro mayor logro ha sido conseguir y mantener la confianza de nuestros clientes. Más de 2.000 empresas han decidido trabajar con GMS. Entre algunas que lideran sus respectivos sectores se encuentran las siguientes:

Sector Financiero:

- Aseguradora del Sur
- Banco Amazonas
- Banco del Pichincha
- Banco del Austro
- Banco del Pacífico
- Banco Internacional
- Cooperativa de Ahorro y Crédito Ejército Nacional
- Cooperativa de Ahorro y Crédito San Francisco
- Cooperativa Juventud Ecuatoriana Progresista
- Helm Bank
- Raul Coka Barriga Seguros
- ZHM Seguros y Reaseguros

Manufactura y Consumo Masivo:

- Chaide & Chaide
- DANEC
- Endesa / Grupo Durini
- Industrias Ales
- INGESA
- La Fabril
- LEVAPAN
- Manufacturas Americanas
- Mercantil Garzozi & Garbu
- Neyplex
- Novopan / Pelikano
- Plásticos Ecuatorianos
- REYBANPAC
- ZaiMella

Educación:

- Colegio Tomás Moro
- Escuela Politécnica del Ejército
- Escuela Politécnica Nacional
- Universidad Católica Santiago de Guayaquil
- Universidad de las Américas
- Universidad Estatal de Bolívar
- Universidad San Francisco de Quito
- Universidad Tecnológica Equinoccial

Gobierno:

- Armada del Ecuador
- Corporación Nacional de Telecomunicaciones - CNT
- Ministerio de Coordinación de Desarrollo Social
- Ministerio de Relaciones Laborales
- Ministerio de Inclusión Económica y Social
- Ministerio de Justicia
- CNEL
- CELEC

Servicios:

- Adecco
- Cobiscorp
- Ernst & Young
- INMEDICAL
- Hospital Metropolitano
- Multitrabajos.com
- Pérez Bustamante y Ponce
- Ils Servilogistics
- Transoceánica

Medios de Comunicación y Publicidad:

- Diario EL UNIVERSO
- Editores Nacionales (Vistazo, América Economía, etc.)
- Gráficos Nacionales (Diario Extra)
- Grupo EL COMERCIO
- Grupo K
- Sonorama

Energía y Petróleos:

- CELEC
- CNEL
- Compañía de Petróleos de los Ríos - Petrolríos
- Consejo Nacional de Electricidad
- Empresa Eléctrica Regional Centro Sur
- Empresa Eléctrica de Riobamba
- EP Petroecuador
- Lutexsa Industrial – TERPEL
- Operaciones Río Napo
- P & S – Petróleos y Servicios
- SERTECPET
- SINOPEC International Petroleum Service Ecuador
- Sipetrol

Comercialización:

- Almacenes La Ganga
- Autolasa
- Comercial JAHER
- Consorcio NOBIS
- Distribuidora Farmacéutica - DIFARE
- Firmesa Industrial
- Grupo KFC
- Marcimex
- IIASA Caterpillar
- Juan Marcet
- Tiendas Industriales Asociadas - TIA
- Toyota del Ecuador

Servicios y Soluciones

En un entorno empresarial cada día más interconectado, se ha vuelto indispensable asegurar una correcta integración entre los componentes que sustentan la información de su negocio: seguridad informática, telecomunicaciones y aplicaciones. GMS ofrece experiencia y soluciones del más alto nivel en cada una de estas áreas, para asegurar a su empresa la correcta coordinación y óptimo funcionamiento de las mismas.

Seguridad Informática

La evolución de amenazas informáticas exige cubrir cada vez más frentes, sean capas de infraestructura dentro de nuestra red o dispositivos fuera de ella. Ofrecemos una amplia gama de soluciones especializadas para que su organización no sea vulnerada por el eslabón más débil de la seguridad:

Sophos es una de las empresas más grandes de seguridad informática a nivel mundial con más de 25 años de experiencia y aproximadamente 2.000 empleados. (Sophos UTM) protege a más de 100.000 redes, sean de PYMES, gobiernos, multinacionales o TELCOS, con una solución robusta e integral para la seguridad perimetral. Sophos UTM cuenta con diversas certificaciones y reconocimientos, incluyendo la distinción como líder en el Cuadrante Mágico de Gartner de soluciones UTM.

