ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

"IMPLEMENTACIÓN UN SERVIDOR QUE PERMITA GESTIONAR Y ASEGURAR DISPOSITIVOS MULTIPLATAFORMA BLACKBERRY, ANDROID E IOS EN ENTORNOS CORPORATIVOS PARA EL DEPARTAMENTO DE POSVENTA DE LA EMPRESA TELEFÓNICA-QUITO"

TESIS DE GRADO

Previa la obtención del título de:

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

Presentado por:

NOBOA SILVA ANDRÉS ALFREDO

OLEAS CASTELO PABLO ESTEBAN

RIOBAMBA – ECUADOR

-2014 -

A Dios por darnos vida y mucha fuerza para enfrentar todas las pruebas.

A nuestras familias por siempre apoyarnos demostrarnos que todo es posible con voluntad y esfuerzo.

A nuestros padres por ser esas personas que siempre nos han alentado a esforzarnos enseñándonos que todo esfuerzo trae una gran dicha y por siempre ser ese ejemplo a seguir.

A Shaeska y Liset por su apoyo y comprensión.

De manera especial al Ing. Juan Carlos Oleas por su apoyo y colaboración incondicional.

A los Ingenieros de la Empresa Telefónica, por toda su cooperación y ayuda en el desarrollo de nuestro tema de Tesis.

Al Ing. Wilson Baldeón por sus sugerencias y contribuciones hacia el presente trabajo.

ANDRES----PABLO

A NUESTRA QUERIDA Y AMADA FAMILIA

ANDRES----PABLO

FIRMAS RESPONSABLES Y NOTA

NOMBRE	FIRMA	FECHA
Ing. Iván Menes **DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. Wilson Baldeón **DIRECTOR DE ESCUELA ING. EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES**	_____	_____
Ing. Wilson Baldeón **DIRECTOR DE TESIS**	_____	_____
Ing. Vicente Yuquilema **MIEMBRO DEL TRIBUNAL**	_____	_____
DIRECTOR CENTRO DE DOCUMENTACIÓN	_____	_____

NOTA DE LA TESIS:_____

RESPONSABILIDAD DE LOS AUTORES

Nosotros, Andrés Alfredo Noboa Silva y Pablo Esteban Oleas Castelo, somos responsables de las ideas, doctrinas, resultados expuestos en esta Tesis y el patrimonio intelectual de la misma pertenecen a la Escuela Superior Politécnica de Chimborazo.

_____

Andrés Alfredo Noboa Silva

_____

Pablo Esteban Oleas Castelo

ÍNDICE DE ABREVIATURAS

ACRÒNIMO	SIGNIFICADO
3G	Tercera Generación
A2DP	Advanced Audio Distribution Profile
AAC	Advanced Audio Coding
AD	Active Directory
AMD	Advanced Micro Devices
AMR	Audio/modem riser
API	Aplication Programming Interface
BDS	BlackBerry Device Service
BES	BlackBerry Enterprise Service
CDMA	Code División Múltiple Access
CEO	*Chief Executive Officer*
CPU	Central Processing Unit
DRM	Digital Rights Management
DTV	*digital TV*
EA	Electronic Arts
EDGE	Enhanced Data Rates for GSM Evolution
EV-DO	Evolution-Data Optimized o Evolution-Data Only
ext4	Fourth Extended Filesystem
FQDN	Fully Qualified Domain Name
GB	*Gigabyte*
GIF	Graphic Interchange Format
GPS	Global Position System
GSM	Global System for Mobile communications
HSP	High Speed Proxy
HTML	HyperText Markup Language
IBM	International Business Machines
IDC	International Data Corporation
iDEN	Integrated Digital Enhanced Network
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services

IMAP	Internet Message Access Protocol
iOS	Iphone Operating System
IP	Internet Protocol
JIT	Just in time
JPG	Joint Photographic Experts Group
LED	Light Emitting Diode
MAC	Media Access Control
MMS	Multimedia Messaging Service
MP3	MPEG-1 Audio Layer 3
MPEG	Moving Picture Experts Group
MTP	Media Transfer Protocol
NDK	Native Development Kit
NFC	Near Field Communications
NTFS	New Technology File System
OpenGL	Open Graphics Library
OS	Operating system
OWA	Outlook Web Access
PC	Personal Computer
PNG	Portable Network Graphics
POP3	Post Office Protocol 3
PTP	Picture Transfer Protocol
RAM	Random Access *Memory*
RIM	Research in Motion
RTP	Real Time Protocol
SD	Secure Digital
SDK	Software Development Kit
SIP	Session Initiation Protocol
SMS	Short Messagins Service
SP	Service Pack
SQL	Structured Query Language
TI	Tecnologías de Información
UDS	Universal Device Service
UM	Unified Messaging
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol

VPN	Virtual Private Network
WAP	Wireless Application Protocol
Wi Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WVGA	Wide Video Graphics Array
WXGA	Wide eXtended Graphics Array
XML	Extensible Markup Language
XP	*eXPerience*
YAFFS	Yet Another Flash File System
ZTE	Zhong Xing Telecommunication Equipment Company Limited

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La movilidad empresarial cada vez ha ido desarrollándose de manera exponencial, es así como las empresas necesitan estar conectadas a la red de su empresa a través del internet a cualquier hora y en cualquier momento.

Al ser sumamente necesario poseer movilidad empresarial surge el gran problema de la seguridad en todos los puntos críticos de las redes, y es por esta causa que se van desarrollando muchas tendencias hacia la movilidad empresarial segura.

La movilidad empresarial podrá transformar procesos, operaciones y desarrollar modelos de negocio más rentables.

Han pasado 3 años desde que Apple lanzó su iPhone, llevando a los smartphones al mercado masivo, pero los smartphones han existido realmente, de una forma u otra, desde 1993. La diferencia entre ese entonces y ahora, es que los primeros smartphones solo estaban disponibles para altos ejecutivos, ya que su precio resultaba prohibitivo para la mayoría de las personas. .

Adicionalmente, el crecimiento de las tecnologías, el incremento en el manejo y automatización de datos y el mercado global tan competido han hecho que los negocios no sean lo mismo y la tendencia tanto en el mercado de consumo como en el empresarial sea cada vez más orientado a la movilidad. Es decir, llevar el trabajo a donde se genera la acción y donde el personal puede tomar ventaja de ello y no al revés, comprometer un lugar físico para desarrollar un determinado trabajo.

La movilidad empresarial se está alejando cada vez más de los dispositivos para centrarse en las tareas de gestión, desde el acceso seguro a las infraestructuras y contenidos de la empresa, hasta el uso de sus aplicaciones. Por ello, disponer de dispositivos móviles profesionales que abarquen estas nuevas necesidades será clave para las empresas.

Una de estas soluciones empresariales recién desarrolladas es BlackBerry Enterprise Server 10 la cual fue lanzada recientemente para Ecuador siendo

esta poca administrada y manejada en el país siendo un tema muy nuevo el lograr la unificación de sistemas operativos que hasta el momento era demasiado difícil.

CAPÍTULO I

MARCO REFERENCIAL

1.1. INTRODUCCIÓN

En el presente capítulo se plantea la situación actual del entorno empresarial, así como la necesidad de facilitar la movilidad corporativa, se presenta la situación actual ante los Smartphones y como se ha ido desarrollando las soluciones tecnológicas.

1.2. ANTECEDENTES

La continua evolución tecnológica, creó la necesidad de que las empresas extiendan las barreras del trabajo cotidiano en las oficinas a lugares diferentes a estos, dicha necesidad hizo que se generaran equipos donde se pueda compactar todas las funciones disponibles en las oficinas tales como internet, correo, intranet, aplicaciones corporativas, etc., en un solo equipo y sumado a eso la necesidad de una movilidad continua dio lugar al nacimiento de dispositivos móviles hoy conocidos como Smartphone.

En la actualidad hay diversa gama de Smartphone con distintos sistemas operativos tales como Android, BlackBerry, IPhone (IOS), etc.

A nivel mundial, actualmente el uso de Smartphone, se ha convertido en algo cotidiano y normal para el medio en el que se está desarrollando la sociedad, la misma que tecnológicamente va creciendo a pasos agigantados.

Según la IDC, durante el primer semestre del 2013, el mercado mundial de teléfonos celulares mostró un aumento de un 4%, y cómo se había pronosticado, se habían vendido más Smartphone que teléfonos normales, teniendo que con 418,6 millones de unidades, el 51,6% del total, equivalente a 216,2 millones de celulares, correspondieron a Smartphone [1].

A nivel latinoamericano según la misma IDC durante 2013, la industria latinoamericana de TI crecerá 10.3%, totalizando 140.5 mil millones de dólares. El Hardware constituirá casi dos tercios del crecimiento, mientras que el software representará el 13%, y servicios el 21%. Los tres lo harán a tasas similares durante 2013. México, Brasil y Colombia serán los mercados de mayor crecimiento, con tasas de 13%, 12% y 11%, respectivamente [2].

Hablando específicamente de marcas se tiene que Samsung fue la empresa que capturó el mayor porcentaje de la cuota de mercado de los Smartphone con un 32.7%, seguido de Apple con 17.3%, LG con un 4.8%, Huawei con 4.6%, y ZTE con 4.2%.

En Ecuador, al igual que a nivel mundial, el uso de Smartphone se va haciendo más común, aunque según la misma Advance Consultora la preferencia por Smartphone en éste momento, es del 20.8% frente al 79.2% [3] que tienen por otro tipo de teléfonos celulares.

Es así que se deduce que éstos usuarios que pertenecen al 20.8% son en su mayoría ejecutivos, empresario y también personas con mayor fuente de ingresos económicos.

En la conferencia BlackBerry Live, que se llevó a cabo del 14 al 16 de mayo del 2013, la empresa anunció que gradualmente irá introduciendo sus servicios para Android 4.x y el IPhone (con iOS5 o superior), y que incluirá todas las funciones (chat, transferencia de archivos, video llamadas), sin costo [4].

La razón, es la constante evolución de los sistemas operativos, con opciones más innovadoras para el usuario, así como más facilidad en la gestión de datos. Es así como un estudio realizado por la empresa como Zscaler, que proporciona soluciones de seguridad para Internet, revela la verdadera tendencia en el uso del tráfico web empresarial móvil a nivel mundial. La sorpresa fue que más de un 40% utiliza Android. Detrás vendría BlackBerry con un 37.26% y después IOS con solo un 22.38% del mercado empresarial. [5]

1.3. JUSTIFICACIÓN DEL PROYECTO DE TESIS

La necesidad de tener una plataforma que soporte Smartphone con diferentes Sistemas Operativos, hizo que se abriera un abanico de oportunidades a empresas como Airwatch, Good for Enterprise, Sybase Afaria, entro otras a generar multiplataforma que permitieran soportar Smartphone con sistemas operativos diferentes, también es importante mencionar que la plataforma Exchange con su servicio Active Sync es soportado por la mayoría de Smartphone independiente del Sistema Operativo que contengan.

Estas plataformas según sus características presentan diferentes niveles de seguridad, diferentes niveles de administración y diferentes niveles de aplicación de políticas de TI, por lo que dependerá de las necesidades de cada empresa y los costos que estén dispuestos a asumir.

Al convertirse los Smartphone en una herramienta indispensable para el funcionamiento y crecimiento de las empresas, trajo consigo a los

administradores de seguridad de la información un terrible dolor de cabeza, para tratar de controlar la seguridad de la información de las empresas que circulan por los dispositivos móviles, si bien es cierto las plataformas permiten administrar los dispositivos y tener seguridad en la transmisión de la información, no permiten asegurar que la información crítica, delicada, confidencial sea protegida y manejada de una forma adecuada.

En virtud de esto BlackBerry hace una actualización a su servicio corporativo conocido como BES y le agrega el BlackBerry Balance, que lo que hace es proteger los datos corporativos sin limitar la experiencia del usuario, también aísla la información corporativa y evita que los utilice en canales personales es decir no se puede copiar, pegar, etc. Y asegura la privacidad de los datos personales del usuario.

Pese a que BlackBerry tiene una de las plataformas más seguras del mercado para la administración y gestión de los datos corporativos seguía presentado una gran falencia y es que no es una multiplataforma que permita integrar otras marcas y Sistemas Operativos a su plataforma, llevándole a perder mercado.

Para solucionar este problema BlackBerry lanza su nueva plataforma BlackBerry 10 o BES, la misma que permite integrar Android y IOS (IPhone) a su plataforma de administración y gestión de correo, agregando la seguridad que le caracteriza al BlackBerry de una forma más limitada a estos dispositivos, pero con la capacidad de aplicar políticas e individualizar la parte corporativa de la parte personal individual.

Con esto lo que se busca es analizar las diferentes plataformas que existen en el mercado y compararlas con una nueva funcionalidad que tiene BlackBerry para la gestión multiplataforma que permita asegurar la información corporativa.

Se va a instalar esta nueva plataforma en un servidor virtualizado en donde se aplicaran políticas de gestión y seguridad en los diferentes dispositivos multimarca para verificar el adecuado funcionamiento de la protección de información de una empresa o corporación.

1.4. OBJETIVOS

1.1.1. OBJETIVO GENERAL

- Implementar un servidor que permita gestionar y asegurar dispositivos multiplataforma BlackBerry, Android e IOS en entornos corporativos para el departamento de Posventa de la empresa Telefónica-Quito

1.1.2. OBJETIVOS ESPECÍFICOS

- Aislar la información de trabajo en un entorno corporativo para prevenir la filtración de canales a través de la copia de archivos.
- Brindar seguridad en un entorno móvil de punta a punta para dispositivos BlackBerry, Android e IPhone.
- Analizar la infraestructura que soporta el servicio multiplataforma para la gestión de dispositivos.
- Describir como distingue BDS entre los datos empresariales y los personales.
- Implementar un servidor que ayude al departamento de posventa de Telefónica a ofertar su nueva solución tecnológica.

1.5. HIPÓTESIS Y OPERACIONALIZACIÓN DE VARIABLES

La administración de dispositivos móviles multiplataforma asegurará la información en un entorno corporativo.

Las variables a considerar en este proyecto son:
Número de políticas de TI configuradas vs número de políticas ejecutadas correctamente por plataforma, vienen a ser las variables independientes y la variable dependiente es la seguridad de la información.

CAPÍTULO II

TELEFONÍA MÓVIL

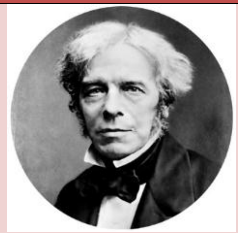
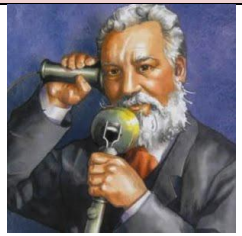
2.1. INTRODUCCIÓN A LOS SISTEMAS CELULARES

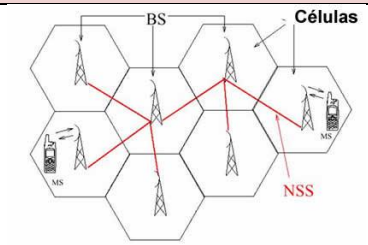
En este capítulo se detalla todo lo relacionado a los sistemas móviles o celulares, su historia, evolución, tipos y características.

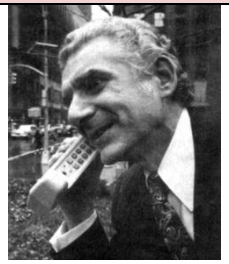
Se describen los sistemas celulares, conociendo su historia y desarrollo, sus características, tipos y aplicaciones y finalmente se hace hincapié en los Smartphones indicando clases, plataformas, utilidades.

2.2. HISTORIA Y EVOLUCIÓN DE LOS SISTEMAS CELULARES

En la tabla II.I se observa un resumen de la historia de la telefonía celular:

AÑO	HECHO	CARACTERÍSTICAS	FIGURA
1846	Michael Faraday empieza los estudios sobre la conducción de la electricidad en el espacio.	Su mayor logro fue la postulación de la ley de inducción electromagnética, mostrando que un campo magnético en movimiento podía inducir una corriente eléctrica en una bobina	 **FIGURA II. 1 Michael Faraday** Fuente: http://www.biografiasyvidas.com/biografia/f/faraday.htm
1876	Alexander Graham Bell inventa el teléfono convencional	Diseñó un aparato para convertir el sonido en impulsos eléctricos, invento inscrito en el registro de patentes estadounidense en 1876.	 **FIGURA II. 2 Alexander Graham Bell** Fuente: http://implantadacoclearfeliz.blogspot.com/2012/05/197-ejemplo-de-superacion-alexander.html

1894	La comunicación inalámbrica, formalmente fue presentada en 1894 por un joven italiano llamado Guglielmo Marconi.	A partir de su investigación sobre la transmisión y recepción de ondas electromagnéticas, logró llegar a separar el transmisor y receptor hasta 121 Km.	 **FIGURA II. 3 Guglielmo Marconi** Fuente: http://www.biografiasyvidas.com/biografia/m/marconi.htm
1947	Se generaron las ideas de una sistema de comunicación por “células” que le permitían a los usuarios ser identificado desde cualquier punto que se hiciera la llamada	El principal inconveniente era la tecnología de la época, no ayudaba para implementar las ideas.	 **FIGURA II. 4 Células de telefonía** Fuente: http://archivo.e-consulta.com/blogs/eureka/?p=7
1949	La comunicación celular empieza con equipos instalados en autos.	En ese tiempo las bandas utilizadas eran de HF y VHF. El inconveniente fue la necesidad de antenas con gran potencia, y por ende el precio era bastante elevado.	 **FIGURA II. 5 Primeros equipos de comunicación celular** Fuente: http://www.informatica-hoy.com.ar/telefonos-celulares/La-historia-del-Telefono-Celular.php

1964	Se implementan los primeros sistemas de selectores de canales automáticos.	Se deja a un lado la necesidad de utilizar el sistema “push to talk” Se elimina también la necesidad de la ayuda de una operadora para la interconexión	 **FIGURA II. 6 Central telefónica antigua** Fuente: http://www.entredosamores.es/madrid%20antiguo/madridantiguo2.html
1971	La compañía AT&T hizo una propuesta para solucionar el problema de proporcionar una eficiencia del espectro de frecuencia mayor	Finlandia se lanza a implementar la primera red pública exitosa de telefonía móvil, llamada la red ARP	**FIGURA II. 7 Logotipo de la empresa AT&T** Fuente: https://www.recordedfuture.com/upcoming-att-phones/
1973	El Dr. Martin Cooper, gerente general de sistemas de Motorola realizó una llamada a sus competidores de AT&T desde su teléfono celular	Cooper viene a ser la primera persona en realizar una llamada de éste tipo.	 **FIGURA II. 8 Martin Cooper realizando la primera llamada telefónica móvil** Fuente: http://www.bberryblog.com/hoy-se-cumplen-40-aos-de-la-primera-llamada-por-telfono-mvil/

1977- 1987	Los teléfonos celulares se hacen de acceso al público en general.	La ciudad de Chicago empezó con 2000 clientes y luego se unió Washington DC y Baltimore. Japón lanza el producto a las masas Se lanzan los Sistemas móviles de telefonía avanzados (AMPS).	 **FIGURA II. 9 Siemens C1** Fuente: http://www.generacionyoung.com/blogs/tecnologia-cumplen-40-anos-primera-llamada-movil/
1988	Se crea el estándar TDMA	Oficializado en 1991	 **FIGURA II. 10 Ericsson T18 (TDMA)** Fuente: http://jasonirwin.ca/2011/02/20/the-first-cell-phone/
1996	Bell Atlantic Mobile lanza la primera red comercial CDMA en los Estados Unidos [6]	Aparece el Motorola StarTAC, la rápida adopción por parte del público y su atractivo diseño lo ubicaron en el mejor producto masivo de ese año (según la revista Business Week) –a pesar de costar u$s1000 el equipo- [7]	 **FIGURA II. 11 Motorola StarTAC** Fuente: http://www.conexionbrando.com/1342831