Kaspersky Lab es uno de los líderes mundiales en seguridad interna, especialista en tecnología antimalware. Fundada en Moscú en 1997, hoy protege a más de 300 millones de usuarios por todo el mundo. Su tecnología es regularmente premiada por analistas y publicaciones de renombre como Virus Bulletin, ICSA Labs, AV Comparatives y Gartner, quien considera a Kaspersky Lab entre los líderes de su cuadrante de proveedores antimalware.

AlienVault es una compañía privada con sede en Silicon Valley, cuenta con el respaldo de Trident de Capital, Kleiner Perkins Caufield & Byers, GGV Capital Intel Capital, Sigma West, Adara Venture Partners, Top Tier de capital y empresas de correlación. Los laboratorios de AlienVault llevan a cabo la investigación de seguridad sobre las amenazas y vulnerabilidades globales. Unified Security Management de Alien Vault cuenta con diversas certificaciones y reconocimientos, incluyendo la distinción como visionario en el Cuadrante Mágico de Gartner en soluciones security information and event management (SIEM).

FireEye es líder en la lucha contra ataques selectivos avanzados que utilizan malware avanzado, exploits desconocidos (zero-day) y tácticas de amenazas persistentes avanzadas. Las soluciones de FireEye complementan los firewalls tradicionales y de próxima generación, las soluciones de prevención de intrusiones, los antivirus y las puertas de enlace, que son incapaces de detener las amenazas avanzadas, dejando huecos de seguridad en las redes. La tecnología de FireEye actúa en todas las fases del ciclo de vida de un ataque con un motor que no emplea firmas y que utiliza análisis con información de estado para detectar las amenazas desconocidas.

Qualys es el líder mundial en soluciones de gestión de vulnerabilidades y compliance, reconocido como tal por múltiples analistas incluyendo Gartner. Sus soluciones están en uso por miles de empresas en cerca de 100 países, incluyendo más de la mitad de las empresas en el Forbes Global 100. Su tecnología permite escanear vulnerabilidades en IP's internas, IP's externas y aplicaciones web, además de realizar escaneos de cumplimiento de políticas, incluyendo normas internacionales como PCI.

Safend, empresa especializada en soluciones DLP (prevención de fugas de información), fue fundada en Israel en el año 2003, y ahora es subsidiaria de Wave Systems, empresa líder en seguridad basada en hardware. Sus soluciones se destacan por su facilidad de uso y permiten inspeccionar el contenido del tráfico en un endpoint para asegurar su cumplimiento con políticas granulares de control de confidencialidad, además de manejar la encripción de datos y el uso de puertos, medios removibles y conexiones inalámbricas.

Consultoría

Las decisiones de inversión en soluciones informáticas deben basarse en una visión clara de los problemas, sus impactos y sus soluciones, para así asegurar que generen un retorno para la empresa. GMS puede ayudar a lograr este objetivo a través de servicios de consultoría, sea esta en relación a procesos TICS, seguridades o infraestructura.

Áreas de competencia en procesos TICS:
Estrategia de servicios basada en Buenas Prácticas ITIL
Alineación de TICS con estrategias corporativas
Definición de proyectos y construcción de mapas de ruta
Definición de políticas de buen uso de TICS

Áreas de competencia en seguridades:
Sistemas de Gestión de Seguridad de Información (SGSI), incluyendo ISO 27000
Clasificación de información
Continuidad de negocio
Protección de infraestructuras críticas
Ethical Hacking
Capacitación en ISO 27.000, SGSI, análisis GAP, gobierno TI, Ethical hacking, protección de infraestructuras críticas, entre otros

Áreas de competencia en infraestructura:
Auditoría de hardware y software
Optimización de uso de recursos tecnológicos (ej. ancho de banda)
Análisis de retorno sobre la inversión (ROI) en proyectos de infraestructura

Seguridad Contra Fraudes Financieros

Durante más de 16 años, Kaspersky Lab ha investigado y desarrollado tecnologías de protección eficaz contra todo tipo de ciberamenazas, entre ellas las relacionadas con prevención de fraude. Aprovechando esta experiencia, Kaspersky Lab desarrolló Kaspersky Fraud Prevention, una plataforma tecnológica integral, altamente adaptada y fácil de usar , que puede ser ampliamente aplicada a diferentes sectores, tales como: sector financiero, entidades militares o gubernamentales, derecho y justicia, salud, entre otros. Teniendo como principal objetivo salvaguardar la información sensible que es transmitida entre los diferentes actores.

Kaspersky® FRAUD PREVENTION

Kaspersky Fraud Prevention proporciona una protección rigurosa a los diferentes niveles de intercambio de informacion en linea, sea estos por portales web, dispositivos moviles, o generando un analisis de comportamiento de los usuarios de los diferentes sistemas. Su combinación exclusiva de tecnologías y servicios de seguridad garantiza un sistema de protección de alto nivel, de esta forma las transacciones se benefician de tecnologías antifraude automáticas, sin trastornos en la experiencia del cliente.

Kaspersky Lab fue recientemente galardonado por: AV-TEST, con el PREMIO A LA INNOVACIÓN 2013 en la categoría de Transacciones Seguras, como reconocimiento a su papel pionero en la búsqueda de la batalla y contra los criminales en línea.

Desarrollo de software

Sea que requiera servicios o herramientas, GMS puede aportar mucho a los proyectos de desarrollo de aplicaciones en su empresa o institución.

Desarrollo de Software

Con un equipo humano con estándares elevados, metodologías formales en las fases de análisis, diseño, programación, pruebas e implementación, y el uso de herramientas avanzadas, GMS es su socio ideal para enfrentar su próximo proyecto. Sea el desarrollo de su nuevo sistema back-office, la creación de un portal de reportes, o simplemente un servicio de acompañamiento, GMS puede marcar la diferencia.

gms apps seguras

Desarrollo de aplicaciones móviles seguras que se integren al sistema central de una forma transparente, las cuales pueden ser usadas por los diferentes socios de negocio: los clientes, los proveedores y empleados. Estas aplicaciones se podrán diseñar en base a los requerimientos y oportunidades que se vayan identificando.

Facturación Electrónica

Aplicación desarrollada por GMS alojada en la Nube de Amazon, asegurando y protegiendo de esta manera los datos e información de la empresa y por otro lado eliminando la necesidad de inversión en infraestructura y Software. El servicio de facturación electrónica incluye todo el proceso de generación y administración de comprobantes electrónicos autorizados por el SRI.

GeneXus™

GeneXus es la primera herramienta inteligente para crear, desarrollar y mantener en forma automática aplicaciones multiplataforma. Con GX, las puede adaptar fácilmente a los cambios del negocio y las nuevas posibilidades brindadas por la evolución tecnológica. GX es producto de la empresa Uruguaya Artech, fundada en 1988 con oficinas en Brasil, México, Japón y China para soportar a miles de clientes a nivel mundial.

Reconocimientos

Gracias al compromiso con nuestros clientes, el nivel de nuestras soluciones, y nuestros sistemas de gestión, GMS ha logrado reconocimientos internacionales que son motivo de gran orgullo para nosotros. Entre ellos, se destacan los siguientes:

- **Kaspersky Lab**

2007: Partner del Año, Latinoamérica
2008: Spirit of Kaspersky
2009: Partner del Año, Latinoamérica
2010: Reseller del Año, Latinoamérica
2010-2011: Consejo Consultivo de Partners
2011: Partner del Año (Enterprise), Mercados Emergentes (Latinoamérica + África + Medio Oriente + Europa del Este)
2012: Partner del Año para Mercados Emergentes.
2013: Mejor proyecto del año

- **Sophos**

2010: Partner del Año, Sudamérica Hispana
2011: Partner del Año (Sophos UTM), Latinoamérica
2013: Partner del Año Latam
2014: Top Performer 2014