Finales 90’s	Los teléfonos de formato “candybar” de Nokia fueron un hit.	Poseían pantalla mono-cromática, una antena externa y un cuerpo cuadrado.	 **FIGURA II. 12 Nokia 6160 (1998) y Nokia 8260 (2000)** Fuente: http://unmundomovil.blogspot.com/2010/08/la-evolucion-del-celular-con-imagenes.html
2001	El Kyocera QCP6035 fue el mejor producto de éste año.	Fue el primer teléfono basado en Palm OS.	 **FIGURA II. 13 Kyocera QCP6035** Fuente: http://unmundomovil.blogspot.com/2010/08/la-evolucion-del-celular-con-imagenes.html
2002	La empresa Research In Motion lanza al mercado el Blackberry 5810.	• Organizador personal, envío y recepción de e-mails, teclado “thumb”, teléfono móvil GSM en un mismo dispositivo • Otros teléfonos también son lanzados como el T-Mobile Sidekick y el Sony Ericsson	 **FIGURA II. 14 Blackberry 5810** Fuente: http://unmundomovil.blogspot.com/2010/08/la-evolucion-del-celular-con-imagenes.html

2003	NOKIA lanza su N-GAGE	Quería combinar teléfono celular y dispositivo de juego, pero no tuvo gran aceptación, en parte por su extraño diseño curvo que no era práctico y también porque el altavoz y el micrófono del teléfono estaban situados en el borde lateral del aparato	 **FIGURA II. 15 Nokia N-Gage (2003)** Fuente: http://unmundomovil.blogspot.com/2010/08/la-evolucion-del-celular-con-imagenes.html
2004	Motorola Razr v3 puso el diseñó a otro nivel.	Líneas escasas y apariencia metálica lisa.	 **FIGURA II. 16 Motorola Razr v3 (2004)** Fuente: http://unmundomovil.blogspot.com/2010/08/la-evolucion-del-celular-con-imagenes.html
2005	El Motorola Rokr fue lanzado en septiembre	Unió el reproductor de música iTunes de Apple, y el excelente diseño de Motorola.	 **FIGURA II. 17 Motorola Rokr (2005)** Fuente: http://unmundomovil.blogspot.com/2010/08/la-evolucion-del-celular-con-imagenes.html

2006	Research In Motion lanza el teléfono Blackberry Pearl.	Con un fino diseño y teclado SureType fue el primer Blackberry en incluir una cámara y un reproductor de audio y video.	 **FIGURA II. 18 Blackberry Pearl (2006)** Fuente: http://unmundomovil.blogspot.com/2010/08/la-evolucion-del-celular-con-imagenes.html
2007	Apple presentó al mundo lo que llamaron la Reinvención del teléfono, el IPHONE.	Diseño innovador, que carecía de keypad numérico, cámara fotográfica de 2 mp, la habilidad de sincronizar, iTunes con el teléfono, entre otros [8].	 **FIGURA II. 19 Apple IPhone (2007)** Fuente: http://unmundomovil.blogspot.com/2010/08/la-evolucion-del-celular-con-imagenes.html
2009	Samsung Electronics lanza el Samsung Galaxy i7500.	El mayor acierto de la compañía Samsung, en cuanto a telefonía se refiere	 **FIGURA II. 20 Samsung Galaxy i7500** Fuente:

			http://www.microsiervos.com/archivo/gadgets/samsung-galaxy-i7500.html
2010	Arranca la competencia entre APPLE, SAMSUNG, y BLACBERRY.	El objetivo era uno solo, llegar a ser la mejor plataforma que ofrezca servicios móviles en el mundo.	 **FIGURA II. 21 Imagen comercial sobre la competencia entre las 3 plataformas** Fuente: http://www.cnmeonline.com/news/in-wake-of-blackberrys-
2013	ANDRIOD de Google y el hardware de Samsung están a la delantera en cuanto a preferencia de los usuarios	Blackberry decide unificarse con las otras 2 plataformas, dado paso a que BBM sea compatible con ANDRIOD y IOS, lo mismo hizo con su plataforma de administración a nivel corporativo BES10	 **FIGURA II. 22 Blackberry 10 el último OS de Blackberry** Fuente: http://www.tapscape.com/bes-10-now-available-allows-blackberry-os-and-ios-management/

TABLA II. I HISTORIA COMUNICACIONES CELULARES

Fuente: Elaboración propia

2.3. Cronología de las comunicaciones por RF

El avance de las comunicaciones RF también fue fundamental en todo el desarrollo de la telefonía celular. En la siguiente tabla II.II se detalla de manera cronológica, cómo empezó a ser utilizado él espacio RF del espectro electromagnético para las comunicaciones.

1921	El Departamento de Policía de Detroit transmite órdenes a los policías mientras conducen los patrulleros.
1932	La Policía Civil de la ciudad de Nueva York adopta la misma técnica que opera en la banda de onda corta de 2MHz.
1933	La Comisión Federal de Comunicaciones de los Estados Unidos autoriza la utilización de 4 canales en la banda de 30MHz a 40MHz, en forma experimental.
1945	La empresa Bell desarrolla osciladores que alcanzan la banda de los 150MHz, frecuencia muy elevada para la época, y propone aplicarla en la telefonía móvil.
1946	La empresa Bell emprende un servicio comercial de telefonía móvil en la banda de 35MHz y otro en la de 150MHz, este último con intervalo de 60kHz entre canales, con 6 canales de voz liberados para uso comercial.
1947	Se inaugura un Sistema de Telefonía Móvil a lo largo de la ruta Nueva York-Boston, que opera en la banda de 35MHz a 44MHz. Empleando “Simplex Push-to-Talk” y una telefonista lo auxiliaba, con un procedimiento poco utilizado por el asistente de teléfono común. Además el abonado tenía que conseguir una vía (canal) desocupada, antes de solicitar su llamada. Pese a los inconvenientes presentados, la demanda por este tipo de servicio era muy grande y la poca oferta originaba una larga lista de espera de los que pretendían usarlo. El sistema era sencillo, el abonado debía solicitar un canal a la operadora

	para que se haga la comunicación. Establecido el contacto, cada abonado podía hablar a su debido tiempo dado que se empleaba una sola portadora, de ahí que cada vez que un abonado terminaba la oración empleaba el término “cambio” que le indicaba al abonado remoto que podía oprimir su botón del micrófono para empezar a hablar.
1955	Se crean nuevas técnicas y los circuitos electrónicos ya permiten la incorporación de nuevos canales de transmisión dentro de los ya existentes. Así, de 6 canales originales, se incorporan otros 5 canales, con intervalos de 30kHz entre unos y otros.
1956	La técnica anterior se aplica en la banda de los 450MHz y el gobierno norteamericano autoriza la creación de 12 canales en ese sistema.
1964	Se crea una nueva técnica, denominada de MJ, en la que se permite el mejor aprovechamiento del uso de los canales existentes y ya no se utiliza más el Push-to-Tolk (tener que apretar un botón para poder hablar), ahora el usuario puede entablar una comunicación sin pausa.
1969	Extienden la automatización hasta la banda de los 450MHz (MTS o Mobile Telephone Service), bautizado como sistema MK. Estos dos sistemas, el MJ y el MK, fueron los precursores del IMTS (Improved Mobile Telephone System), estandarización adoptada hasta que surge el modelo AMPS. Presionado por el mercado y, lógicamente, por las empresas, operadoras, el gobierno norteamericano pega un salto al vacío y libera la banda de los 75MHz en las operaciones de la telefonía fija, y la banda de los 40MHz en las operaciones de telefonía móvil.
1971	La Bell acepta el desafío y presenta un trabajo que demuestra que puede lograrlo.

1974	La FCC (Comisión Federal de Comunicaciones de los Estados Unidos) reglamenta la operatividad de la banda, con pequeñas alteraciones.
1975	La empresa Illinois Bell recibe autorización para operar el sistema recién adoptado.
1983	Nace el sistema AMPS (Advanced Mobile Phone Service), con la implementación, en la ciudad de Chicago, del Sistema Celular, completamente diferente a todo lo desarrollado hasta entonces.

TABLA II. II CRONOLOGÍA DESARROLLO RF

Fuente: Elaboración propia

Con el surgimiento de la telefonía móvil celular se amplió considerablemente el número de usuarios, debido al tipo de técnica usada que ha permitido que la telefonía móvil se convierta en un producto de gran consumo. Como consecuencia del avance tecnológico, los aparatos celulares poseen más características y aplicaciones, que ayudan a los usuarios a su vida cotidiana y laboral. Y algo más, se sabe que es mucho más fácil y barato implantar un sistema de telefonía celular que un sistema de telefonía fija tradicional, resulta más rápida y el usuario ve incrementados los beneficios [9].

2.4. FUNCIONAMIENTO DE LOS SISTEMAS CELULARES

Antes de la implementación del sistema celular como se conoce actualmente, existieron sistemas de comunicación móvil previos, los cuales intentaron cubrir la necesidad de la comunicación en movimiento.

Los sistemas de comunicación móvil que precedieron a la telefonía celular fueron: la Comunicación Móvil de Radio, el Servicio de Telefonía Móvil (MTS) y el Servicio de Telefonía Móvil Mejorado (IMTS) [10].

2.5. Componentes de un sistema celular

Un sistema celular para su funcionamiento está compuesto por los siguientes elementos:

Unidades de telefonía móvil y portátil: Ambas unidades son prácticamente iguales diferenciándose en la potencia de salida del transmisor. Las unidades portátiles tienen una potencia de salida más baja y una antena menos eficiente. Cada teléfono consiste en una unidad de control, un transceptor de radio, una unidad lógica, y una antena. La unidad de control supervisa todas las interfaces de usuario mientras que el transceptor utiliza un sintetizador de frecuencias para sintonizar los canales asignados. La unidad lógica se relaciona con las acciones del suscriptor y con los comandos al transceptor y a la unidad de control.

Las celdas (radio bases): La radio base provee la interface entre el MTSO y las unidades móviles. Tiene una unidad de control, cabinas de radio, antenas y una planta de generadora eléctrica y terminales de datos. Opera bajo la dirección del centro de conmutación. Administra cada uno de los canales de radio en el sitio, supervisa las llamadas, enciende y apaga el transmisor y receptor de radio, inyecta información a los canales de control y realiza pruebas de diagnóstico en el equipo del sitio de la celda.

La PSTN: es una matriz de conmutación controlada digitalmente cuyo objetivo es proporcionar una conexión entre dos o más terminales. Dependiendo de la densidad de población una PSTN podría tener cerca de 100,000 terminales conectadas a ella. Por lo tanto un área metropolitana mayor podría tener más de un switch PSTN interconectado

El conmutador central móvil (MTSO, Mobil Telephone Switching Office, oficina de conmutación de telefonía móvil) : El conmutador central el procesador y conmutador de las celdas. Está interconectada con la Oficina Central de telefonía pública fija. Controla el procesamiento

y tarificación de llamadas. El MTSO es el corazón del sistema celular móvil, se considera parte de la familia de PSTN.

Las conexiones o enlaces: Los enlaces de radio y datos interconectan los tres subsistemas. Estos enlaces pueden ser por medio de antenas de microondas terrestres o por medio de líneas arrendadas.

- Una célula es un área geográfica cubierta por señales RF.
- La fuente de radio frecuencia (RF) está localizada en el centro de la célula.

La forma y tamaño de la célula dependen de muchos parámetros:

1. Potencia de transmisión (ERP).
2. Ganancia y patrón de la antena.
3. Ambiente de propagación.
4. Nivel de recepción de la señal (RSL) en el borde de la célula (-90dbm definido en el borde de la célula).

- Por lo tanto una célula es prácticamente irregular.
- Cada estación base tiene diferente potencia de transmisión [11].

2.6. Generaciones de las comunicaciones móviles

En la siguiente figura II.23 se observa la evolución de los sistemas móviles.

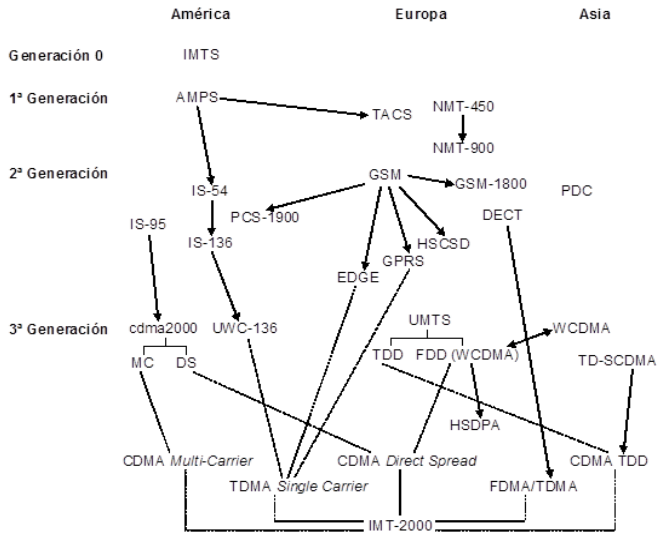


FIGURA II. 23 Generaciones de las comunicaciones móviles [19].

2.6.1. Cuadro de las generaciones celulares.

A continuación se presenta un cuadro con las generaciones celulares desde la llamada generación cero hasta las proyectadas 5, 6 y 7g.

GENERACIONES	CARACTERÍSTICAS	TECNOLOGÍAS	
Generación 0	Surge de la necesidad de mejorar su antecesor push-to-talk, el cual transmitía y recibía en unas sola frecuencia, y para saber quién transmitía, había la necesidad de pulsar un botón y sólo uno de los dos usuarios podía hacer 1 sola cosa a la vez.	IMTS (Improved Mobile Telephone System)	Daba a disposición de los usuarios 23 canales espaciados entre 150 y 450 MHz, y tenía una capacidad máxima del orden de los 1.000 usuarios, con esto ya no se transmitía y recibía en una sola frecuencia. Para los años 80 la demanda del servicio era muy alta, es por eso que los proveedores se vieron en la necesidad de seguir evolucionando, hasta llegar hasta el sistema de telefonía móvil actual [9].
Primera generación	Hizo su aparición en 1979 Analógica y estrictamente para voz. Calidad de enlaces era muy baja (2400	AMPS (Advanced Mobile Phone System)	Se introdujo el concepto de celda y de handoff entre celdas. Diseño basado en dar cobertura dividiendo la zona de cubrimiento en

	bauds). Imprecisa en la transferencia de celdas. Carecía de seguridad.		varias celdas, lo que permite un mejor aprovechamiento del espectro AMPS funciona en un ancho de banda de 25 MHz útiles. Divide las comunicaciones de lo que corresponde a protocolo, y de voz en canales que en la práctica son frecuencias diferentes. La identificación del terminal, en el sistema AMPS se llama NAM [12].
		DAMPS (Digital Advanced Mobile Phone System)	Es una evolución de AMPS que pasa de usar técnica de acceso FDMA a FDMA/TDMA. Es una digitalización del sistema AMPS. La voz se digitaliza con un vocoder de 8 Kb/s. Cada portadora de 30 KHZ soporta 3 time slots. La primera versión digitalizó el canal de voz (IS 54B) y permitió la coexistencia entre AMPS y DAMPS. La última fase consistió en digitalizar el canal de control a objeto de permitir

			servicios como SMS (IS 136) [12].
Segunda generación	Fue digital Utiliza protocolos de codificación más sofisticados y se emplea en los sistemas de telefonía celular actuales Los protocolos de 2G soportan velocidades de información más altas que 1G por voz, pero limitados en comunicación de datos. En Estados Unidos y otros países se le conoce a 2G como PCS (Personal Communication Services) [13].	GSM (Global System for Mobile)	Se utiliza GSM para denominar a una familia de tecnologías que incluye GPRS, EDGE y UMTS/HSDPA Permite que varios usuarios compartan un mismo canal de radio merced a una técnica llamada multiplexado por división de tiempo (TDM). Brinda acceso constante a servicios de voz de alta calidad y servicios optimizados (por ejemplo, mensajería de texto) [14]. Extensa cobertura También utiliza una técnica llamada "frequency hopping" (salto de frecuencias) que minimiza la interferencia de las fuentes externas y hace que las escuchas no autorizadas sean virtualmente imposibles. Autenticación de la Identidad del Abonado Confidencialidad de la Identidad del Abonado

			Confidencialidad de los Datos de Señalización Confidencialidad de los Datos del Usuario
		2.5G	Más rápida y económica que 3G Más capacidades adicionales que los sistemas 2G, como: GPRS (General Packet Radio System), HSCSD (High Speed Circuit Switched), EDGE (Enhanced Data Rates for Global Evolution), IS-136B e IS-95Bm entre otros [15].
Tercera generación	Permite estar conectado de forma permanente a Internet a través del teléfono móvil, el ordenador de bolsillo y el ordenador portátil. Propone una mejor calidad y fiabilidad, una mayor velocidad de transmisión de datos y un ancho de banda superior. El primer país en implementar una red comercial 3G a gran escala fue Japón [16].	UMTS (Universal Mobile Telephone System)	Permite introducir muchos más usuarios a la red global del sistema, y además permite incrementar la velocidad a 2 Mbps por usuario móvil. Facilidad de uso y bajos costos Nuevos y mejorados servicios Acceso rápido

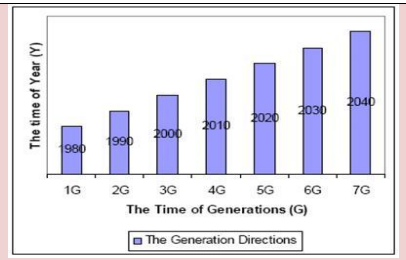
Cuarta generación	Basada totalmente en IP Es una generación con proyección a mejorar la eficiencia, la reducción los costes, la ampliación y mejora de los servicios ya prestados y una mayor integración con los ya protocolos existentes. El concepto de 4G englobado dentro de 3G incluye técnicas de avanzado rendimiento radio como MIMO y OFDM [17].	WIMAX	División de frecuencia ortogonal múltiple. Aplica Viterbi y turbo aceleradores para avanzar en corrección de errores. La radio WiMax es mucho más sencillo [18].
		LTE (Long term evolution)	División de frecuencia ortogonal múltiple, Aplica Viterbi y turbo aceleradores para avanzar en corrección de errores. Utiliza una sola frecuencia portadora division multiple access (SC-FDMA) para la señalización de enlace ascendente [18].
Generaciones del futuro	- Con el avance de la tecnología a pasos agigantados, existen analistas y escritores, que se atreven a visualizar las generaciones del futuro que serias las 5,6, y 7G.	Desde la 5g se proyecta utilizar LAS-CDMA, OFDMA, MC-CDMA, UWB, Network-LMDS e IPv6; pasando por la sexta generación que se integrarán sistemas de comunicación satelital y para la séptima generación el roaming y el handover deberían ocurrir en el espacio.	 **FIGURA II. 24 Evolución de las generaciones celulares** Fuente: "The Future of Mobile Wireless Communication Networks", X li, A Gani, R SIleh and O. Zakaria, International Conference con Communication Software and Networks, 2009.

Tabla II. III Generaciones Celulares

Fuente: Elaboración propia

CAPÍTULO III

PLATAFORMAS Y S.O DE SMARTPHONES

3.1. INTRODUCCIÓN

Un dispositivo móvil para su funcionamiento lleva un sistema operativo en el cual se cargan todas sus funcionalidades y aplicaciones.

En este capítulo se detalla los tres sistemas operativos o plataformas que dominan el mercado mundial abarcando la gran mayoría de dispositivos en uso: Android que es una versión de Linux usado principalmente por los teléfonos Samsung, IOS que es la plataforma de Apple cuyos equipos insignia son los IPhones, y la plataforma BlackBerry que hasta hace poco dominaba el mercado corporativo bajo la cual funcionan los dispositivos con el mismo nombre.

3.2. PLATAFORMA ANDROID

Android es un sistema operativo basado en Linux, el cual fue diseñado en su mayoría para dispositivos móviles que cuenten con pantalla táctil, como son los Smartphones y las Tablet-PC, esta plataforma es usada en los smartphones Samsung.

3.2.1. HISTORIA ANDROID

El primer Smartphone que atrajo la atención del público fue el BlackBerry de la compañía canadiense Research In Motion, como resultado de la fragmentación del mercado celular tanto el costo de los teléfonos y el mantenimiento del servicio ponía esta tecnología lejos del alcance de la gran mayoría de usuarios. No fue sino hasta la introducción del IPhone en el 2007, que el concepto de un Smartphone fácil de usar, estándar y de un precio accesible desató la masificación de los Smartphone más allá de la esfera empresarial.

Lo que hizo que se buscara una equidad de plataformas, no fue la publicidad de IBM, ni los trucos monopólicos de Microsoft, fue simplemente un conjunto de estándares públicos que permitían a cualquiera desarrollar hardware o software para el IBM PC, además, la compatibilidad con las PC era una característica importante que todo fabricante deseaba ofrecer.