- **Asociación Brasilera de Calidad (ABIQUA)**

2010: Premio Panamericano de Calidad 2010

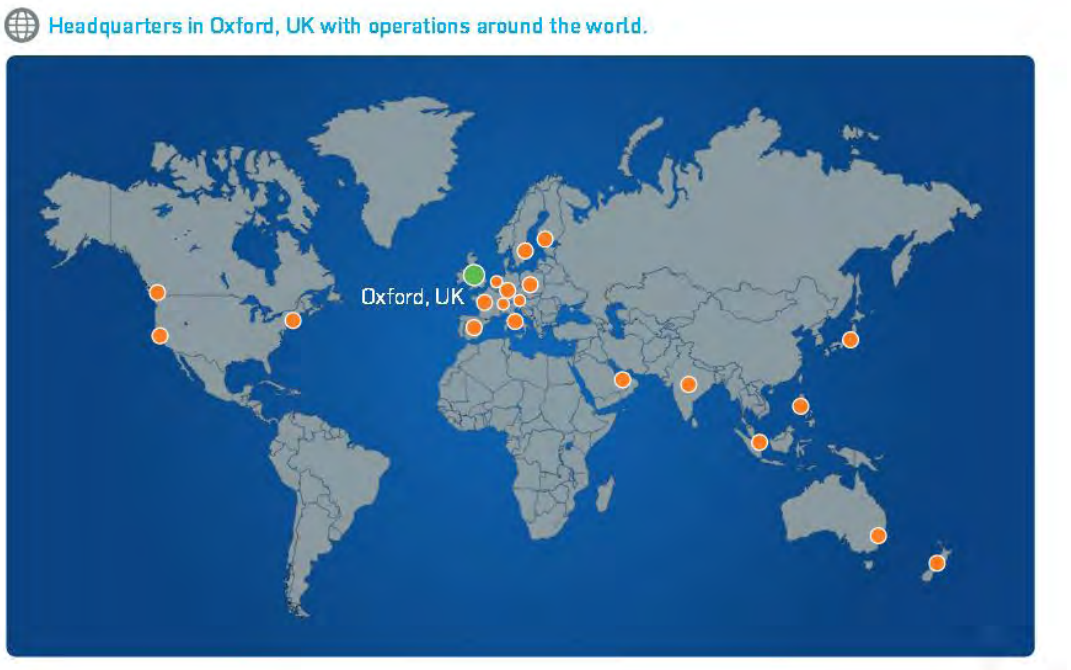
II. Información sobre soluciones ofertadas

Sophos Endpoint Protection

Antivirus sofisticado a la vez que sencillo, protección contra amenazas avanzadas, filtrado web y cumplimiento de políticas. Sophos Endpoint Protection hace que sea muy sencillo asegurar sus sistemas Windows, Mac y Linux contra programas maliciosos y amenazas avanzadas tales como ataques selectivos. Nuestra protección de última generación para estaciones de trabajo aúna tecnología innovadora como, por ejemplo, la detección de tráfico malicioso, con información sobre amenazas en tiempo real de Sophos Labs para ayudarle a prevenir, detectar y corregir amenazas de forma sencilla. También incorporamos filtrado web, control de aplicaciones, control de dispositivos y mucho más, directamente en el ligero agente para estaciones de trabajo, para que las políticas de su organización se apliquen en cualquier lugar al que vayan sus usuarios.

Perfil empresarial

Sophos es una compañía británica que ofrece las soluciones de seguridad para Internet más completas y fáciles de usar disponibles actualmente, al combinar las mejores aplicaciones del mercado y un rendimiento a nivel corporativo. Sophos cuenta con oficinas en todo el mundo y sus centros de operaciones están en Oxford (Inglaterra) y Boston (EE.UU). Además cuenta con laboratorios de análisis de malware en Australia, Hungría, Inglaterra y Canadá.



Sus galardonados productos proporcionan la protección más reciente con el mejor costo/beneficio. Su oferta de soluciones en Software, Hardware y Virtual Appliance proporciona a los usuarios la flexibilidad necesaria para satisfacer una amplia variedad de escenarios de despliegue. Distribuidos a través de una creciente red de más de 2.500 partners a nivel mundial, los productos de Sophos protegen hoy en día más de 100.000 redes para más de 47.000 clientes en 60 países.

Sophos UTM mantiene presencia en Ecuador desde el año 2004 y se ha convertido en una excelente alternativa para empresas pequeñas, medianas y grandes; cuando se trata de maximizar la protección de sus redes con presupuestos limitados.

Sophos UTM tiene certificaciones ICSA Labs, Common Criteria, y es el único fabricante de soluciones de seguridades que está posicionado dentro del cuadrante de líderes en Gartner con tres productos Unified Threat Management (UTM), Endpoint Protection Platforms y Mobile Data Protection. Con sus funcionalidades superiores y su interface de usuario intuitiva, las soluciones de Sophos han sido elogiadas internacionalmente por publicaciones líderes en seguridad IT.

Protección de redes

Nuestros productos de seguridad para redes incluyen firewalls, Conexiones Wi Fi, VPN, y protección web y del correo electrónico. Todas las funciones de seguridad se controlan en su totalidad desde un solo lugar. Además, nuestra gestión unificada de amenazas es fácil de implementar y gestionar para que los usuarios estén siempre protegidos, allá donde vayan.

Gestión unificada de amenazas

El paquete definitivo de seguridad para redes.

VPN segura

Convierta cualquier oficina en una ubicación segura.

Puerta segura de enlace a Internet

Protección web completa en cualquier lugar.

Cortafuegos de aplicaciones web

Protección poco común contra amenazas comunes.

Cortafuegos de última generación

El infierno de las amenazas para la red.

Conexiones wifi seguras

Conexiones wifi de alto nivel y alta seguridad.

Puerta segura de enlace de correo electrónico

Protección sencilla para un problema complejo.

Protección de usuarios

Desde PC a teléfonos inteligentes, tabletas y portátiles, nuestra seguridad para estaciones protege a los usuarios sin interrumpir su trabajo y sin sobrepasar el presupuesto destinado al antivirus.

Suites de protección de usuarios

La suite de seguridad todo en uno.

Sophos Cloud

Seguridad Sophos. Sencillez de la nube.

Control de dispositivos móviles

Múltiples dispositivos, una única solución.

Antivirus para estaciones de trabajo

Protección básica para ordenadores de sobremesa y portátiles.

Cifrado SafeGuard

Cifrado en todos los puntos.

Protección de Servidores

Nuestra solución antivirus ofrece protección rápida y eficaz en toda la red de servidores físicos y virtuales.

Seguridad para servidores

Servidores, sí. Virus, no. Y compatibilidad con VMware líder en el sector.

Antivirus para sistemas de almacenamiento en red

Seguridad de alta tecnología para almacenamiento de alta tecnología.

SharePoint Security

Colaborar con confianza

PureMessage

Buenas noticias para usted. Malas noticias para el correo no deseado.

Sophos UTM Endpoint Protection

Simplifique la seguridad administrando el antivirus para estaciones de trabajo desde el dispositivo UTM. UTM Endpoint Protection se administra de forma centralizada junto con la protección de la red. Mantenga protegida la red de Windows con un solo agente para estaciones que incluye antivirus, protección web y control de dispositivos. El agente evita programas maliciosos y fugas de datos sin complicados requisitos previos de redes o directorios. Y obtenga los informes detallados para conseguir total visibilidad y limpiar amenazas rápidamente.

Sophos SafeGuard Enterprise

Para mantener la productividad, los usuarios acceden a los datos corporativos desde numerosos dispositivos, independientemente de la política. Para mantener sus datos corporativos seguros y en línea con el cumplimiento normativo, nuestra solución de cifrado protege su información en todas las plataformas. Tenga la certeza de que los datos están siempre protegidos, tanto en dispositivos personales como en recursos compartidos de archivos en red o en la nube. Además, es compatible con Windows 8 y 8.1, así como con el cifrado de discos y archivos en equipos Mac. Sophos SafeGuard Enterprise es la solución de cifrado y protección de datos más completa: desde ordenadores a redes y la nube.

Certificaciones y Premios

Las soluciones para Internet de Sophos han sido probadas por las más representativas publicaciones de seguridad en la industria. Algunas de ellas son:

SC Magazine – Fabricante del año Mayo 2012

Sophos ganó el premio de Fabricante del Año en la revista SC Magazine Awards 2012 en reconocimiento a su alto nivel de satisfacción del cliente, la innovación constante, la influencia sobre la estrategia de seguridad de TI, y su posición de liderazgo en el mercado de protección de punto final y de datos. El premio fue anunciado en la 11 ª Conferencia Anual de Seguridad AusCERT Información.

Gartner Magic Quadrant Leader for Unified Threat Management (UTM), Endpoint Protection Platforms and Mobile Data Protection

ICSA Labs probó y renovó la Certificación de Firewall Certification para la versión actual de Sophos UTM.

Sophos UTM se convirtió en el primer equipo de Administración Unificada de Amenazas (UTM) que recibió la certificación de Common Criteria de la Oficina Federal Alemana para la Seguridad de la Información. Esta certificación asegura a los clientes de los sistemas y procesos de Sophos han sido probados satisfactoriamente por laboratorios acreditados e independientes y que cumplent con estándares de seguridad IT.

InformationWeek - Finalista: Mejor de Interop 2010 (2010/04/16)

Sophos RED fue enunciado como Finalista en Los Premios Lo Mejor de Interop. Los Premios Lo Mejor de Interop Awards reconoce a los expositors que han realizado avances tecnológicos significativos en una categoría específica

Sophos Receives 5 Star Rating from CRNCRN's 2012 Partner Program Guide

Sophos ofrece a los proveedores de soluciones, la información que necesitan para evaluar a los proveedores que ya trabajan o están considerando trabajar. Sophos recibió una calificación de 5 estrellas en la Guía del Socio Programa 2012.