El empresario y desarrollador Andy Rubin tuvo la idea de desarrollar un sistema operativo para celulares basado en la filosofía del Open Source y para ello creo Android. Rubin se había dado cuenta de que la gran fragmentación del mercado hacía imposible que la tecnología evolucionara rápidamente en el sector de los celulares. Por lo tanto decidió plantear la idea de un sistema operativo para celulares que fuera de código abierto, adaptable a cualquier hardware, pero que ofreciera un entorno de desarrollo único que permitiera crear aplicaciones para cualquier hardware. Esta idea es la misma que estaba detrás del éxito del IBM PC.

Rubin ya tenía varios inversionistas de riesgo dispuestos a invertir en el proyecto Android, pero había otro proyecto similar llamado Symbian que también corría sobre Linux. Por lo tanto se aproximó a Google para ofrecerles exclusividad en las búsquedas realizadas desde los celulares con Android a cambio de que Google expresara su apoyo público a la plataforma. Luego de que Rubin le hiciera la presentación a Larry Page en el 2005, este recibió una oferta de compra de parte de Google por $50 millones, y la dirección del departamento de la compañía que se encargaría del desarrollo de la plataforma para celulares.

Aunque el G1 (el primer celular con Android ofrecido por Google) apareció en el último trimestre del 2008, no fue sino hasta la llegada del Nexus One y Android 2.1 (en enero de 2010), que las ventas de celulares con Android se dispararon y consiguieron capturar en menos de un año más de la mitad del mercado de Smartphone en U.S.A., desplazando del primer lugar a Blackberry y sepultando los sueños de conquista global de Apple [20].

3.2.2. ETIMOLOGíA

Android es de código abierto en su mayoría ya que pertenece a Google, y está bajo la licencia Apache, que es libre y de código abierto. La estructura de Android se compone de Apps que se ejecutan en un entorno de Java sobre un núcleo de bibliotecas de Java en una máquina virtual denominada Dalvik, con compilación en tiempo de ejecución. Compila, por la naturaleza de Java, a una máquina virtual. Este sistema operativo tiene unas 12 millones de líneas de código, incluyendo las 3 millones de líneas de XML, 2.8 millones de líneas en C y 2.1 millones de líneas de Java. También hay 1.75 millones de líneas en C++.

El nombre Android hacen alusión a la novela de Philip K. Dick ¿Sueñan los androides con ovejas eléctricas?, que posteriormente fue adaptada al cine como Blade Runner. Tanto el libro como la película se centran en un grupo de androides llamados replicantes del modelo Nexus-6. El nombre del logotipo es “Andy”.

Las versiones de Android reciben el nombre de postres en inglés. En cada una el postre elegido empieza por una letra distinta siguiendo un orden alfabético:

A: Apple Pie (v1.0), Tarta de manzana
B: Banana Bread (v1.1), Pan de plátano
C: Cupcake (v1.5), Panque.
D: Donut (v1.6), Rosquilla.
E: Éclair (v2.0/v2.1), Pastel francés.
F: Froyo (v2.2), (Abreviatura de «frozen yogurt») Yogur helado.
G: Gingerbread (v2.3), Pan de jengibre.
H: Honeycomb (v3.0/v3.1/v3.2), Panal de miel.
I: Ice Cream Sandwich (v4.0), Sándwich de helado.
J: Jelly Bean/Gummy Bear (v4.1/v4.2/v4.3),
K: KitKat (v4.4) [21].

3.2.3. CARACTERÍSTICAS

Los sistemas Android manejan varias características incorporadas como:

- Framework de aplicaciones: permite el reemplazo y la reutilización de los componentes.
- Navegador integrado: basado en el motor open Source Webkit.SQlite: base de datos para almacenamiento estructurado que se integra directamente con las aplicaciones.
- Multimedia: Soporte para medios con formatos comunes de audio, video e imágenes planas (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF).
- Máquina virtual Dalvik: Base de llamadas de instancias muy similar a Java.
- Telefonía GSM: dependiente del terminal.
- Bluetooth, EDGE, 3g y Wi-fi: dependiente del terminal.
- Cámara, GPS, brújula y acelerómetro: Dependiente del terminal
- Pantalla Táctil [22].

3.2.4. ARQUITECTURA

Android maneja una estructura bastante sencilla y se conforma de 4 componentes:

En la siguiente figura III.1 se muestra la estructura del sistema Android

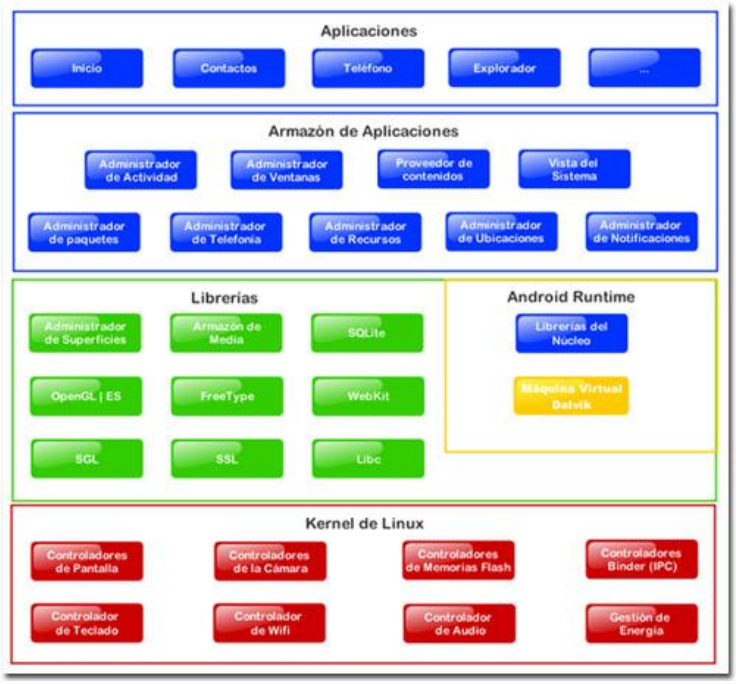


FIGURA III. 1ARQUITECTURA ANDROID

FUENTE: http://www.configurarequipos.com/doc1107.html

3.2.5. LOGO

En la siguiente figura III.2 se indica el logo característico de Android:

FIGURA III. 2LOGO ANDROID

FUENTE: http://www.configurarequipos.com/doc1107.html

Este logo fue diseñado para ser el símbolo internacional de Android, y es de código abierto, al igual la propia plataforma. No hay referencias culturales a otros personajes o iconos culturales. El proceso fue muy simple. El fundador de Android hizo una investigación sobre el tema androide/robot. Estaba claro que el logo necesitaba estar relacionado con el nombre del SO. El primer paso fue crear un gigantesco motherboard con todo tipo de androides y robots que estuvieran inspirados en el SO. El siguiente paso fue explorar una gran variedad de lenguajes visuales y direcciones artísticas (desde dibujos basados en píxeles hasta realistas o dibujos animados). Estuvieron dos diseñadores trabajando en ello. [23]

3.2.6. VENTAJAS Y DESVENTAJAS DE ANDROID

3.2.6.1. VENTAJAS DEL SISTEMA ANDROID

El código de Android es abierto: Google liberó Android bajo licencia Apache. Cualquier persona puede realizar una aplicación para Android.
Hoy día hay más de 650.000 aplicaciones disponibles para teléfonos Android, aproximadamente 2/3 son gratis. Además la libertad de código permite adaptar Android a bastantes otros dispositivos además de teléfonos celulares. Está implantado en Tablets, GPS, relojes, microonda, incluso hay por internet una versión de Android para PC.

El sistema Android es capaz de hacer funcionar a la vez varias aplicaciones y además se encarga de gestionarlas, dejarlas en modo suspensión si no se utilizan e incluso cerrarlas si llevan un periodo determinado de inactividad. De esta manera se evita un consumo excesivo de batería. Esta es una de sus mayores ventajas por la rapidez con la que carga una aplicación abierta previamente. Por ejemplo al abrir Google Maps, en un momento la aplicación localiza la posición en el mapa [24].

3.2.6.2. DESVENTAJAS DEL SISTEMA ANDROID

A pesar de ser una ventaja el ser un sistema multitarea: El hecho de tener varias aplicaciones abiertas hacen que el consumo de la batería aumente y como no todas las aplicaciones Android las cierra hay que instalar una aplicación para que las cierre. En la tienda de Android hay una buena cantidad de aplicaciones para este fin, así que el problema es solucionable pero debería venir pre instalado de fábrica.

Duración de la batería: la batería en un celular Android se agota muy rápido. Utilizando las aplicaciones de manera moderada la batería puede llegar a durar más, pero para un usuario que usa mucho sus aplicaciones la batería no tiende a durar, lo que se puede solucionar con algunas aplicaciones, pero volvemos a lo mismo no viene pre instalada de fábrica, hace falta una aplicación externa al sistema Android para optimizar mejor la batería.

Poco intuitivo: Para la mayoría el sistema operativo es muy complicado. Por ejemplo se vuelve complicado configurar el teléfono, esto te puede llevar mucho tiempo, y esto es generado por la interfaz de Android. Hay aplicaciones que ayudan en tareas que deberían ser sencillas como desinstalar otras aplicaciones pero, otra vez, volvemos a lo mismo se hace necesario instalar aplicaciones para solucionar el problema [24].

3.3. PLATAFORMA IOS

Esta es otra plataforma o sistema operativo móvil, que pertenece a la empresa Apple Inc. En su inicio se lo desarrollo para el IPhone, pero después sirvió en otros dispositivos como el IPod Touch, IPad y el Apple TV. Una característica importante es que el sistema IOS no puede ser instalado en sistemas operativos diferentes a los de Apple. Su cuota en el mercado ha ido en crecimiento pero siempre ha sido relegado por el sistema Android.

3.3.1. HISTORIA DE IOS

Apple tenía una cierta incertidumbre para ir al mercado de la telefonía móvil, lo que Apple quería, era un teléfono con un buen diseño, características únicas, atractivo y que funcionara bajo un sistema nunca antes visto, es por eso, que en 2005 fue la primera vez que Apple habló de la posibilidad de que hubiera un teléfono en su compañía, en una conferencia, en el Motorola ROKR.

Apple estaba planeando lanzar al mercado un teléfono con una pantalla totalmente táctil sin algún teclado físico, totalmente en la pantalla, bastante minimalista, que funcionara bajo la idea de un Sistema Operativo de una computadora en un teléfono, produciendo el IPhone, un Smartphone: Teléfono, Computadora y Multimedia, de aquí salió IOS.

IPhone OS, apareció por primera vez en Enero del 2007, con el IPhone EDGE, en ese entonces IOS no tenía tal fama ni un interés por parte de los desarrolladores debido a que la versión 1.0 no tenía la opción de instalar aplicaciones de terceros y era bastante sencilla pero funcional.
El interés fue aumentando cuando los rumores comenzaron a principios de 2008 cuando se decía que desarrolladores de juegos y de aplicaciones como EA, Gameloft, entre otras, estaban programando aplicaciones que funcionaran en la plataforma del IPhone y del IPod Touch, y fue así hasta junio del 2008 cuando se presentó el IPhone 3G, con la versión 2.0 que incluía la tienda de aplicaciones o App Store, con ello la opción de instalar aplicaciones en el IPod Touch o el IPhone sin ningún límite.

Con la versión del ahora llamado IOS 4.0, sufrió importantes cambios como una pantalla de inicio totalmente personalizada, con la opción de poner tu propio fondo de pantalla, crear carpetas y multitarea. Dispositivos que funcionan con IOS

Actualmente IOS tiene más de 500,000 de Aplicaciones desarrolladas por terceros, corriendo bajo su plataforma, las competencias no llegan a ese

número tan alto, por ejemplo Android Honeycomb (La plataforma del IPad) apenas llega a las 100 aplicaciones y hay otras que no pasan de 20, conclusión, IOS ha hecho que tanto el IPhone como el IPod Touch y el IPad sea un éxito por su capacidad de hacer absolutamente todo, desde jugar, tomar fotografía y chatear hasta pagar impuestos.[26]

3.3.2. INTERFAZ DE USUARIO

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) [26].

3.3.3. VERSIONES IOS

Detalla la evolución que ha tenido el sistema operativo IOS desde el 2007 Cabe recalcar que las versiones de software de IOS van de la mano con versiones de Hardware llamados IPhone.

3.3.3.1. IPhone OS 1 (Junio de 2007 junto al IPhone original)

El lanzamiento de esta versión fue portada de la revista Time como el invento del año bajo calificativos tan difíciles de discutir como “El teléfono que ha cambiado los teléfonos para siempre”, el IPhone original cayó como una bomba en 2007. Incluso después de su presentación, nadie esperaba que fuese a tener un impacto tan grande en la industria.

Aquella primera versión tenía grandes carencias, pero también grandes aciertos como sus aplicaciones de correo electrónico y navegación por Internet, un reproductor digno de llevar el nombre de la familia IPod y una revolucionaria interfaz multitáctil tan intuitiva como versátil con decenas de detalles nunca vistos hasta ese momento: un teclado táctil que de verdad podías utilizar, las listas con inercia, el rebote… Google Maps y YouTube también formaban parte de las apps de serie, pero el único modo que tenían el resto de desarrolladores para llegar al IPhone era a través de aplicaciones web [27].
En la figura III.6 se muestra el IPhone:

Figura III. 3 IPHONE OS1

FUENTE: http://www.applesfera.com/ios/la-evolucion-de-ios-desde-2007-hasta-la-actualidad-especial-historia-wwdc

3.3.3.2. IPhone OS 2 (Junio de 2008 junto al IPhone 3G)

La segunda versión tuvo como objetivo, pulir muchos de los detalles que se habían dejado sin atención para poder lanzar el IPhone original a tiempo. Acompañó al IPhone 3G, el primer modelo en cruzar las fronteras estadounidenses y llegar a países como España, y su novedad más

significativa fue el lanzamiento de la App Store y el soporte de aplicaciones nativas de terceros.

Fue todo un éxito y en apenas dos meses la App Store ya contaba con más de 3.000 apps que habían sido descargadas 100 millones de veces. Un año después se convertirían en más de 85.000 apps y 2000 millones de descargas. Algo inaudito para una tienda digital de aplicaciones que sería rápidamente imitada por la competencia.

Otras novedades interesantes de esta versión fueron la visualización de documentos adjuntos de Microsoft Office e iWork en Mail, reproducción de vídeos de YouTube directamente desde Safari, sincronización push de correo electrónico, calendario y contactos, geo etiquetado de las fotografías realizadas con la cámara, mejoras de seguridad como el soporte de WPA2/802.1X o el borrado remoto, y capacidad para realizar capturas de pantalla [27].

En la figura III.7 se detalla el IPhone 3G

Figura III. 4 IPHONE OS2

FUENTE: http://www.applesfera.com/ios/la-evolucion-de-ios-desde-2007-hasta-la-actualidad-especial-historia-wwdc

3.3.3.3. IPhone OS 3 (Junio de 2009 junto al IPhone 3GS)

Esta versión tuvo más de 100 nuevas características, la novedad estrella de esta versión fue sin duda la esperada función de copiar, cortar y pegar, pero no

fue la única: soporte de mensajes MMS; búsquedas con Spotlight; teclado apaisado para apps como Mail, Mensajes, Notas y Safari; mejoras en el API del GPS para permitir la navegación paso a paso; nuevas apps como la Brújula digital, Notas de voz o Buscar mi IPhone; grabación de vídeo en el 3GS con sencillas opciones para editarlos o compartirlos y el novedoso control del enfoque mediante una simple pulsación.

Safari también pasó a contar con soporte de HTML5 y registró grandes mejoras en su motor de JavaScrit, aumentando su velocidad entre 3 y 16 veces según el caso. Además, al fin era capaz de autocompletar los campos de los formularios con nuestra información.

Las notificaciones push para aplicaciones de terceros, el control por voz, el soporte de Nike+ y las opciones de accesibilidad con funciones como VoiceOver también se estrenaron en esta versión [27].

La figura III.8 muestra el IPhone 3GS

Figura III. 5 IPHONE OS3

FUENTE: http://www.applesfera.com/ios/la-evolucion-de-ios-desde-2007-hasta-la-actualidad-especial-historia-wwdc

3.3.3.4. IOS 4 (Junio de 2010 junto al IPhone 4)

Esta es probablemente la versión de IOS más ambiciosa lanzada hasta la fecha. IOS 4, estrenó nuevo nombre para señalar que ya no se trataba solo de un teléfono nunca más para englobar también al IPad y el IPod Touch.

Más de 100 nuevas características y 1500 nuevas APIs para desarrolladores con las que liberar toda la potencia del IPhone 4: Multitarea, carpetas, FaceTime (en aquel momento, tan solo sobre Wi-Fi), Game Center, soporte para la primera pantalla Retina de la manzana (con cuatro veces la resolución del IPhone 3GS), mayor soporte para empresas, grandes mejoras en Mail, fondos de pantalla personalizados, soporte de teclados Bluetooth, modo para fotografías HDR y nuevas apps como iMovie e iBooks. Una gran versión [27].

La figura III.9 muestra el IPhone 4

Figura III. 6 IPHONE OS4

FUENTE: http://www.applesfera.com/ios/la-evolucion-de-ios-desde-2007-hasta-la-actualidad-especial-historia-wwdc

3.3.3.5. IOS 5 (Octubre de 2011 junto al IPhone 4S)

Esta versión fue la última versión en la que se presentó Steve Jobs antes de su muerte cuatro meses después y es imposible ignorar que su estado de salud ya era tremendamente delicado en ese momento.

En cuanto a IOS 5, el Centro de Notificaciones, iMessage, iCloud y Siri fueron las grandes novedades de esta versión en la que también se estrenaron los recordatorios, la integración con Twitter y una gran cantidad de mejoras de la app Cámara incluyendo el acceso directo desde la pantalla de bloqueo, la posibilidad de utilizar el botón de volumen como disparador, o más funciones de edición fotográfica. En total 200 nuevas prestaciones que en España nos dejaron con un sabor de boca agridulce a causa de la tardía e incompleta llegada de Siri a nuestro idioma ensombreciendo otras novedades importantes como la sincronización inalámbrica con iTunes y el fin de la dependencia de un ordenador para configurar los dispositivos IOS [27].

En la figura III.10 se presenta el IPhone 4S

Figura III. 7 IPHONE OS5

FUENTE: http://www.applesfera.com/ios/la-evolucion-de-ios-desde-2007-hasta-la-actualidad-especial-historia-wwdc

3.3.3.6. IOS 6 (Septiembre de 2012 junto al IPhone 5)

Esta es la última versión presentada por Scott Forstall, el antiguo vicepresidente sénior de Software IOS antes de su caída en desgracia justamente un año después de la muerte de su principal aliado en la compañía, Steve Jobs. Los errores con el lanzamiento del nuevo servicio de Mapas (con una app notablemente más avanzada pero con errores de bulto frente a los datos de Google Maps utilizados hasta ese momento) no le ayudaron en la lucha de poder interna que se estaba desarrollando sobre el futuro de IOS y de la que Jonathan Ive terminó saliendo victorioso.

Al margen de esto, IOS 6 trajo novedades interesantes como un Siri vitaminado al fin en español, integración con Facebook, la función de Compartir Fotos en Streaming a través de iCloud, Passbook, algunos refinamiento realmente notables en las funciones básicas del teléfono (como enviar mensajes predeterminados al colgar una llamada), sincronización de pestañas en Safari entre todos nuestros equipos y dispositivos, fotografías panorámicas de hasta 28 mega píxeles de serie con el IPhone 4S o superior y un montón de pequeños pero necesarios detalles [27].

La figura III.11 muestra el IPhone 5:

Figura III. 8 IPHONE OS6

FUENTE: http://www.applesfera.com/ios/la-evolucion-de-ios-desde-2007-hasta-la-actualidad-especial-historia-wwdc

3.3.3.7. IOS 7 (Septiembre 2013 para IPhone 5)

Esta es la última versión lanzada al mercado por Apple en el cual el desbloqueo del equipo se lo hará mediante huella dactilar, los equipos que se podrán actualizar son los que van desde IPhone 4, IPad 2 e IPod Touch de quinta generación y modelos superiores, así como IPad mini [28].