III. Planes de Soporte

GMS agradece la oportunidad de presentarle esta oferta de servicios de soporte. Para nosotros es muy importante entregar productos y servicios que satisfagan los más altos estándares de protección y seguridad de la información de nuestros clientes. Para ello consideramos que un adecuado soporte sobre dichas herramientas es esencial para lograr su adecuado manejo y garantizar el éxito en la aplicación de las políticas de seguridad de cada organización.

Considerando las características particulares en cada empresa, GMS ha puesto a disposición de nuestros clientes distintas alternativas de soporte para ajustarse a las necesidades de cada una de ellas, es así que ofrecemos los siguientes planes:

Tipo de Plan	Horas Incluidas	Precio	Beneficios adicionales
Estándar	5	$250,00	Descuento superior al 35% en el precio de horas de soporte sin plan
Preferente	10	$500,00	Beneficios de ***Plan Estándar*** más posibilidad de uso en servicios de capacitación de GMS
Premium	50	$2.500,00	Beneficios del ***Plan Preferente*** más bono de 10% de horas adicionales
Platinum	100	$5.000,00	Beneficios del ***Plan Premium*** más posibilidad de uso en servicios de consultoría de GMS

Todos los planes de soporte están sujetos a las siguientes condiciones:

- Las horas pueden ser utilizadas en cualquier momento por un año calendario desde la fecha de su compra.
- El tiempo de soporte presencial será contabilizado en incrementos de horas enteras, mientras que el soporte remoto será contabilizado en incrementos de media hora.
- Se define como horario de oficina el periodo entre las 08:00 y 18:00 en días laborables. El tiempo de soporte entregado fuera de este horario será multiplicado por un factor de recargo del 50% en días laborables y del 100% en fines de semana o feriados.
- ***No se contabiliza*** el tiempo de soporte entregado bajo garantía propia del servicio o producto adquirido, bajo las políticas de los fabricantes correspondientes. Tampoco se toma en cuenta el tiempo requerido para recibir, identificar y asignar el tipo de solicitud de soporte requerido por el cliente. Adicionalmente no se tomará en cuenta el tiempo requerido para solventar problemas de configuración o gestión derivados del servicio del personal de GMS.
- Nuestro servicio es administrado sobre una herramienta certificada en ITIL, lo que nos permite un óptimo seguimiento de cada requerimiento. Al ser cliente de GMS, automáticamente se obtiene acceso a este sistema, el cual incluye un portal web que permite visualizar el estado actual e histórico de cada ticket de servicio. Los servicios de soporte se prestan bajo modalidad 7x24.
- En el caso que el cliente adquiera un nuevo plan de soporte, el período de vigencia del saldo de horas del plan anterior automáticamente será extendido por un año calendario adicional.

IV. Propuesta Técnica

1. Sophos Endpoint Protection

Detalle
Aspectos Destacados Protección innovadora que incluye seguridad contra programas maliciosos. Control de datos, dispositivo, aplicación y web para cumplimiento de las políticas. Filtrado web aplicado en la estación dentro o fuera de la red corporativa. Alto rendimiento incluso en sistemas más antiguos. Administración sencilla y centralizada. Implantación flexible con su elección de administración local o basada en la nube. 

Descripción de funciones

- **Protección innovadora**
  Sophos Endpoint Protection va mucho más allá de la prevención de programas maliciosos conocidos basados en firmas. Correlaciona actividades y comportamientos sospechosos utilizando información sobre amenazas en tiempo real de SophosLabs. Desde URLs maliciosas hasta códigos de ataque web y desde cambios inesperados del sistema hasta tráfico de comando y control, conectaremos los puntos para que sus estaciones y datos estén protegidos. El resultado: menos ordenadores infectados y una mayor protección contra ataques selectivos y filtraciones de datos

- **Control total**
  Aplique sus políticas de datos, dispositivos, aplicaciones y web con facilidad, gracias a la perfecta integración en el agente para estaciones y en la consola de administración.