Entre las nuevas características de la versión final de IOS 7 también están las nuevas voces para Siri y nuevos tonos de llamada.

Esta nueva versión supone un cambio visual y organizativo y según confirmó el vicepresidente de ingeniería de software de Apple, Craig Federighi, IOS 7 también contará con nuevos y rediseñados tonos de llamada para el IPhone.

El nuevo sistema tendrá mayor simplicidad visual en IOS 7: la interfaz de usuario tiene un diseño "plano", un estilo que ya ofrece Windows Phone, nuevos iconos y una nueva tipografía, anunciaron sus representantes.

Deslizando el dedo hacia la parte inferior de la pantalla, los usuarios irán a una pantalla de ajustes frecuentes, entre los que se incluyen la selección del modo avión, la gestión de la conexión Wi-fi y de la música, el brillo de pantalla, el reloj, la cámara, la calculadora y la linterna, según publica EFE [29].

La figura III.12 muestra cómo se dio la transición entre IOS 6 e IOS 7:

Figura III. 9 IPHONE OS7

FUENTE: http://elmashimo.com/2013/06/12/esta-es-la-diferencia-entre-los-iconos-de-ios-6-vs-ios-7/

3.4. PLATAFORMA BLACKBERRY

BlackBerry OS es una plataforma desarrollada por la empresa RIM para sus dispositivos BlackBerry. Este sistema entre sus principales funciones es multitarea y tiene soporte para diferentes métodos adoptados por RIM para su uso en computadoras de mano, particularmente la trackwheel, trackball, touchpad y pantallas táctiles.

Su historia se remonta la aparición de los primeros handheld en 1999. Estos dispositivos tenían 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 [30].

3.4.1. HISTORIA

El éxito obtenido en los últimos meses por BlackBerry es algo relativamente reciente, sin embargo estos dispositivos llevan en el mercado desde 1999.

Un BlackBerry como se lo conoce actualmente es un dispositivo portátil inalámbrico que admite correo electrónico, telefonía móvil, SMS, navegación web y otros servicios de información inalámbricos. Sus creadores son la compañía canadiense, Research In Motion (RIM), los cuales transportan la información a través de las redes de datos inalámbricas de empresas de telefonía móvil.

En mayo de 2005, BlackBerry tenía 5 millones de usuarios, el índice de crecimiento era cada vez mayor, lo que se ha confirmado y superado en los últimos dos años, en los que RIM ha añadido otros 9 millones de abonados. En la actualidad BlackBerry tiene alrededor de 14 millones de abonados. [31]

3.4.2. CARACTERÍSTICAS

El SO de BlackBerry está muy orientado a su uso profesional como gestor de correo electrónico y agenda. A partir de la versión 4 es posible sincronizar el dispositivo con el correo electrónico, el calendario, tareas, notas y contactos de

Microsoft Exchange Server, siendo además compatible con Lotus Notes y Novell GroupWise.

BES (BES) proporciona el acceso y organización del email a grandes compañías identificando a cada usuario con un único Blackberry. Para usuarios pequeños se presenta Blackberry Internet Service, el cual es un programa más sencillo que proporciona acceso a Internet y a correo POP3 / IMAP / OWA sin tener que usar la versión corporativa [32].

3.4.3. HISTORIA DE LOS ÚLTIMOS MODELOS BLACKBERRY

3.4.3.1. BLACKBERRY CURVE SERIES

Dispositivos fabricado por RIM desde 2007, famosos por ser llamados los de gama media orientados al consumidor en nivel de entrada estos teléfonos son la línea más popular de BlackBerry que ahora de ser llamados gama media están pasando a ser gama alta con sus últimos modelos que reinventan a la línea curve como lo son el BlackBerry Curve 9380 el primero en esta línea en ser totalmente táctil y el BlackBerry Curve 9360 el primer celular Curve en incluir la cámara hasta ahora más potente de la línea Curve (5 MP) con Flash LED incluido y agregar el agradable iluminado en el marco del track pad sin quitar el clásico pero adorado teclado físico QWERTY, así que si de beneficios se tratase podríamos concluir que el Curve 9360 es el más avanzado de la línea Curve.

La figura III.17 muestra el BlackBerry Curve:

Figura III. 10 BLACKBERRY CURVE

FUENTE: http://www.bbscnw.com/blackberry-curve-series.php

3.4.3.2. BLACKBERRY BOLD SERIES

Es un teléfono de tamaño grande el cual trae ventajas y una de ellas tener una pantalla grande en él. Esta es un área donde el Bold realmente brilla. Tiene probablemente la mejor pantalla de un teléfono inteligente que nos hemos encontrado. Es de alta resolución con colores que son crujientes. Al ver el vídeo en este teléfono justo al lado de uno de sus competidores que realmente se note la diferencia en la calidad de la imagen.

La negrita viene con el nuevo sistema operativo de BlackBerry, que es una gran mejora con respecto a la anterior. Es mucho más fácil para navegar con la interfaz y también es mucho mejor. Las funciones multimedia son excelentes..

La figura III.18 muestra el BlackBerry Bold:

Figura III. 11 BLACKBERRY BOLD

FUENTE: http://www.bbscnw.com/blackberry-curve-series.php

3.4.3.3. BLACKBERRY TORCH SERIES

El BlackBerry torch representa un nuevo diseño en los teléfonos inteligentes de la compañía, es su primer teléfono deslizable. Aparentemente es la forma en que tienen la intención de ir en el futuro lo que esperamos ver más teléfonos con diseños similares. La antorcha es un teléfono bastante grande en comparación con sus competidores, y que está claramente diseñado para mirar apropiado para el profesional y no tener el aspecto elegante que la mayoría de los consumidores quieren negocio. Una gran parte de la razón de ello fue la

decisión de incluir un teclado QWERTY completo que los usuarios esperan en un BlackBerry, esto requiere que el teléfono sea bastante amplio.

El BlackBerry Torch es el primer producto en utilizar el nuevo sistema operativo de la compañía. Es una gran mejora sobre el viejo ser más fácil navegar. Todas las otras características que usted esperaría encontrar son, por supuesto, como el correo electrónico, mensajería de prueba, y GPS. Hay un buen número de características avanzadas de este teléfono, pero una cosa que nos encontramos fue que el número de aplicaciones que se pueden utilizar es un poco limitado en comparación con otros teléfonos inteligentes. [32]

La figura III.19 muestra el BlackBerry Curve:

Figura III. 12 BLACKBERRY TORCH

FUENTE: http://www.bbscnw.com/blackberry-curve-series.php

3.5. COMPARACIÓN ENTRE PLATAFORMAS

En cuanto a las tres plataformas se ha visto que cada cual tiene sus ventajas y desventajas entre sí, para escoger el modelo adecuado se debería evaluar funcionalidades que se desea tener. A continuación se muestra una tabla en donde se observa una comparación un poco detallada entre estas tres plataformas.

3.5.1. TABLA DE COMPARACIÓN ENTRE PLATAFORMAS POR SUS CARACTERÍSTICAS

La FIGURA III.20 muestra una comparación entre las plataformas celulares en cuanto a sus características: [33].

	Apple iOS 7	Android 4.3	Windows Phone 8	BlackBerry OS 7	Symbian 9.5
Compañía	Apple	Open Handset Alliance	Microsoft	RIM	Symbian Foundation
Núcleo del SO	Mac OS X	Linux	Windows NT	Mobile OS	Mobile OS
Licencia de *software*	Propietaria	Software libre y abierto	Propietaria	Propietaria	Software libre
Año de lanzamiento	2007	2008	2010	2003	1997
Fabricante único	Sí	No	No	Sí	No
Variedad de dispositivos	modelo único	muy alta	media	baja	muy alta
Soporte memoria externa	No	Sí	Sí	Sí	Sí
Motor del navegador web	WebKit	WebKit	Pocket Internet Explorer	WebKit	WebKit
Soporte Flash	No	Sí	No	Si	Sí
HTML5	Sí	Sí	Sí	Sí	No
Tienda de aplicaciones	App Store	Google Play	Windows Marketplace	BlackBerry App World	Ovi Store
Número de aplicaciones	825.000	850.000	160.000	100.000	70.000
Coste publicar	$99 / año	$25 una vez	$99 / año	sin coste	$1 una vez
Actualizaciones automáticas del S.O.	Sí	depende del fabricante	depende del fabricante	Sí	Sí
Familia CPU soportada	ARM	ARM, MIPS, Power, x86	ARM	ARM	ARM
Máquina virtual	No	Dalvik	.net	Java	No
Aplicaciones nativas	Siempre	Sí	Sí	No	Siempre
Lenguaje de programación	Objective-C, C++	Java, C++	C#, muchos	Java	C++
Plataforma de desarrollo	Mac	Windows, Mac, Linux	Windows	Windows, Mac	Windows, Mac, Linux

FIGURA III. 13COMPARACIÓN PLATAFORMAS EXISTENTES POR SUS CARACTERÍSTICAS

FUENTE: http://www.androidcurso.com/index.php/tutoriales-android/31-unidad-1-vision-general-y-entorno-de-desarrollo/98-comparativa-con-otras-plataformas

3.5.2. TABLA DE COMPARACIÓN ENTRE PLATAFORMAS POR SU CUOTA EN EL MERCADO

La figura III.21 muestra una comparación entre las plataformas celulares en cuanto a la cuota en el mercado: [33].

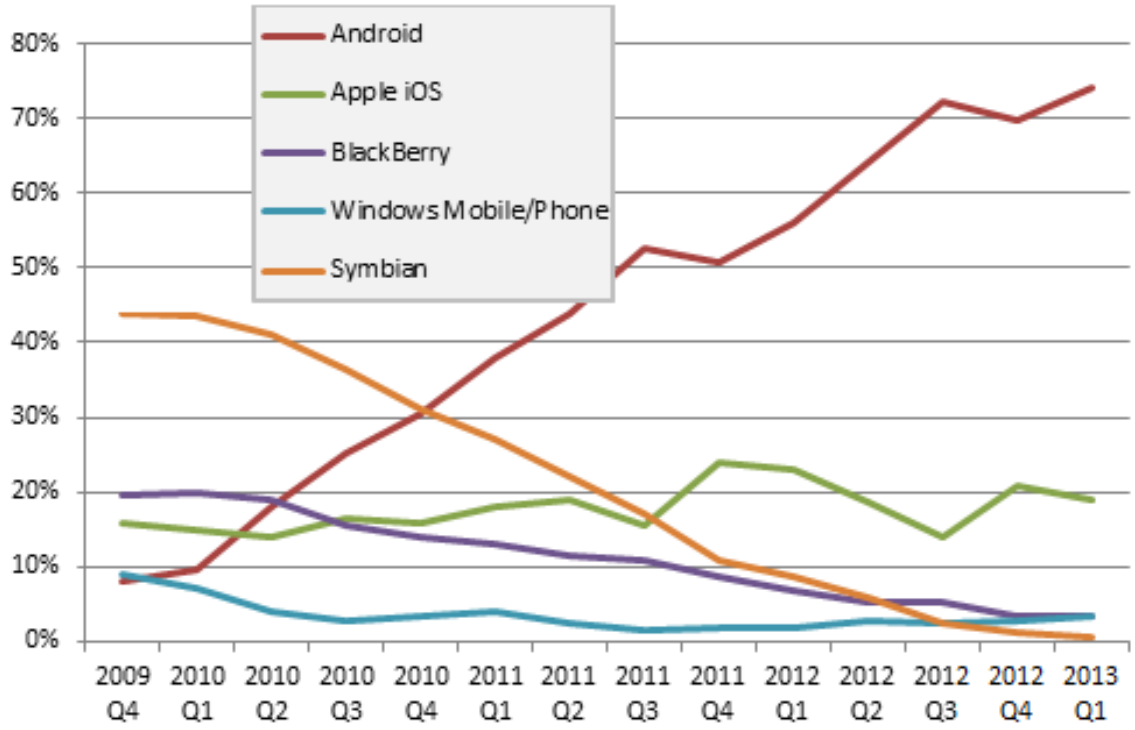


Figura III. 14 PLATAFORMAS POR CUOTA EN EL MERCADO

FUENTE: http://www.androidcurso.com/index.php/tutoriales-android/31-unidad-1-vision-general-y-entorno-de-desarrollo/98-comparativa-con-otras-plataformas

CAPÍTULO IV

SOLUCIONES CORPORATIVAS DE BLACKBERRY

4.1. INTRODUCCIÓN

En este capítulo se explica cómo BlackBerry ha introducido en el mercado varias soluciones para los clientes corporativos, las cuales ayudan a la administración tanto de la empresa como del personal.

BlackBerry tiene su solución óptima que es BES o comúnmente conocido como BES la cual en principio permitió administrar dispositivos BlackBerry, evolucionando hasta lograr una nueva solución llamada BES10 o BDS en la cual BlackBerry ha permitido incluir en la administración otras plataformas como Android e IOS.

4.2. MOVILIDAD EMPRESARIAL

Hoy en día, las empresas han cambiado en una forma radical sus maneras de hacer negocio. Esto llega a planear un desarrollo de procesos y planes tecnológicos en un corto. Mediano y largo plazo. Los cuales permitan optimizar recursos y tiempo, mejorando así la eficiencia en las corporaciones.

Para una empresa la necesidad de desarrollar su mercado móvil es de gran importancia ya que la movilidad empresarial promete aumentar la productividad, un servicio al cliente más eficaz y una ventaja competitiva más elevada, gracias a la capacidad de trabajar, comunicarse y colaborar desde cualquier lugar.

Esta necesidad lleva a buscar unas políticas robustas y transigentes que tengan como fin atraer los recursos humanos en forma más dinámica, logrando así un equilibrio entre trabajo y calidad de vida. Esto se debe, principalmente, a que cada vez son más las actividades productivas que se pueden realizar a distancia.

Con esta necesidad de movilidad se encuentran muchos riesgos;

El primero y el más importante es la seguridad, ya que se debe lograr que los dispositivos accedan a la red sin poner en peligro la información crítica de la empresa y por otro lado, debe buscar la manera de no perder la información o en tal caso protegerla de terceros.

Otro punto a tomar en cuenta en este entorno es que la red debe estar en la capacidad de soportar todo este tráfico, y debe, presentar seguridad hacia los clientes potenciales.

La movilidad mejora a las empresas en temas de competitividad, comunicación, eficiencia, y seguridad, ya que también significa empleados mejor capacitados y naturalmente con mejor desempeño profesional [34].

La figura IV.1 muestra un bosquejo de la movilidad empresarial:

FIGURA IV. **1** **MOVILIDAD EMPRESARIAL**

FUENTE: http://www.bbscnw.com/BlackBerryOS10.php

4.2.1. Aspectos a considerar en un modelo de desarrollo para movilidad empresarial

- Definir el perfil de usuario más adecuado de movilidad.
- Establecer un objetivo y dar prioridad a los pasos para la movilidad empresarial.
- Definir una estrategia para obtener una mayor productividad de los empleados.
- Cuantificar los ahorros de costos operativos.
- Roadmap para incrementar la agilidad estratégica organizacional dentro de un entorno competitivo.
- Asegurar que todos los beneficios potenciales de la movilidad se implementarán.
- Consolidar una única visión de la movilidad empresarial [35].

4.2.2. TENDENCIAS

De acuerdo con un estudio de la asociación europea, Group Speciale Mobile (GSM), el sector móvil mueve alrededor de un billón de dólares cada año, cifra que representa el 1.4% del PIB mundial. Para 2018 –detalla el informe– se

estima que la inclusión de dispositivos móviles supere la barrera de 4,000 millones de unidades en todo el orbe.

Las iniciativas de movilidad consumirán aproximadamente el 20% de los presupuestos de TI en 2014; 17% en 2012, según Cisco Systems.

Conforme los productos y servicios de Movilidad Empresarial avanzan a través del ciclo de vida de sus mercados, surgen innovación y oportunidades para optimizar costos.

Según Mayan Mathen, jefe de Tecnología de Dimension Data para Medio Oriente y África, “Las empresas necesitan tener acceso a la información en tiempo real para tomar decisiones y estar un paso delante de su competencia. La información es poder y hoy la información vuela cada vez más rápido a través de la red” [35].

- **Publico en Movimiento**

Los usuarios de esta era ya no están estáticos, cada vez hay más canales de comunicación en donde se convierte en un reto logar la unificación de estos. Satisfacer las demandas de un público que cada día exige mayor inmediatez y calidad, es la razón para desarrollar estas soluciones que se presentan como una de las principales opciones en el mercado tecnológico [34].

Ha llegado el momento de aplicar la movilidad a la empresa. Según IDC, en 2013, más de 1.190 millones de empleados de todo el mundo utilizarán la tecnología móvil, lo que representa un 34,9% de la población activa.*

El impacto de la movilidad en las empresas es evidente. Cada vez más, se espera que los trabajadores de una empresa gestionen tareas de vital importancia y tomen decisiones en tiempo real, independientemente de donde se encuentren. [36]

En esta búsqueda de la protección de las inversiones tecnológicas, BlackBerry ha desarrollado una plataforma que nos brinda la facilidad de una administración de usuarios corporativos en busca de la movilidad empresarial,

manejando en su mayoría el tema de seguridad que hasta la actualidad era la mayor preocupación de las empresas, además nos permite la unificación con otras dos grandes plataformas como son IOS y Android. [36]

4.3. BlackBerry Enterprise Server 10

Conocido con las siglas BES 10. Es una aplicación que proporciona una solución integral de administración de dispositivos móviles, y de administración de aplicaciones, así como, las características de seguridad que la empresa necesita para administrar todos los Smartphone BlackBerry, tabletas BlackBerry PlayBook, dispositivos IOS y dispositivos Android. Sea cual sea el dispositivo, modelo, aplicación o entorno operativo, BES 10 equilibra las necesidades del usuario y la empresa manteniendo el ritmo óptimo de ella.
La plataforma BES 10 maneja tres componentes en su desarrollo óptimo, las cuales nos permiten interactuar entre aplicaciones sin importar la plataforma bajo la cual se desarrolle en Smartphone. Estas son

- BDS
- UDS
- BlackBerry Managment Studio [38].

4.3.1. CARACTERÍSTICAS DE BES 10

- Gestión de la mayoría de dispositivos:
- Simple, interfaz unificada:
- Experiencia confiable y segura:
- Balanceo entre trabajo y necesidades personales:

.

Otros elementos de seguridad están disponibles en función del tipo de dispositivo.

4.3.2. CARACTERÍSTICAS DEL MANEJO DE LOS DISPOSITIVOS

- Administración basada en navegador
- Activado de dispositivos
- Administracion de dispositivos
- Gestión de grupos de usuarios
- Control de acceso a Microsoft ActiveSync
- Ver informes de usuario e información del dispositivo
- Administrar licencias para características específicas y controles del dispositivo

4.3.3. ARQUITECTURA BES 10

La figura IV.2 muestra la arquitectura en la que se basa BES 10

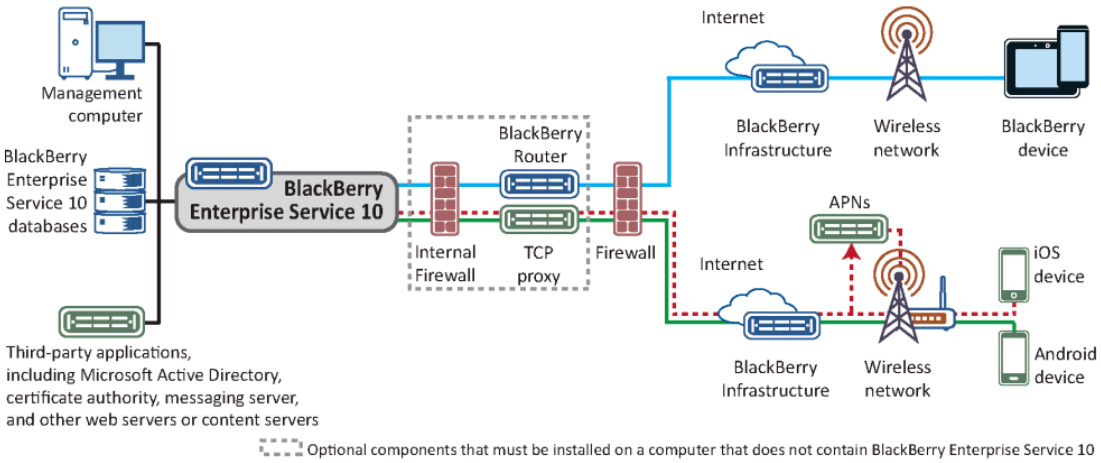


Figura IV. 2 ARQUITECTURA BES 10

FUENTE:
http://docs.BlackBerry.com/%20BLACKBERRY%20DEVICE%20SERVICE%20ADVANCED%20ADMINISTRATION%20GUIDE.PDF

- **BES 10**

Es el conjunto de servicios que se utiliza para gestionar los dispositivos en un ambiente multiplataforma.