  - ✓ **Control web:** Filtrado web basado en categorías aplicado dentro y fuera de la red corporativa.
  - ✓ **Control de la aplicación:** Bloqueo de aplicaciones por categoría o nombre con solo un clic.
  - ✓ **Control del dispositivo:** Acceso controlado a medios extraíbles y dispositivos móviles.
  - ✓ **Control de datos:** Prevención de pérdida de datos (DLP) utilizando reglas pre integradas o personalizadas

- **Alto rendimiento**
  Sophos Endpoint Protection se configura continuamente para ofrecer el mejor rendimiento. El agente ligero protege a sus usuarios sin ralentizar sus tareas. Las actualizaciones de protección ocupan poco espacio (menos de 30 KB habitualmente), de modo que las actualizaciones se pueden aplicar fácilmente en su red y estaciones de trabajo.

- **Simplicidad sofisticada**
  Al igual que su aplicación favorita para web o teléfonos inteligentes, Sophos Endpoint Protection ofrece una funcionalidad sofisticada junto con una experiencia de usuario sencilla e intuitiva. El despliegue rápido y fácil, las políticas predeterminadas bien equilibradas y la configuración automática de HIPS son solo algunos ejemplos de cómo hacemos las cosas de manera diferente.

- **Implementación y sistema de licencias flexibles**
  Elija administración local o en la nube, en función de la que sea más adecuada para su negocio. Sophos Cloud ofrece una consola basada en la web con políticas que los usuarios tienen que cumplir en todos los dispositivos y plataformas. Nuestra solución local le otorga el control total de su infraestructura de administración. Ambas ofrecen un rendimiento excepcional y protección con licencia por usuario, no por dispositivo

2. Opciones de Licenciamiento

Opciones de licencia

	Sophos Cloud Enduser Protection	Sophos Cloud Endpoint Protection Advanced	Sophos Cloud Endpoint Protection Standard	Enduser Protection	Endpoint Protection Advanced	Endpoint Protection Standard
Administración	**Basada en la web, alojada por Sophos en la nube**			**Basada en Windows, implementación local**		
Políticas basadas en el usuario	✔	✔	✔			
Protección contra programas maliciosos	✔	✔	✔	✔	✔	✔
HIPS	✔	✔	✔	✔	✔	✔
Seguridad web	✔	✔	✔	✔	✔	✔
Control web (filtrado)	✔	✔		✔	✔	✔
Detección de tráfico malicioso	✔	✔	✔	Muy pronto	Muy pronto	Muy pronto
Control de parches				✔	✔	
Restricción de aplicaciones				✔	✔	✔
Control de dispositivos	✔	✔		✔	✔	✔
Prevención de fugas de datos				✔	✔	
Cortafuegos cliente				✔	✔	✔
Administración delegada				✔	✔	✔
Sincronización con Active Directory	✔	✔		✔	✔	✔
Protección contra spam y programas maliciosos para Microsoft Exchange				✔	✔	✔
Protección contra programas maliciosos para almacenamiento en red (NetApp, EMC, Oracle)				✔	✔	
Gestión de dispositivos móviles	✔			✔		
Filtrado web, seguridad de dispositivo Android y cifrado móvil integrados				Opcional		
Soporte para sistema operativo	Windows, Mac; iOS, Android	Windows, Mac	Windows, Mac	Windows, Mac, Linux; iOS, Android, Windows Mobile, Windows Phone, BlackBerry	Windows, Mac, Linux	Windows, Mac

V. Propuesta Económica

1. Sophos Endpoint Protection.

Cant.	Detalle	1 Año Precio Total
526	Mobile Device Management, Mobile Application Management, BYOD Management, Platforms: iOS, Android, Windows Phone 8, centrally managed Mobile Security (AV, Web filtering) for Android, Secure Workspace (Documents) and Secure Email (Email, calendar, contacts) container apps, Sophos Mobile SDK.	$ 25,042.86
1	Instalación 50 equipos y transferencia de conocimientos para que el cliente pueda gestionar la instalación de equipos restantes.	$ 600.00
	TOTAL	**$ 25,642.86**

Observaciones generales

- Los valores indicados están en USD.
- Forma de pago: 100% a 30 días plazo.
- Validez de la oferta: 30 días
- Tiempo de entrega: 20 días laborables (desde la orden de compra)
- En caso de solicitar servicios de soporte y configuración adicionales a los cotizados GMS pone a su disposición las tarifas de planes de soporte especificados en el inciso III de Planes de Soporte.