- **BES 10 databases**

Las bases de datos de BES 10 son un conjunto relacionales de las mismas, que contienen información de la cuenta de usuario y configuración.
Estas bases de datos son las siguientes:

- **BlackBerry Configuration Database:** Contiene datos utilizados para la gestión de BlackBerry 10 y los dispositivos BlackBerry PlayBook
- **Managment Database:** contiene información utilizada para la gestión de dispositivos IOS y Android.

- **Microsoft Active Directory**

La información de la cuenta de usuario se obtiene de Microsoft Active Directory, esta información es necesaria para crear cuentas de usuario [38].

4.3.4. COMPONENTES BES 10

4.3.4.1. BDS

La solución BDS consta de varios componentes y características que amplían los métodos de comunicación de la empresa a los dispositivos BlackBerry. La misma solución protege los datos que están en tránsito en todos los puntos entre el dispositivo y BDS.

Para proteger los datos en tránsito a través de Wi-Fi y las redes móviles, BDS y el dispositivo, utilizan criptografía de clave simétrica para cifrar los datos enviados entre ellos. La solución BDS está diseñada para impedir que terceros, incluidos los proveedores de servicios inalámbricos, accedan a información potencialmente confidencial de su empresa en un formato descifrado.

La solución BDS utiliza la confidencialidad, integridad y autenticidad para ayudar a proteger su organización contra la pérdida o alteración de datos garantizando confianza en la seguridad de los productos BlackBerry [39].
La tabla IV.I muestra los principios sobre los que trabaja BDS:

PRINCIPIOS	DESCRIPCION
Confidencialidad	La solución BDS utiliza criptografía de clave simétrica, para asegurarse que solo los beneficiarios puedan ver el contenido de mensajes de correo electrónico. [39].
Integridad	La solución BDS utiliza la criptografía de clave simétrica para proteger a todos los mensajes de correo electrónico que envía el dispositivo y evita que terceros descifren o alteren los datos del mensaje. Sólo el servicio de BlackBerry Device y el dispositivo conocen el valor de las claves que utilizan para cifrar mensajes y reconocen el formato de un mensaje descifrado y descomprimido. El BDS o el dispositivo rechazan automáticamente un mensaje si no está cifrado con claves que reconozcan como válidas. [39].
Autenticación	Antes de que el servicio de BlackBerry Device envíe los datos al dispositivo, el dispositivo se autentica con el BDS para demostrar que el dispositivo conoce la clave de transporte utilizada para cifrar los datos. La solución BDS evita que los dispositivos falsificados intenten autentificarse con la base de datos. [39].

TABLA IV. IPRINCIPIOS BDS

FUENTE: http://www.bbscnw.com/BlackBerry-curve-series.php

4.3.4.1.1. Características de Seguridad de los dispositivos

La tabla IV.II muestra las características sobre del entorno BDS:

CARACTERISTICA	DESCRIPCION
Protección de los datos entre BDS y los dispositivos	El BDS protege los datos que están en tránsito entre el mismo y un dispositivo. Los dos pueden comunicarse mediante el cifrado de capa de transporte (utilizando AES-256) y TLS. [39].

Protección de los datos empresariales en los dispositivos	El dispositivo protege los datos de trabajo utilizando cifrado XTS-AES-256. Los dispositivos BlackBerry Balance aíslan el entorno personal del entorno corporativo. [39].
Protección de datos personales en los dispositivos	Se puede utilizar una regla de política de TI para requerir que un dispositivo BlackBerry Balance cifre los datos almacenados en el sistema de archivos personales. El dispositivo protege los datos personales mediante cifrado XTS-AES-256. [39].
Control de acceso a los dispositivos de red de la empresa	BDS permite conectar dispositivos a la empresa mediante Wi-Fi o VPN. [39].
Control del comportamiento de un dispositivo	Para controlar el comportamiento de un dispositivo, se puede: • Enviar comandos de administración para bloquear el dispositivo, eliminar permanentemente los datos del trabajo, eliminar permanentemente los datos de usuario y datos de la aplicación, y devolver la configuración del dispositivo. • Enviar una política de TI a un dispositivo para cambiar la configuración de seguridad. Puede utilizar la política de TI para imponer la contraseña del dispositivo en un dispositivo BlackBerry. [39].
Protección de los datos del usuario	El dispositivo permite a un usuario eliminar toda la información y los datos desde la memoria del dispositivo. [39].
Protección BlackBerry OS 10 y BlackBerry PlayBook OS	Cuando se inicia un dispositivo, se completa las pruebas de integridad para detectar daños en el núcleo. BlackBerry 10 OS y PlayBook OS pueden reiniciar un proceso que deja de responder sin afectar negativamente a otros procesos. BlackBerry 10 OS y PlayBook OS validan las solicitudes que las aplicaciones hacen de los recursos en el

	dispositivo. [39].
Protección de datos de las aplicaciones que utilizan sandboxing	El BlackBerry 10 OS y PlayBook OS utilizan sandboxing para separar y restringir las capacidades y los permisos de las aplicaciones que se ejecutan en el dispositivo. Cada proceso de aplicación se ejecuta en su propio entorno. El BlackBerry 10 OS y PlayBook OS evalúan las peticiones de los procesos y manejan su memoria. [39].
Protección de recursos	El BlackBerry 10 OS y PlayBook OS utilizan particiones adaptables para asignar los recursos que no son utilizados por las aplicaciones en condiciones de funcionamiento típicas, y para asegurarse de que los recursos están disponibles para aplicaciones en su funcionamiento máximo. [39].
Gestión de permisos de acceso	El BlackBerry 10 OS y PlayBook OS evalúan cada petición que hace de una aplicación para acceder a una capacidad en el dispositivo. [39].
Verificación del código ROM de arranque	El dispositivo verifica que el código ROM pueda ejecutarse.[39].

TABLA IV. II CARACTERÍSTICAS DE SEGURIDAD BDS

FUENTE:
http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.3.4.1.2. ARQUITECTURA BDS

La figura IV.3 bosqueja la arquitectura de BDS:

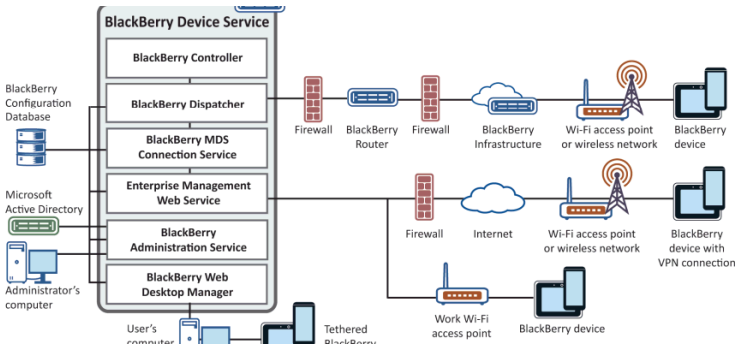


FIGURA IV. 3 ARQUITECTURA BDS

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_

La tabla IV.III indica las componentes presentes en la arquitectura BDS:

COMPONENTES	DESCRIPCION
BAS(BAS)	BAS gestiona BDS mediante las cuentas de usuario y dispositivos que se asocian con él. Se puede administrar cuentas de usuario y asignar grupos, funciones administrativas, configuraciones de software, perfiles de correo electrónico, y las políticas de TI a cuentas de usuario. Se puede actualizar la información del usuario en Microsoft AD y sincronizar la información del usuario de forma manual. [40].
BlackBerry Configuration Database	BlackBerry Configuration Database es una base de datos relacional que contiene información de cuentas de usuario e información de configuración (por ejemplo, detalles de conexión) que los componentes de BDS utilizan. [40].
BlackBerry Controller	BlackBerry Controller controla los componentes de BDS y los reinicia si deja de responder. [40].
BlackBerry Infraestructure	La infraestructura de BlackBerry valida la información de SRP y controla el tráfico que viaja fuera del firewall de la organización y de los dispositivos BlackBerry. [40].
BlackBerry Dispatcher	BlackBerry Dispatcher mantiene una conexión SRP con BlackBerry Infraestructure a través de Internet. BlackBerry Dispatcher se encarga de comprimir, cifrar, descifrar y descomprimir los datos que viajan a través de Internet hacia y desde los dispositivos. [40].
BlackBerry MDS Connection	BlackBerry MDS Connection Service

Service	proporciona una conexión segura entre el agente de gestión de los dispositivos en la empresa y el Servicio Web de la empresa, en BDS. La conexión se utiliza cuando el dispositivo no está conectado a la red Wi-Fi de su empresa o VPN. [40].
BlackBerry Router	BlackBerry Router se conecta a la infraestructura de BlackBerry, que envía los datos a las redes móviles o hacia Internet. [40].
BlackBerry Web Desktop Manager	BlackBerry Web Desktop Manager es una aplicación web que permite a los usuarios activar y administrar dispositivos. [40].
Enterprise Management Web Service	Enterprise Management Web Service es un conjunto de servicios web que comunica por comandos, información de configuración, las políticas de TI, perfiles VPN, perfiles Wi-Fi y los perfiles de correo electrónico entre BAS y el Agente de gestión de empresa en los dispositivos. [40].
Microsoft Active Directory	BAS obtiene información de cuentas de usuario de Microsoft Active Directory requieridas para crear cuentas de usuario en BDS. [40].

TABLA IV. III COMPONENTES BDS

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.3.4.1.3. Autenticación entre BAS y BlackBerry Infraestructure

BlackBerry Infraestructure y BDS deben autenticarse entre sí antes de que puedan transferir datos. BDS utiliza SRP para autenticarse y conectarse a BlackBerry Infraestructure. SRP es un protocolo punto a punto que se ejecuta a través de TCP / IP. El BDS utiliza SRP en contacto con BlackBerry Infraestructure para abrir una conexión. Cuando BDS y BlackBerry Infraestructure abren una conexión, se pueden realizar las siguientes acciones:

- Autenticar con los demás

- Información de configuración de Exchange
- Enviar y recibir datos

El BDS y BlackBerry Infraestructure utilizan la clave de autenticación SRP cuando se autentican entre sí. La clave de autenticación SRP es una clave de cifrado de 20 bytes que BDS y BlackBerry Infraestructure accionan.

Después que se abre una conexión inicial a través de Internet, BDS envía un paquete de información básica a BlackBerry Infraestructure inmediatamente. Un paquete de información básica incluye la información sobre la versión de BDS, identificadores de SRP, y otra información que se requiere para abrir una conexión SRP. Tanto BDS como BlackBerry Infraestructure pueden reconocer el paquete de información básica. BDS y BlackBerry Infraestructure pueden utilizar este paquete para configurar los parámetros de la implementación SRP. [40]

4.3.4.1.4. Protección de la conexión TCP/IP

Después que BDS y BlackBerry Infraestructure abren una conexión SRP, BDS utiliza una dirección TCP / IP persistente para enviar datos a BlackBerry Infraestructure.

La conexión TCP / IP entre BDS y BlackBerry Infraestructure es segura ya que BDS y el dispositivo cifran los datos que se envían entre sí. No hay punto intermedio, descifra y cifra los datos de nuevo.

Una vez iniciado el proceso de activación, no hay tráfico de datos de ningún tipo entre BDS y el dispositivo activado, a menos que el BDS pueda descifrar los datos utilizando una clave valida. Sólo BDS y el dispositivo tienen la clave correcta.

Se debe configurar el firewall de la organización o un servidor proxy para permitir que BDS inicie y mantenga una conexión de salida a BlackBerry Infraestructure a través del puerto TCP 3101 [40].

4.3.4.1.5. Forma de conectar los dispositivos

Los dispositivos pueden conectarse a BDS y acceder a la red de su empresa mediante una serie de métodos de comunicación. Por defecto, los dispositivos intentan conectarse a la red de su empresa mediante los siguientes métodos de comunicación:

Perfiles VPN configurados

Perfiles Wi-Fi configurados

Infraestructura BlackBerry

Perfiles VPN y Wi-Fi personales que el usuario configura en el dispositivo.

La figura IV.4 indica cómo se da cada una de las formas de conexión en BDS:

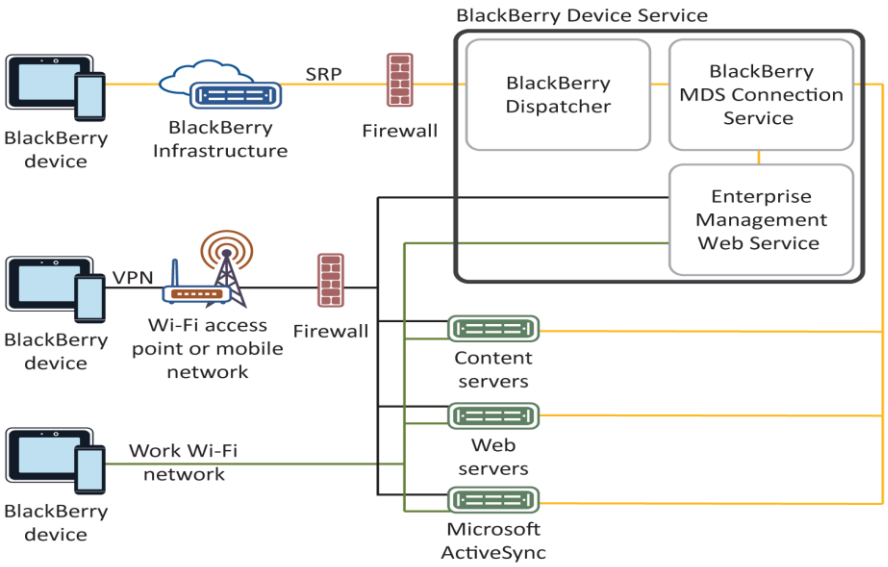


FIGURA IV. 4 FORMAS DE CONEXIÓN DE LOS DISPOSITIVOS EN BDS

FUENTE:
http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.3.4.1.6. Tipos de cifrado que utilizan los dispositivos cuando se conectan a los recursos una organización

La tabla IV.IV muestra los tipos de encriptación que maneja los dispositivos al conectarse en BDS:

TIPO DE ENCRIPTACION	DESCRIPCION
Encriptación Wi-Fi (IEEE 802.11)	Cifra los datos que se envían entre el dispositivo y el punto de acceso inalámbrico, si el punto de acceso inalámbrico fue configurado para utilizar cifrado Wi-Fi. [40].
Encriptación VPN	Cifra los datos que se envían entre el dispositivo y el servidor VPN. [40].
Encriptación TLS	Cifra los datos que se envían entre el dispositivo y BlackBerry Infraestructure. Cifra los datos que se envían entre el dispositivo y BDS. Este tipo de cifrado utiliza un certificado de cliente / servidor. [40].
Encriptación SSL/TLS	Cifra los datos que se envían entre el dispositivo y el servidor, el servidor web o servidor de mensajería que utiliza Microsoft ActiveSync. El cifrado para esta conexión debe configurarse por separado en cada servidor y utiliza un certificado por separado con cada servidor. El servidor puede utilizar SSL o TLS, según cómo esté configurado. [40].
Encriptación AES	Cifra los datos que se envían entre el dispositivo y BDS. Este tipo de cifrado utiliza la clave de transporte del dispositivo. [40].

TABLA IV. IV COMPONENTES BDS

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.3.4.2. UDS

La consola de UDS, también conocido como la consola de administración, proporciona una interfaz basada en Web que se utiliza para administrar las cuentas de usuario, las políticas de TI, perfiles, aplicaciones y dispositivos IOS y Android. Los siguientes son los principales puertos que utiliza la consola de UDS [40].

La siguiente tabla IV.V muestra los tipos de conexión y puertos que utiliza UDS:

UDS	Tipo de Conexión	Puerto por defecto	Donde configurar
Conexión de salida de la consola de administración de la infraestructura de BlackBerry para solicitar una CSR firmado por Research In Motion al configurar el certificado APN	HTTPS	443	--------
Conexiones salientes a la Base de Datos	TCP	1433	Herramienta de configuración BES 10
Conexión entrante y saliente entre los navegadores y la consola de UDS	HTTPS Y HTTP	6443 9440	----------

TABLA IV. V CONEXIONES Y PUERTOS UDS

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.3.4.2.1. CORE

El CORE es un módulo independiente del dispositivo que se instala detrás del firewall de la organización. Realiza las siguientes funciones:

- Gestiona todos los datos que se utilizan para administrar los dispositivos IOS y Android (por ejemplo, la configuración del usuario, grupo de

configuración, la configuración del dispositivo, los controles de aplicación de políticas, y así sucesivamente) y lo almacena en la Base de Datos. El Core es el único componente que accede a la base de datos de gestión.

- El Core se conecta a los siguientes componentes externos:
  - Microsoft Active Directory: utilizando LDAP, para recuperar información de la cuenta de usuario en que BES 10 tiene que buscar y crear cuentas de usuario.
  - APN: para informar a los dispositivos IOS en contacto con el módulo, cuando la configuración asignada al dispositivo se actualiza (por ejemplo, actualización de política de TI o del perfil VPN que se aplica a la misma).
  - Servidor de correo a través de SMTP, para enviar mensajes de correo electrónico de activación e incumplimiento de política.
  - Servidor de base de datos: utilizando ADO.NET, para hacer las conexiones de base de datos y ejecutar consultas o comandos.
  - Servidor SCEP, usando HTTP, para obtener un código de desafío, el dispositivo puede utilizar para la inscripción de certificados.

4.3.4.2.1.1. Puertos

La siguiente tabla IV.VI muestra los puertos que se deben habilitar para el funcionamiento del CORE de UDS:

CORE	Tipo de conexión	Puerto por defecto
Conexiones salientes del módulo	HTTP HTTPS	80 443
Conexión de salida a BlackBerry Secure Connect Service para enviar notificaciones APNs	HTTP	2195

Conexiones entrantes y salientes al módulo de comunicación, Programador y BlackBerry Web Services	HTTPS	9081
Conexiones entrantes y salientes a BlackBerry Secure Connect Service	HTTPS	38081

TABLA IV. VI PUERTOS DEL CORE DE UDS

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.3.4.2.2. Módulo de Comunicación

El módulo de comunicación es una puerta de enlace entre los dispositivos IOS, y Android hacia BES 10. Es responsable de la conversión de los protocolos soportados en los dispositivos hacia el dispositivo utilizado por el Core. El módulo de comunicación debe ser accesible desde cualquier red Wi-Fi utilizada por los dispositivos IOS y Android.

4.3.4.2.2.1. Puertos

La siguiente tabla IV.VII muestra los puertos que se deben habilitar para el funcionamiento del Módulo de Comunicación de UDS:

MODULO DE COMUNICACION	Tipo de conexión	Puerto por defecto
Conexiones entrantes y salientes al Core	HTTPS	9081
Conexiones entrantes y salientes a BlackBerry Secure Connect Service	HTTPS	33443

TABLA IV. VII PUERTOS MÓDULO DE COMUNICACIÓN UDS

FUENTE:
http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.3.4.2.3. BlackBerry Secure Connect Service

Es un servicio web responsable de proporcionar conectividad a los dispositivos IOS y Android desde detrás del firewall. Elimina la necesidad de abrir varios puertos de entrada a BES 10 y permite a todos los dispositivos IOS y Android gestionar la comunicación.

4.3.4.2.3.1. Puertos

La siguiente tabla IV.VIII muestra los puertos que se deben habilitar para el funcionamiento de BlackBerry Secure Connect de UDS:

BLACKBERRY SECURE CONNECT SERVICE	Tipo de conexión	Puerto por defecto
BlackBerry Infraestructure	TCP	3101
Conexiones entrantes y salientes al Módulo de comunicación	HTTPS	33443
Conexiones entrantes y salientes al Core	HTTPS	380881

TABLA IV. VIII PUERTOS BLACKBERRY SECURE CONNECT DE UDS

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722

4.3.4.2.4. APN

APN es un servicio para dispositivos IOS proporcionadas por Apple, que BES 10 utiliza para comunicar a los dispositivos IOS con el módulo de comunicación para actualizar la configuración (tales como Wi-Fi perfil, perfil VPN, o actualizaciones de perfiles de Microsoft ActiveSync) y suministrar información para el inventario de los dispositivos de la organización.

4.3.4.2.4.1. Puertos

La siguiente tabla IV.IX muestra los puertos que se deben habilitar para el funcionamiento de los APN de UDS:

APN	Tipo de conexión	Puerto por defecto
Conexiones salientes de dispositivos IOS que utilizan una red Wi-Fi hacia una APN	TCP	5223
Conexiones salientes al Core	HTTPS	9081

TABLA IV. IX PUERTOS APN UDS

FUENTE:
http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.3.5. DIFERENCIACIÓN ENTRE DATOS CORPORATIVOS Y DATOS EMPRESARIALES

4.3.5.1. BLACKBERRY BALANCE

La siguiente figura IV.5 muestra un gráfico de la conexión mediante la cual BlackBerry Balance diferencia los datos personales de los datos de trabajo:

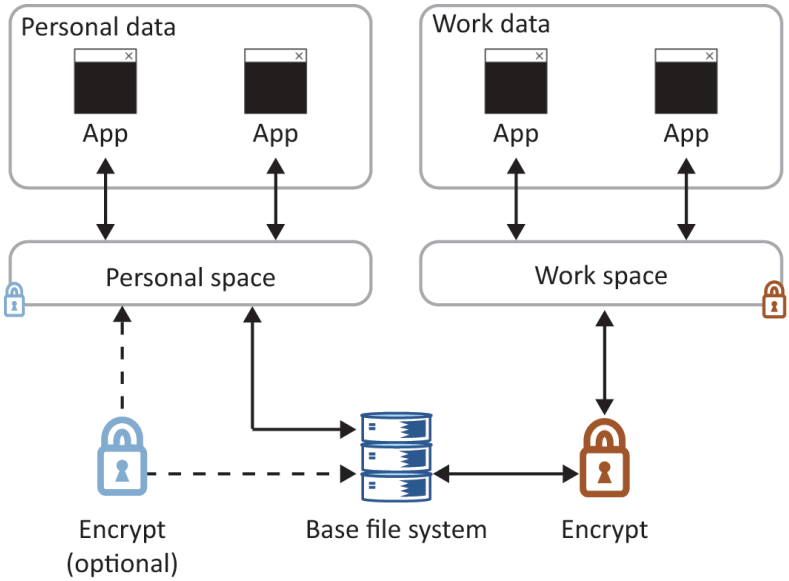


FIGURA IV. 5 BLACKBERRY BALANCE

FUENTE:
http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

La organización mediante la tecnología BlackBerry Balance permite a los usuarios utilizar un dispositivo para el trabajo y uso personal. Por ejemplo, la empresa puede permitir que los usuarios activen sus dispositivos personales en la misma, sin dejar de ser un dispositivo de uso personal, en el cual se manejen dos entornos, el personal y el laboral.

Las características de BDS junto con la de BlackBerry Balance pueden controlar los dispositivos a través de la protección de contenidos y recursos (datos, aplicaciones y conexiones de red) de la organización así como permiten un diferente manejo entre los datos y aplicaciones de la compañía en relación a los datos y aplicaciones personales. Estas características tienen los siguientes beneficios:

- Permitir a la organización, controlar el acceso a los datos y aplicaciones de la empresa en los dispositivos.
- Ayudar a evitar que los datos de su organización sean comprometidos hacia medios externos.
- Proporcionar una experiencia unificada para los usuarios cuando acceden a datos personales y de trabajo dentro de algunas aplicaciones básicas.
- Permitir instalar y administrar aplicaciones de la empresa en los dispositivos.
- Permitir un borrado de datos empresariales y las aplicaciones personales que de los usuarios que ya no forman parte de la organización
- Permitir a los administradores controlar las conexiones de red para el trabajo y las aplicaciones personales [41].

BlackBerry Balance está diseñado para el trabajo independiente ya que utiliza áreas separadas del dispositivo llamadas espacios de separación entre trabajo y actividades personales. Un espacio es un área distinta del dispositivo que permite la segregación y la gestión de los diferentes tipos de datos,

aplicaciones y conexiones de red. Si se tiene diferentes espacios, cada uno de estos debe tener sus normas para el almacenamiento de datos, los permisos de aplicaciones y enrutamiento de red. Los espacios separados ayudan a los usuarios a evitar actividades como la copia accidental de los datos corporativos hacia espacios personales o exponer los datos de trabajo confidenciales durante un Video chat.
El dispositivo cifra el espacio de trabajo durante el proceso de activación. Es posible utilizar una regla de políticas TI cifrar la separación del espacio personal.

Los dispositivos que no están activados en BDS operan sólo en espacio personal. Cuando se activa un dispositivo en BDS mediante la opción BlackBerry Balance, se crea un espacio de trabajo en el dispositivo. El espacio personal en el dispositivo permanece intacto durante el proceso de activación y los datos del usuario, aplicaciones o conexiones de red, que el usuario estaba utilizando para que el dispositivo se haya activado en BDS estarán disponibles para el usuario en el espacio personal del dispositivo [42].

Conservando el espacio personal original en el dispositivo se ofrece a los usuarios la posibilidad de utilizar los dispositivos para las actividades permitidas por las políticas de seguridad dadas y así no puede usar este espacio personal para actividades como la descarga de videos, jugar juegos en línea, subir fotos personales y entrar a redes sociales logrando así proteger el contenido de la empresa almacenado en el espacio de trabajo.
El espacio de trabajo es un área separada del dispositivo para los recursos de trabajo, que también proporciona una versión modificada del llamado BlackBerry World que contiene las aplicaciones que la organización permite a los usuarios descargar y utilizar en el trabajo. El espacio de trabajo también ofrece un área separada del dispositivo en el que los usuarios pueden crear, editar y guardar documentos de trabajo [42].

4.3.5.2. FORMA DE CLASIFICAR DATOS PERSONALES Y EMPRESARIALES

Los dispositivos BlackBerry, Android e IOS pueden distinguir entre los datos usados a nivel empresarial y los datos que es para su uso personal. Los dispositivos clasifican los datos como de trabajo o personales, basados en el origen de los datos, y estas forma de clasificar determinan cómo estos la plataforma se encarga de proteger y manejar los datos en los dispositivos.

Por ejemplo, si los datos vienen de una cuenta de trabajo, se almacena en el espacio de trabajo del dispositivo, y si los datos provienen de una cuenta personal, se almacena en el espacio personal del dispositivo. Después de clasificar los datos como datos de trabajo o datos personales, los datos personales no pueden ser reclasificados como datos laborales y los de trabajo no pueden ser reclasificados como datos personales [43].
La siguiente tabla IV.X describe cada clasificación de aplicaciones y muestra ejemplos de aplicaciones que pertenecen a cada entorno:

DESCRIPCIÓN	APLICACIÓN
Aplicaciones que sólo están disponibles en el espacio de trabajo y muestran solo datos de trabajo	• BlackBerry World para empresas • Cualquier aplicación implementada por la organización • Cualquier aplicaciones descargada de BlackBerry World para empresas
Aplicaciones que sólo están disponibles en el espacio personal y muestran solo datos personales	• BBM en la cual una política impida los contactos que no pertenezcan a la empresa. • BBM vídeo en la cual una política impida los contactos que no pertenezcan a la empresa. • BlackBerry Newsstand • BlackBerry History

	• BlackBerry World • Calculadora • Cámara • Brújula • Aplicaciones de Mensajería Instantánea • Facebook para dispositivos BlackBerry • Funciones del Teléfono • Mensajes de texto SMS en la cual una política impida los contactos que no pertenezcan a la empresa. • Correo de voz visual en la cual una política impida los contactos que no pertenezcan a la empresa. • Tiempo • Cualquier aplicaciones que los usuarios descargan de BlackBerry World (incluyendo BlackBerry Runtime para aplicaciones de Android)
Aplicaciones que están disponibles tanto en el espacio de trabajo como en el espacio personal las cuales son controladas por las política IT aplicadas en BES 10	• BlackBerry Remember • BlackBerry Hub • Calendario • Contactos • Búsqueda
Aplicaciones que tienen que tienen una parte en el entorno de trabajo y otra en el entorno personal las cuales son controladas por las política IT aplicadas en BES 10	• Adobe Reader • Navegador • Documents To Go • Administrador de archivos • Ayuda

	• Música • Imágenes • Print To Go • Vídeos • Técnica de Seguridad • Información general

TABLA IV. X APLICACIONES DE ENTORNO PERSONAL Y DE TRABAJO

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

Cabe destacar que las aplicaciones Android en su totalidad son etiquetadas como aplicaciones personales y no pueden ser enviadas al entorno de trabajo, con lo cual se asegura la empresa y su información crítica [43].

4.3.5.3. FORMAS DE PROTEGER LOS DATOS EMPRESARIALES Y LOS PERSONALES

Los datos son asegurados mediante la encriptación de los datos almacenados en el espacio de trabajo.

Los dispositivos también pueden proteger los datos personales mediante la encriptación de los archivos almacenados en el espacio personal si es requerido. Los dispositivos también pueden cifrar los archivos almacenados en tarjetas de memoria que se insertan en los dispositivos, sólo los datos personales se pueden guardar en tarjetas de memoria.

Los dispositivos cifran sólo el contenido que no está cifrado.

4.3.5.3.1. PROTECCIÓN DEL ENTORNO DE TRABAJO

Los dispositivos mediante BES 10 cifran los datos almacenados en el entorno de trabajo mediante encriptación XTS -AES -256.

Un dispositivo genera aleatoriamente una clave de cifrado para cifrar el contenido de un archivo. Las claves de cifrado están protegidas por un sistema jerárquico de la siguiente manera:

- El dispositivo cifra los archivos con la clave dada por el dominio de trabajo y almacena la clave de cifrado como un atributo de metadatos del archivo
- La clave de dominio de trabajo es una clave generada aleatoriamente la cual se almacena en los metadatos del sistema de archivos y se cifra mediante la clave maestra de trabajo.
- También se genera aleatoriamente la clave maestra de trabajo. La clave principal de trabajo se almacena en la NVRAM del dispositivo y se cifra con la clave maestra del sistema
- La clave maestra del sistema se almacena en el bloque de memoria protegida en el dispositivo
- El bloque de memoria protegida replay, se cifra con una clave que se encuentra incorporada en el procesador.
- Las claves de cifrado de archivos, la clave de dominio de trabajo, la clave maestra de trabajo, y la clave maestra del sistema se generan mediante BlackBerry OS Cryptographic Kernel, que es una herramienta de BES 10.

4.3.5.3.2. PROTECCIÓN DEL ENTORNO PERSONAL

Los dispositivos permiten la encriptación de archivos personales en los dispositivos utilizando el " Espacio Personal de Cifrado de datos " la cual es una regla de política de TI para activar el cifrado en el espacio personal de los dispositivos, si la regla de " Espacio Personal de Cifrado de datos " se establece en Sí, los archivos almacenados en el espacio personal del dispositivo están encriptados, si esta regla se establece en No, los usuarios pueden optar por cifrar los archivos en el espacio personal con la opción de cifrado de dispositivos en la configuración de seguridad y privacidad del dispositivo.

Si el cifrado está activado para el espacio personal del dispositivo, el dispositivo encripta los archivos almacenados en el sistema de archivos personales

mediante XTS-AES-256. Un dispositivo genera aleatoriamente una clave de cifrado para cifrar el contenido de un archivo [44].

4.3.5.3.3. PROTECCIÓN MEDIANTE REGLAS DE CONTRASEÑA

Para asegurar el contenido del cuando los dispositivos están activados en BDS mediante la característica BlackBerry Balance, los dispositivos requieren que los usuarios establezcan una contraseña para el espacio de trabajo. Si no se desea que los usuarios introduzcan una contraseña para acceder a los contenidos de trabajo, se puede establecer la "Contraseña requerida para el espacio de trabajo" mediante una regla de política TI en No.

Usted puede utilizar las reglas de política para hacer cumplir una contraseña para el espacio de trabajo o todo el dispositivo y luego controlar los requisitos de contraseña para la contraseña, como la complejidad y la duración.

4.3.5.3.4. BORRADO EN LOS ESPACIOS DE TRABAJO

Para proteger los datos de la empresa, se puede eliminar todos los datos de trabajo en dispositivo mediante una limpieza de dispositivo. Todos los datos personales se mantienen en el dispositivo. Esto es aconsejable cuando usuario ya no trabaja en la empresa, o se ha extraviado algún equipo. [39]

En la siguiente tabla IV.XI se muestran ejemplos de los datos que se eliminan cuando los dispositivos borran los datos del espacio de trabajo:

ITEM	DESCRIPCIÓN
Mensajes de correo electrónico	• Los mensajes de correo electrónico enviados a la cuenta de correo electrónico del usuario y los mensajes de correo electrónico que el usuario envía a la cuenta de correo electrónico de la empresa. • Todos los mensajes de correo electrónico que el usuario crea

	usando su cuenta de correo.
Datos Adjuntos	Los archivos adjuntos que se envían a la cuenta de correo electrónico y los archivos adjuntos que el usuario envía a la cuenta de correo electrónico. Los archivos adjuntos que el usuario guarda en el espacio de trabajo.
Entradas de calendario	Las entradas de calendario que el usuario crea usando su calendario de trabajo.
Contactos	Contactos que BDS sincroniza con la cuenta de correo electrónico del usuario.
Recordatorios BlackBerry	Todas las tareas y notas que BDS sincroniza con la cuenta de correo electrónico del usuario.
Navegadores	Todos los datos de los navegadores.
Archivos	Los archivos que el usuario accede y descarga desde la red de su organización.
Políticas IT	Políticas IT asociadas con la empresa.
Claves de dispositivo	Borrado de contraseña de comunicación. Lo que evita que el dispositivo se comunique con el servicio BES 10.
Aplicaciones de trabajo	Aplicaciones de trabajo que el usuario descarga e instala en un dispositivo.
Datos de trabajo	Datos que se asocian con las aplicaciones de trabajo en el dispositivo.
Perfiles Wi-FI	Perfiles Wi-Fi que el usuario configura en el dispositivo.
Perfiles VPN	Perfiles VPN que el usuario configura en el dispositivo.

TABLA IV. XI **BORRADO DE ESPACIOS UDS**

FUENTE:
http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.3.5.4. LICENCIAS DE DOMINIO Y DE DISPOSITIVOS

Las licencias controlan la cantidad de dispositivos BlackBerry, IOS y Android que pueden existir en un dominio de BES 10 al mismo tiempo. Los tipos de licencia que utiliza una organización determinarán las funciones y los dispositivos que se pueden gestionar a través de BES 10. Una licencia se utiliza cuando un usuario activa un dispositivo, el cual utiliza sólo un tipo de licencia a la vez.

Se debe utilizar BlackBerry Management Studio para administrar las licencias. Dependiendo del método de activación de licencias que se elija, se puede activar las licencias en BlackBerry Management Studio o en el Centro de cuentas BlackBerry. La consola de BDS sólo acepta las BlackBerry Mobile Voice System CAL, que son las licencias registradas [41].

.

4.3.5.4.1. Tipos de Licencias

A menos que se indique lo contrario, se puede activar los dispositivos con un plan de servicio o una conexión Wi-Fi. BES 10 versión 10.1 admite los siguientes tipos de licencia:

La siguiente tabla IV.XII describe cada tipo de licencia de BES 10:

TIPO DE LICENCIA	DESCRIPCIÓN
EMM – Corporate for BlackBerry	Para activar: • Dispositivos BlackBerry 10 y Tablets BlackBerry PlayBook que utilizan la tecnología BlackBerry Balance • Los dispositivos que ejecutan BlackBerry 10 OS versión 10.1 o posterior y tienen un plan de servicio que soporta el trabajo en espacios únicos.
EMM – Corporate	Para activar: • Dispositivos BlackBerry 10 y

	Tablets BlackBerry PlayBook que utilizan la tecnología BlackBerry Balance • Dispositivos que ejecutan BlackBerry 10 OS versión 10.1 o posterior y tener un plan de servicio que soporta el trabajo en espacios únicos • Dispositivos IOS y Android

TABLA IV. XII LICENCIAS BES

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.3.5.5. CONFIGURACIÓN DEL SERVIDOR DE LICENCIAS

La forma de activar una licencia de dominio es la siguiente:

Cuando al instalar se inicia de forma predeterminada, esta es la instancia activa. Cuando la empresa obtiene las licencias, recibe uno o más ID de activación, al activar las licencias, se registra el ordenador como el servidor de licencias para el dominio. El proceso registra la dirección MAC del servidor con la infraestructura de licencias BlackBerry, el cual almacena las licencias usadas [41].

4.3.5.6. ACTIVACIÓN DE LICENCIAS

En el estado licencia, se muestra un icono de advertencia hasta que se active la misma. Se debe activar las licencias antes de activar los dispositivos, eligiendo un método de activación que sea apropiado para el entorno de la organización, teniendo en cuenta que la agrupación de NIC no es compatible. Si la agrupación de NIC se configura en el servidor de licencias, este debe ser desactivarlo antes de activar las licencias [41].

4.3.5.6.1. Métodos de activación

En la tabla IV.XIII se detalla los métodos para activar las licencias de BES 10

METODO	DESCRIPCIÓN
Basado en ID de licencia	En este método se asignan todas las licencias disponibles asociados a un dominio BES 10. Si ya se ha asignado algunas licencias a un dominio, sólo las licencias que quedan disponibles.
Basado en Host ID	Para distribuir licencias asociadas con un ID de activación de licencia a través de múltiples dominios BES 10, se puede utilizar el ID de host para registrar el servidor de licencias de un dominio y especificar el número de licencias para asignar a la misma.
Basada en archivos	Si el servidor de licencias no tiene acceso a Internet, se puede utilizar un archivo de envió de licencia y otro de respuesta de licencia para activarlas manualmente y así asignarlas a un dominio BES. Se debe iniciar sesión en el Centro de cuentas BlackBerry para utilizar este método de activación.

TABLA IV. XIII LICENCIAS BES

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_Security_Technical_Overview-en.pdf

4.4. COMPARACIÓN DE LA NUEVA SOLUCIÓN BES 10 EN RELACION A LAS SOLUCIONES EXISTENTES

En este tema se compara dispositivos, y funciones a través de BES 10, BlackBerry Business Cloud Services, BES y BES Express.

Para comparar la solución BES 10 en relación a las soluciones ya existentes, se van a ocupar tablas para comparar de acuerdo a:

- Dispositivos soportados
- Funciones de datos y mensajería
- Funciones de activación
- Funciones de seguridad

4.4.1. DISPOSITIVOS SOPORTADOS

La tabla IV.XIV compara las diferentes plataformas de BES10 en relación a los dispositivos soportados:

CARACTERÍSTICA	BES 5.0 SP4	BES 5.0 EXPRESS	BES PARA MICROSOFT OFFICE 365	BBCS(BlackBerry Bussines Cloud Services)	BES 10
Dispositivos	Soporta dispositivos compatibles con BlackBerry 7.1 y anteriores	Soporta dispositivos compatibles con BlackBerry 7.1 y anteriores	Soporta dispositivos compatibles con BlackBerry 7.1 y anteriores	Soporta dispositivos compatibles con BlackBerry 7.1 y anteriores	Soporta: • Serie BlackBerry 10 • PlayBook tablets • Dispositivos Android • Dispositivos IOS

TABLA IV. XIV COMPARACIÓN DE DISPOSITIVOS SOPORTADOS

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_comparisonchart-en.pdf

4.4.2. FUNCIONES DE DATOS Y MENSAJERIA

La tabla IV.XV compara las diferentes plataformas de BES10 en relación a las funciones de datos y memoria:

CARACTERÍSTICA	BES 5.0 SP4	BES 5.0 EXPRESS	BES PARA MICROSOFT OFFICE 365	BBCS(BlackBerry Bussines Cloud Services)	BES 10
Entornos de Mensajería	Microsoft Exchange Dominio IBM Novel GroupWise:	Microsoft Exchange Dominio IBM	Microsoft Office 365	Microsoft Office 365	Entornos de mensajería que soportan Microsoft ActiveSync *
Email	X	X	X	X	X**
Búsqueda de contactos	X	X	X	X	X**
Envíos de mensaje	X	X	X	X	X**
Eliminación permanente de mensajes	X	X	X	X	X**
Mensajes de correo electrónico con HTML y contenido multimedia	X	X	X	X	X**
Mensaje de correo electrónico a distancia	X	X	X	X	X**

Bandeja de entrada separada trabajo y cuentas personales	X	X	X	X	X**
Sincronización de contactos personales y carpetas de emails	X	X	X	X	X**
Sincronización de datos del organizador (memos y tareas)	X	X	X	X	Soporta 10 dispositivos BlackBerry, dispositivos Android y dispositivos IOS solamente **
Sincronización de calendario	X	X	X	X	X**
Posibilidad de enviar las entradas del calendario	X	X	X	X	X**
Archivos adjuntos	X	X	X	X	X**

TABLA IV. XV COMPARACIÓN DE FUNCIONES DE DATOS Y MENSAJERÍA

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_comparisonchart-en.pdf

Notas:

* Secure Work Space para dispositivos Android e IOS solo compatible con Microsoft Exchange

** Soporta configuración de un cliente de Microsoft ActiveSync en el dispositivo para proporcionar sincronización entre el dispositivo BlackBerry y los servidores de mensajería que soportan Microsoft ActiveSync. En los dispositivos Android y dispositivos IOS la funcionalidad se proporciona, y puede ser limitada por, las capacidades del dispositivo.