VI. Escalamiento de soporte y recomendaciones

Para asegurar la mejor experiencia de nuestros clientes con las soluciones que ofrecemos, preparamos documentos que explican los contactos y mecanismos de escalamiento de soporte, más las recomendaciones de uso de las herramientas implementadas.

Quito: 399-3000 Guayaquil: 263-0400 Cuenca: 410-3320 Bogotá: +57 1 744 3993

Soporte 24 horas: +593 9 983-9231

soportegms@gms.com.ec

Escalamiento de soporte

Impacto	Tiempo de Atención y Solución en horas*					
	1er Nivel		2do Nivel		3er Nivel / Proveedor	
	Atención	Solución	Atención	Solución	Atención	Solución
Critico	1	4	1	8	1	24
Alto	1	6	1	16	1	48
Medio Alto	2	8	2	36	2	96
Medio	4	16	4	48	4	120
Bajo	8	24	8	72	8	144

Impacto	Descripción
Critico	Afectación completa al cliente
Alto	Afectación a un grupo de cliente
Medio Alto	Afectación a un usuario
Medio	No afecta a usuarios - degradación de servicio
Bajo	No afecta a usuarios - Servicios complementarios

El documento completo de escalamiento será puesto a disposición del cliente a la entrega del servicio.

* Los valores expuestos se aseguran en un 90% de incidentes o requerimientos, en caso de requerir ampliación de estos plazos, esto será debidamente comunicado y acordado con el cliente. Los tiempos se comienzan a contabilizar desde el primer contacto efectivo con el Centro de Soporte de GMS.

ANEXO 4.- LISTA DE APLICACIONES

No.	Aplicación	Descripción	Responsable
1	Activos Fijos	Software de manejo de activos e inventarios	Jenny Vasquez
2	ICS	Software de prediccion de Coberturas	Alexander Almeida
3	Inspecciones	Software de control y generacion de informes de inspecciones	Alexander Almeida
4	E - SIGEF	Software de gestion y conexión con Ministerio de Finanzas	Alexandra Mejía
5	QUIPUX	Software de Gestion y Control de Documentos	Alexandra Mejía
6	Homologaciones	Software para control y registro de terminales homologados	José Díaz
7	Infracciones y Sanciones	Software para control y registro de las infracciones y sanciones emitidas	Jenny Vasquez
8	SAMM	Software para control de sistemas moviles	Carlos Balladares
9	SAM – RNI	Software de gestion de mediciones de radiacion no ionizante	Coordinacion Zonal 5
10	Señal móvil Ecuador	Software para registro de problemas de niveles de calidad por usuarios	Coordinacion Zonal 6
11	Reclamos SM - RIT	Software para control de Reclamos realizados por usuarios	Gabriela Jurado
12	Planillaje	Software para registro y gestion de Pagos por usos de frecuencias	Jenny Vasquez
13	Rol de pagos	Software para generacion de rolos de pagos	Jenny Vasquez
14	OnBase	Software de archivo y consulta de documentos	Jenny Vasquez
15	Geoportal	Software de visualizacion de cobertura de servicios de telecomunicaciones	Jenny Vasquez
16	Patrocinio Judicial	Software de manejo de instancias judiciales	Víctor Ramirez
17	Publicaciones Web	Software para administracion de la pagina web	Luis Ibarra
18	Registro de Títulos Habilitantes (SACOF)	Software para administracion y consulta de Titulos Habilitantes	Luis Ibarra
19	SACER	Software para control y gestion de estaciones de control de espectro radioelectrico	Luis Ibarra
20	SIRATV	Software de ingreso de datos tecnicos de concesion de sistemas de Radio, Television y Audio y Video por Suscripcion	Luis Ibarra
21	SPECTRA	Software de ingreso de datos tecnicos de concesion de Frecuencias	Luis Ibarra
22	SIETEL	Software de ingreso de parametros contractuales de Sistemas de Valor Agregado, Portadores, Audio y Video por Suscripcion	José Díaz
23	SIGER	Software de Consulta de datos que se encuentran en el Espectra	Víctor Ramirez
24	CORREO ELECTRÓNICO	Software de Correo Electrónico	Maribel Saraguro
25	PAGINA WEB	Software o Pagina web de ARCOREL	Dirección de Comunicación
26	INTRANET	Software o Pagina web de acceso internos	Dirección de Comunicación
27	TELEFONÍA IP	Software de gestion y administracion de telefonia IP	Giovanny Males
28	ANTIVIRUS	Software de proteccion de virus	Maribel Saraguro