4.4.3. FUNCION DE ACTIVACIÓN

La tabla IV.XVI compara las diferentes plataformas de BES10 en relación a la función de activación:

CARACTERÍSTICA	BES 5.0 SP4	BES 5.0 EXPRESS	BES PARA MICROSOFT OFFICE 365	BBCS(BlackBerry Bussines Cloud Services)	BES 10
Métodos de activación	Activación wireless: • Red móvil • Wi-Fi de la empresa Activación cableada: • BAS • BlackBerry Desktop Software • BlackBerry Web Desktop Manager	Activación wireless: • Red móvil • Wi-Fi de la empresa Activación cableada: • BAS • BlackBerry Desktop Software • BlackBerry Web Desktop Manager	Activación wireless: • Red móvil • Wi-Fi de la empresa Activación cableada: • BAS • BlackBerry Web Desktop Manager	Activación wireless: • Red móvil • Wi-Fi de la empresa Activación cableada: • BAS • BlackBerry Web Desktop Manager	Activación wireless: • Red móvil • Wi-Fi de la empresa Activación cableada: • BAS • BlackBerry Web Desktop Manager

TABLA IV. XVI COMPARACIÓN DE FUNCIONES DE ACTIVACIÓN

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_comparisonchart-en.pdf

4.4.4. FUNCIONES DE SEGURIDAD

La tabla IV.XVII compara las diferentes plataformas de BES10 en relación a las funciones de seguridad:

CARACTERÍSTICA	BES 5.0 SP4	BES 5.0 EXPRESS	BES PARA MICROSOFT OFFICE 365	BBCS(BlackBerry Bussines Cloud Services)	BES 10
Cifrado mejorado	S/MIME PGP	S/MIME PGP	Microsoft Office 365	Microsoft Office 365	S/MIME en dispositivos BlackBerry 10 e IOS
Separación entre espacio laboral y personal	X	X	X	X	X
Protección de dispositivos perdidos o robados	X	X	X	X	X
Reglas de Políticas IT	X	X	X	X	X
Inscripción de certificados para los dispositivos				X	X
Configuración de proxy TCP para conectarse a BlackBerry Infraestructure	X	X	X		X

TABLA IV. XVII COMPARACIÓN DE FUNCIONES DE SEGURIDAD

FUENTE: http://docs.BlackBerry.com/es/admin/deliverables/52722/BlackBerry_Enterprise_Service_10_version_10.1_comparisonchart-en.pdf

CAPÍTULO V

INSTALACIÓN DE LA SOLUCION MULTIPLATAFORMA

5.1. INTRODUCCIÓN

En el presente capítulo se procede a la instalación de los servidores tanto de correo en este caso Microsoft Exchange Server 2010 así como el servidor de dominio BES 10.1.1 los cuales funcionaran bajo el dominio @posventadatos.ec, dando antes una revisión hacia los requerimientos de cada servidor así como la lista de compatibilidad necesaria para el correcto funcionamiento de las aplicaciones.

Además se muestra la parte correspondiente a activación de licencias y dispositivos.

5.2. INSTALACIÓN DE MICROSOFT EXCHANGE 2010

El servidor de correo electrónico será instalado en un servidor con las siguientes características:

- Procesador Quad-Core AMD Opteron(tm) de 2.70 Ghz

- Memoria RAM de 6 Gb
- Sistema Operativo Microsoft Windows Server 2008 x64 SP 2
- Disco Duro de 50 Gb

La forma de trabajo en el servidor será de forma remota a través de la aplicación TeamViewer 8.0

En cuanto a las licencias de Exchange varían según los precios mostrados a continuación. En la siguiente tabla V.I se observa la lista de licencias requeridas para la instalación de Microsoft Exchange 2010.

Unid	Descripción		Total €
1	Exchange Server Standard	648,98 €	648,98 €
10	Exchange Standard CAL 2010	61,89 €	618,90 €
1	Windows 2008 R2 Server Enterprise	2.161,89 €	- €
	Precio Total		1.267,88 €

TABLA V. I Licencias requeridas para la instalación del servidor de correo electrónico Exchange 2010

Fuente: http://gonzgomez.blogspot.com/2012/08/instalacion-de-servidor-de-correo.html

Estas licencias ya están adquiridas por telefónica así como las licencias de Windows Server 2008.

5.2.1. PASOS PREVIOS A LA INSTALACIÓN

Los pasos a realizar antes de la instalación son los siguientes:

- Comprobar las especificaciones de la maquina
  - **CPU**

    Sistema basado en arquitectura x64 con procesador Intel que soporte la arquitectura Intel 64 Intel EM64T) o procesador AMD que soporte la plataforma AMD64.No hay soporte para los procesadores Intel titanium de la familia IA64.
  - **Sistema operativo**

Microsoft Windows Server® 2008 x64 Standard y Enterprise Edition con Service Pack 2 o Microsoft Windows Server® 2008 R2 Standard y Enterprise Edition

- **Sistema operativo para instalar las herramientas de gestión**

  Ediciones de de 64-bit de Microsoft Windows® Vista o Microsoft Windows® 7 o Windows Server 2008. Nota: Requisitos solo para las herramientas de gestión.

➢ Requisitos adicionales para ejecutar Exchange Server 2010

- **Memoria**

  4 Gb de RAM mínimo para el software de servidor, más 5 Mb de RAM recomendado para cada buzón.
- **Espacio de disco:**

  Mínimo de 1,2 Gb de espacio en disco para la instalación.
  500 Mb de espacio disponible en disco para cada paquete de idioma de Unified Messaging (UM) que se desee instalar.
  200 Mb de espacio disponible en el disco de sistema.
- **Medios de instalación**

  Unidad de DVD-ROM o una carpeta accesible, en red o local.
- **Sistema de archivos:**

  Particiones de disco formateadas con NTFS.
- **Monitor:**

  Resolución de 800x600 o superior.
- **Requisitos previos**

  Si estos requisitos previos no están instalados, el proceso de instalación de Exchange Server 2010 lo avisa y muestra enlaces a los lugares instalación; Se necesita acceso a internet si estos requisitos previos de instalación no están ya instalados o disponibles en la red local.
- **Microsoft .NET Framework 3.5 SP1**
- **Windows PowerShell v2.0**

  Estos requisitos pueden variar en función de la configuración del sistema y las funcionalidades concretas a instalar. En la siguiente figura V.1 observamos la información del equipo [44].

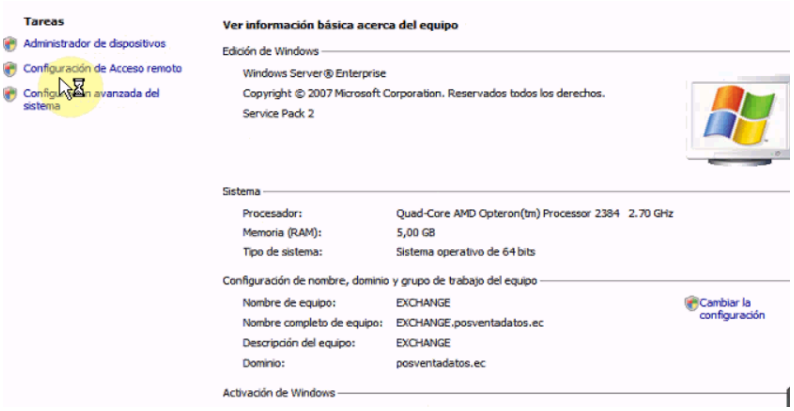


FIGURA V. 1INFORMACIÓN DEL EQUIPO

FUENTE: ELABORACIÓN PROPIA

- Comprobar los datos del equipo. En la figura V.2 se observa el dominio.

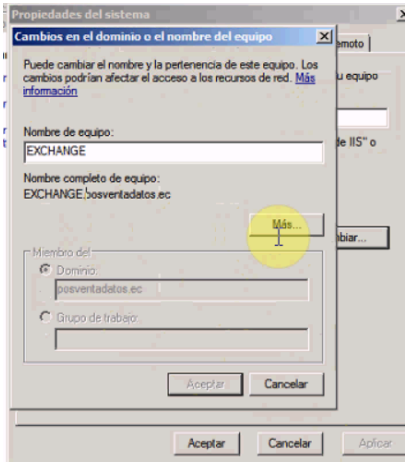


FIGURA V. 2 Dominio equipo

Fuente: Elaboración propia

Este equipo pertenece a la empresa telefónica con lo que se tiene definido el nombre del equipo, la configuración IP y el dominio que es posventas.ec

La configuración IP es la siguiente. En la figura V.3 se observa los datos de la configuración IP.

FIGURA V. 3 Configuración Ip

Fuente: Elaboración propia

- **[Nombre del equipo]** EXCHANGE.posventadatos.ec
- **[IP address]** 10.111.126.210
- **[Subnet Mask]** 255.255.255.248
- **[Default Gateway]** 10.111.126.209
- **[Prefered DNS server]** 127.0.0.1

5.2.2. INSTALACIÓN MICROSOFT EXCHANGE 2010

➢ Para instalar EXCHANGE SERVER 2010, se empieza con la imagen (**Setup)** que ya está en el servidor y se la corre. En la figura V.4 se observa la imagen de instalación.

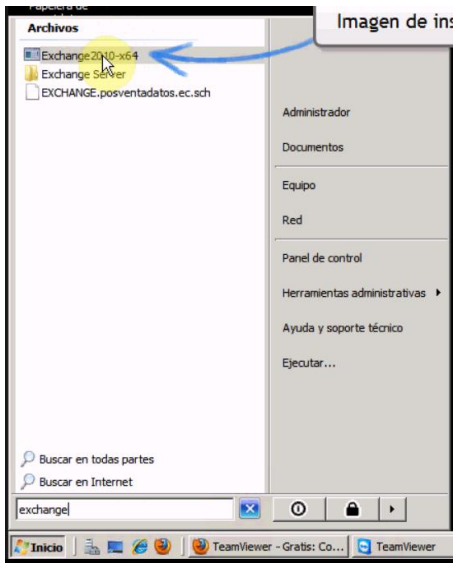


FIGURA V. 4 Imagen de instalación de EXCHANGE SERVER 2010

Fuente: Elaboración propia

- Los 2 primeros pasos ya están realizados, se debe continuar con el paso 3 de la instalación que es de los leguajes, se escoge instalar los lenguajes existentes en el DVD, que en éste caso es una archivo exe. En la figura V.5 se observa la interfaz de selección de lenguaje.

FIGURA V. 5 Selección de lenguajes en la instalación de EXCHANGE SERVER 2010

Fuente: Elaboración propia

- Se da clic en la opción **Instalar Microsoft Exchange** con una instalación típica. En la figura V.6 se muestra la interfaz de instalación de Microsoft Exchange.

FIGURA V. 6 Ícono de instalación de MICROSOFT EXCHANGE

Fuente: Elaboración propia

- Con la comprobación de los prerrequisitos es posible que nos arroje el programa de instalación alertas que deberían solucionar, para activar determinadas características e instalar Microsoft Office Filter Pack 2010. En la figura V.7 se tiene los cheques de instalación.

FIGURA V. 7 Cheques de la preparación

Fuente: Elaboración propia

NOTA: Para los inconvenientes de éstas alertas, se encuentra toda la documentación necesaria para la resolución en la página de soporte de Microsoft "http://support.microsoft.com/?ln=es-es", en su mayoría se puede acceder directamente, dando un clic en *Acción Recomendada*

En la figura V.8 se observa la página de soporte Microsoft.

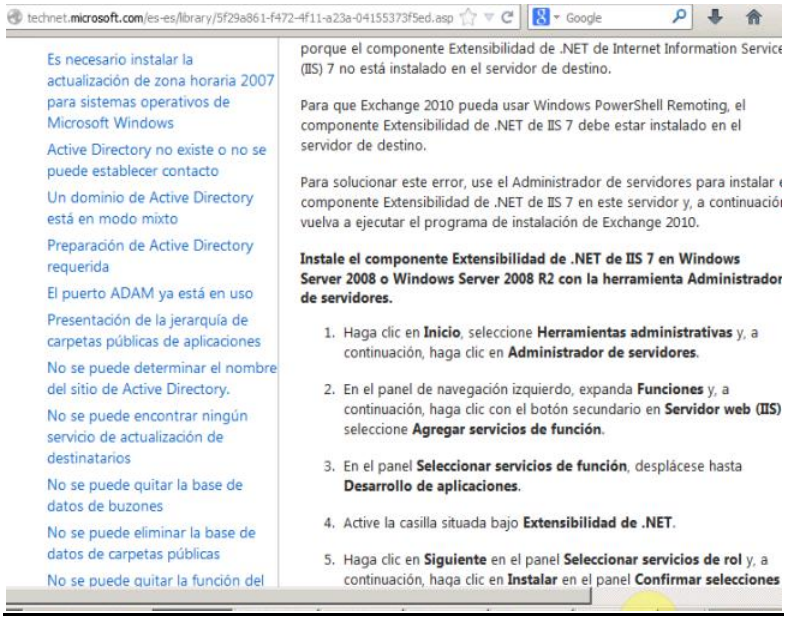


FIGURA V. 8 Soporte Microsoft

Fuente: Elaboración propia

- Con la resolución de las alertas, se procede a instalar. En la figura V.9 se ve que los requerimientos están completados.

FIGURA V. 9 Instalación posterior a los chequeos de herramientas necesarias

Fuente: Elaboración propia

En la figura V.10 se observa la interfaz para finalizar la instalación.

FIGURA V. 10 Instalación posterior a los chequeos de herramientas necesarias (2)

Fuente: Elaboración propia

- Lo siguiente es la configuración del Exchange 2010 sp2, se ejecuta **Exchange Management Console**.

- Se abre el árbol de configuración, Lo primero que se configurará será un nuevo send connector [conector de envío] que se utiliza para transferir los mensajes salientes de Exchange a través de Internet. Para ello se extiende *Organization configuration* [Configuración de la Organización] y se selecciona *Hub transport* [Transporte de concentradores], en la pestaña central se selecciona *Send connectors* [Enviar conectores] y en el panel lateral derecho de *Action* [Acciones] se elige *New send connector* [Nuevo conector de envío]. En la figura V.11 se observa el Exchange Management Console.

FIGURA V. 11 Exchange Managment Console

Fuente: Elaboración propia

- Se da el nombre al nuevo conector. En la figura V.12 se observa la interfaz para dar nombre al servidor.

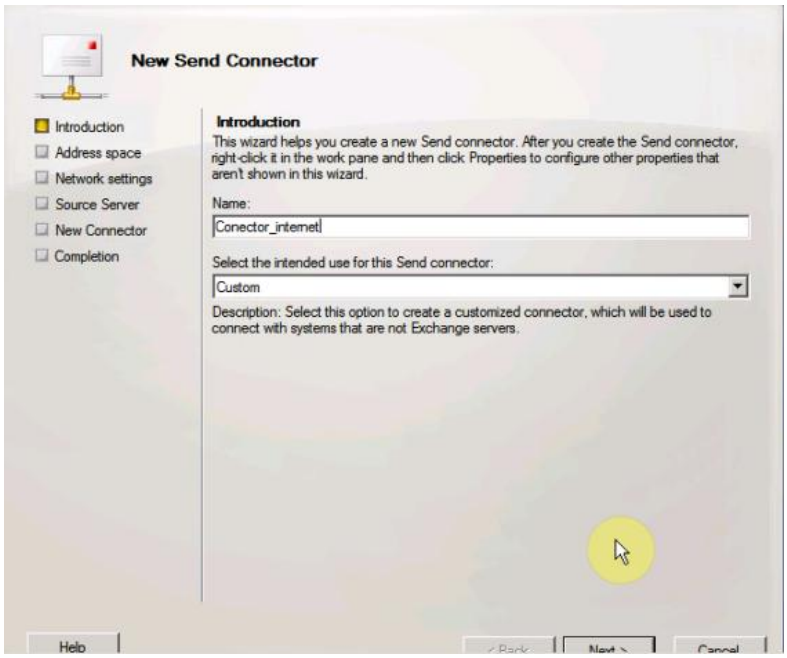


FIGURA V. 12 Creación y configuración de un conector de envío

Fuente: Elaboración propia

- En Address space se introduce [*] para que este “send connector” esté configurado para enviar mensajes de correo electrónico a cualquier dominio en Internet. Sigue clic en OK. En la figura V.13 se observa la interfaz para crear un conector de envío.

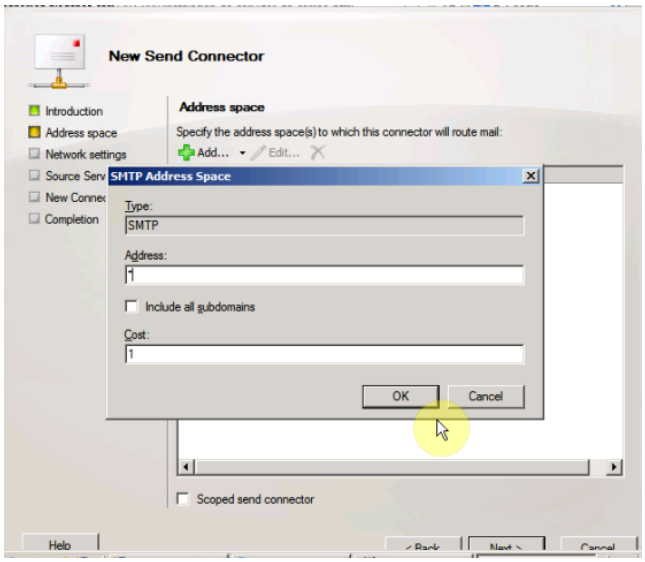


FIGURA V. 13 Creación y configuración de un conector de envío (2)

Fuente: Elaboración propia

- Siguen 2 botones de “next” más y con un botón “new” y se crea el nuevo conector. En la figura V.14 observamos la interfaz de la creación del conector de envío con éxito.

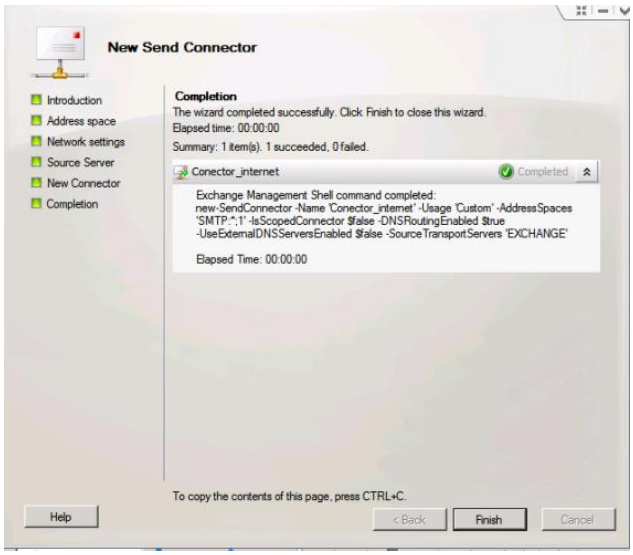


FIGURA V. 14 Creación y configuración de un conector de envío (3)

Fuente: Elaboración propia

- Se revisa en Specify the FQDN this connector will provide in response to HELO or EHLO, ubicada en propiedades del conector si figura el nombre de nuestro servidor “**EXCHANGE.posventadatos.ec”.** En la figura V.15 se observa la ventana para cambiar o verifica el nombre del servidor.

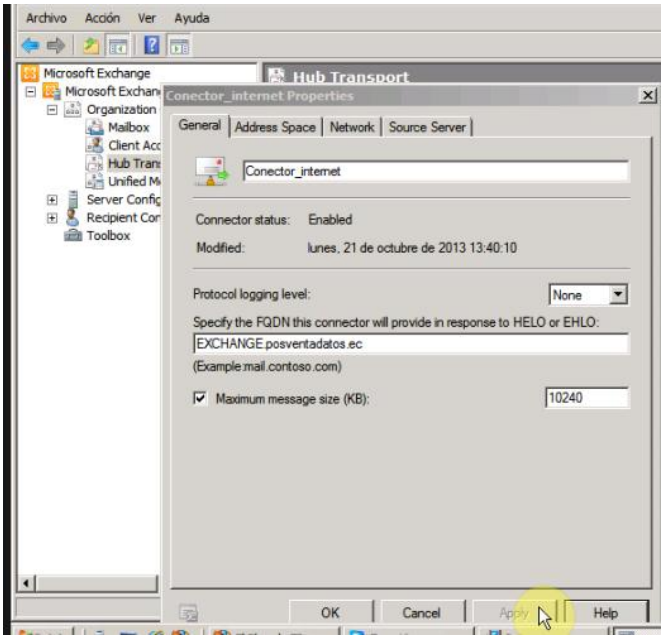


FIGURA V. 15 Nombre del servidor

Fuente: Elaboración propia

- Se añade el dominio público [posventadatos.ec] a los dominios aceptados por nuestro servidor Exchange, para ello se extiende *Organization configuration* [Configuración de la Organización], se selecciona *Hub transport* [Transporte de concentradores], en la pestaña central se selecciona *Accepted Domains* [Dominios Aceptados] y en el panel lateral derecho de *Action* [Acciones] se elige *New Accepted Domains* [Nuevo dominio aceptado]. En la figura V.16 se observa la ventana de aceptación de dominios.

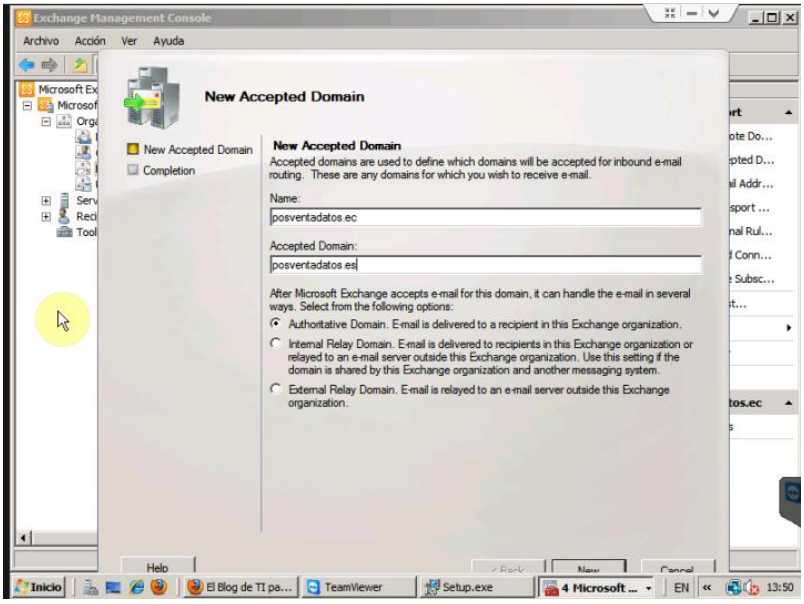


FIGURA V. 16 Adición del dominio público

Fuente: Elaboración propia

- Se asignan a nuestros usuarios de correo electrónico, para eso:
  Se dirige a Recipient configuration [Configuración de destinatarios] y se selecciona *Mailbox* [Buzón], en el panel lateral derecho de *Action* [Acciones], clic en New *Mailbox* [Nuevo buzón].

    - Se da clic en User MAILBOX, y posterior a esto se debe crear nuevos ya que con usuarios existentes no se cuenta, entre los creados debe estar uno para la cuenta de BLACKBERRY, tomando en cuenta algo muy importante, debe tener asignado el rol de usuario y no de administrador. En la figura V.17 se observa la interfaz de creación de cuentas.

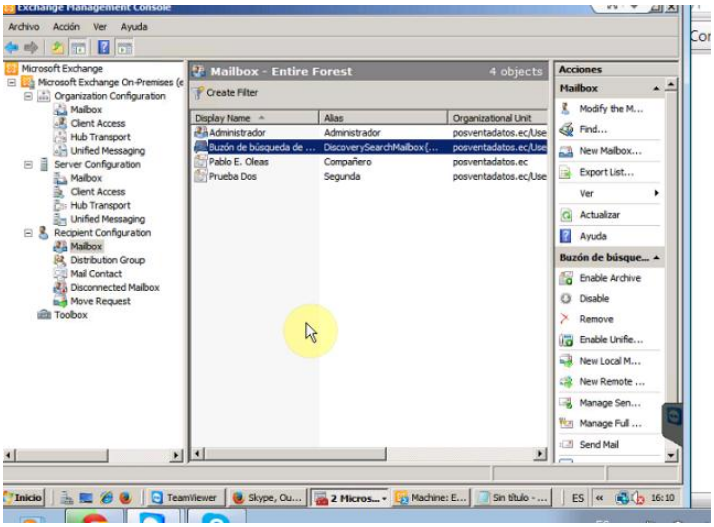


FIGURA V. 17 Creación de cuentas mail de usuario

Fuente: Elaboración propia

5.2.3. Asignación de permisos de cuenta de servicio de BES para Microsoft Exchange

Antes de empezar se debe revisar el siguiente check list de los permisos que se requieren para que la cuenta de servicio BES funcione correctamente.

- Local Administrator rights on the BES
  (Derechos como administrador local en el BES))
- Local Security Policy permissions for the BES service account
  (Permisos de políticas de seguridad local para la cuenta de servicio de BES*)*
- Send as permission at the Domain level
  (Permisos de envío a nivel de dominio)
- Microsoft Exchange permissions at the Administrative Group level
  (Permisos de Microsoft Exchange a nivel de grupo administrativo)
- Microsoft Exchange permissions at the Microsoft Exchange Server level
  (Permisos de Microsoft Exchange a nivel de servidor)
- Microsoft Exchange Throttling permissions for the BES service account
  (Cambio de permisos limitados de Microsoft para la cuenta de servicios del servidor BlackBerry)

- Database permissions for managing the BlackBerry Configuration Database
  (Permisos a nivel de base de datos para gestionar su configuración de BlackBerry Configuration Database)

5.2.3.1. TAREA 1

Para asignar la cuenta de servicio local del BES derechos de administrador en el ordenador que aloja el BES, se realizó los siguientes pasos:

1. Dirigirse a [*Inicio*] > [*Programas*] > [*Herramientas administrativas*] > [*Usuarios y equipos de Active Directory*]
2. Se va a la carpeta [*Builtin*]
3. Se agrega el miembro con el nombre de BESAdmin, se chequea el nombre y se aplica. En las figuras V.18, 19 se puede observar la ventana para la asignación la cuenta de servicio local del BES derechos de administrador en el ordenador que aloja el BES.

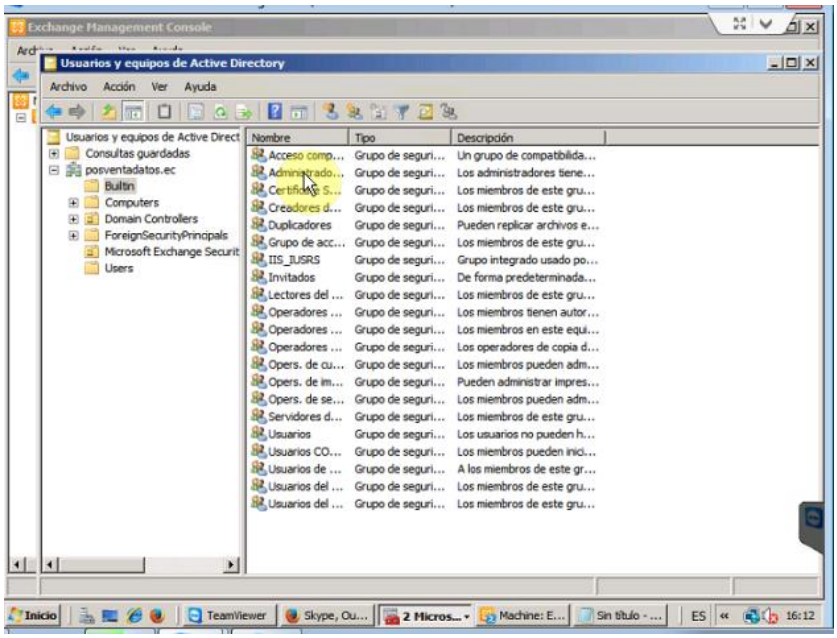


FIGURA V. 18 Asignación la cuenta de servicio local del BES derechos de administrador en el ordenador que aloja el BES

Fuente: Elaboración propia

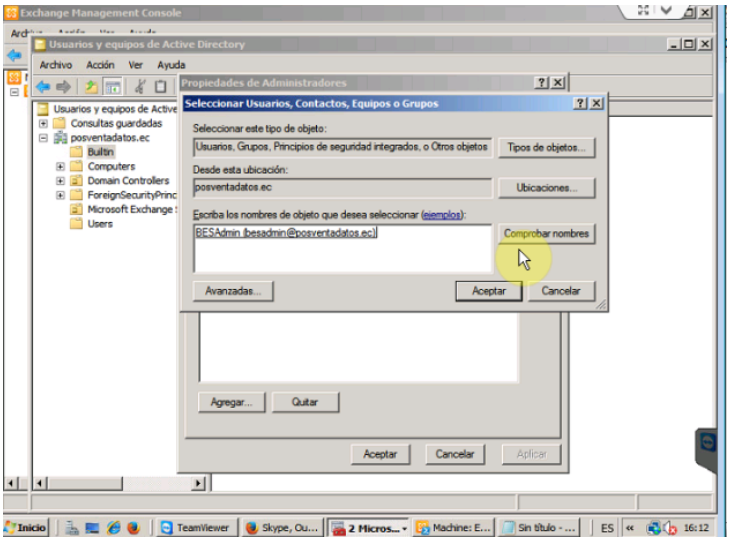


FIGURA V. 19 Asignación la cuenta de servicio local del BES derechos de administrador en el ordenador que aloja el BES (2)

Fuente: Elaboración propia

5.2.3.2. TAREA 2

Para asignar permisos de política de seguridad local, para la cuenta de servicio de BES, se debe completar los siguientes pasos en el ordenador que aloja el BES.

Este procedimiento permite que la cuenta de servicio de BES pueda acceder a la computadora local y ejecutar BES como un servicio de Windows.

1. Se dirige a [*Inicio*] > [*Programas*] > [*Herramientas administrativas*] > [*Directiva de seguridad local*] > [*Asignación de derechos de usuarios*] > [*Iniciar sesión como servicio*]

2. Se agrega al usuario del grupo ***POSVENTADATOS\BESAdmin.*** en la siguiente figura V.20 se observa la ventana para el acceso de cuenta.

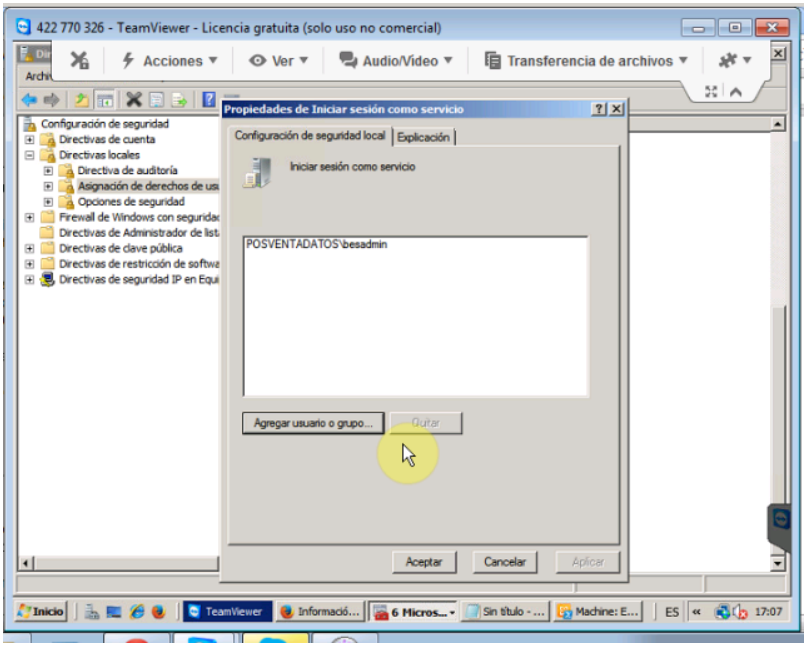


FIGURA V. 20 Acceso cuenta de servicio de BES pueda a la computadora local y ejecutar BES como un servicio de Windows.

Fuente: Elaboración propia

5.2.3.3. TAREA 3

Para conceder permiso de enviar al Active Directory en una sola cuenta para todos los usuarios de teléfonos inteligentes BlackBerry en un dominio de Active Directory de Microsoft o un contenedor:

1. Se dirige a [*Inicio*] > [*Programas*] > [*Herramientas administrativas*] > [*Usuarios y equipos de Active Directory*]

2. En el menú [*ver*] >se marca [*características avanzadas*] > dentro del dominio, en las propiedades de usuarios se da permisos especiales a BESAdmin.
   01:32:93 tarea 3. En la figura V.21 se observa la interfaz para modificar permisos de Active directory.

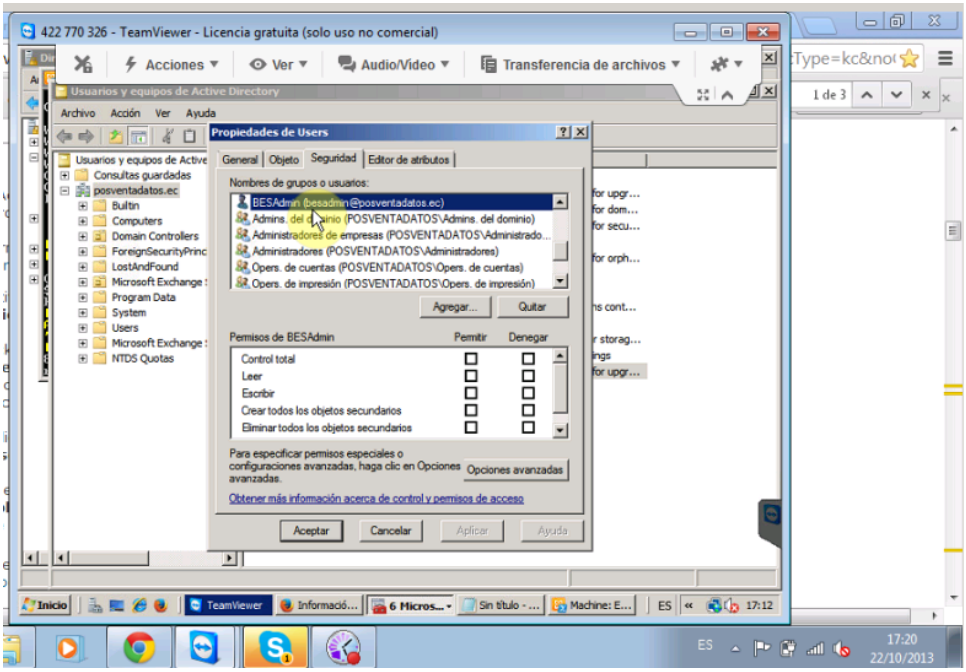


FIGURA V. 21 Permiso de enviar al Active Directory en una sola cuenta para todos los usuarios de teléfonos inteligentes BlackBerry en un dominio de Active Directory de Microsoft o un contenedor

Fuente: Elaboración propia

5.2.3.4. TAREA 4

Se debe ingresar a **EXCHENGE MANAGEMENT SHELL** se tiene que tipear los siguientes comandos para asignar permisos de Microsoft Exchange Server en el nivel de grupo administrativo.

- *>Add-RoleGroupMember "View-Only Organization Management" -Member "BESAdmin"*

- *>Get-RoleGroupMember "View-Only Organization Management"*

En la figura V.22 se observa la asignación de servicios a nivel administrativo.

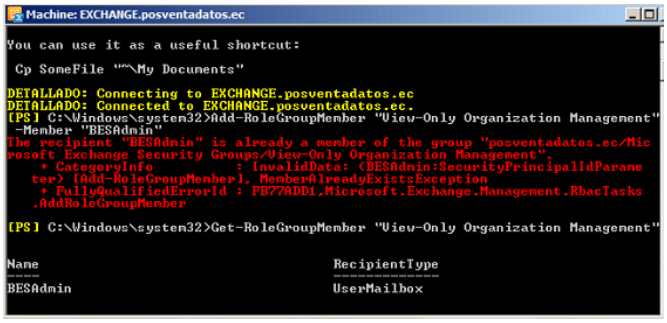


FIGURA V. 22 Permisos a nivel de grupo administrativo

Fuente: Elaboración propia

5.2.3.5. TAREA 5

Para asignar permisos de servidor a nivel de base de datos:

1. Se accede a **EXCHENGE MANAGEMNT SHELL**

- *>Get-MailboxDatabase | Add-ADPermission -User "BESAdmin" -AccessRights ExtendedRight -ExtendedRights Receive-As, ms-Exch-Store-Admin, ms-Exch-Store-Visible*

- *>Add-ADPermission -Identity "CN=ORGNAME,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=Domain_1,DC= Domain_2, DC=Domain_3" -User "BESAdmin" -AccessRights ExtendedRight -ExtendedRights Receive-As, ms-Exch-Store-Admin, ms-Exch-Store-Visible*

En la figura V.23 se observa los miembros.

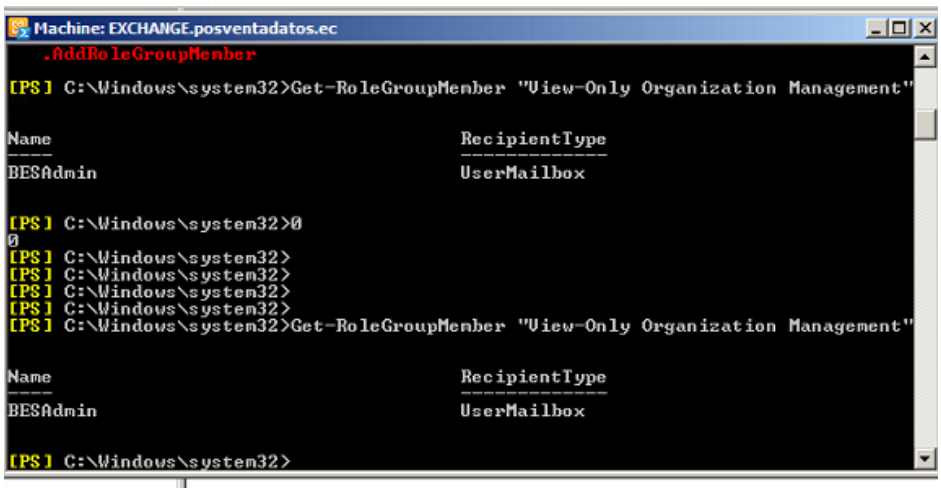


FIGURA V. 23 Visualización miembros

Fuente: Elaboración propia

2. Se verifica los permisos de EXCHANGE requeridos:

- *>Get-Mailboxdatabase -identity "Mailbox Database 0372917875" | Get-ADPermission | where-object { ($_.extendedrights -like "*receive*" -or $_.extendedrights -like "*ms- exch-store-visible*" -or $_.extendedrights -like "*ms-Exch-Store-ad*") -and ($_.User -like "*BESadmin*") } | select Identity, User, Extend dRights, IsInherited | ft –wrap*

En la figura V.24 se observa los permisos que tienen los miembros.

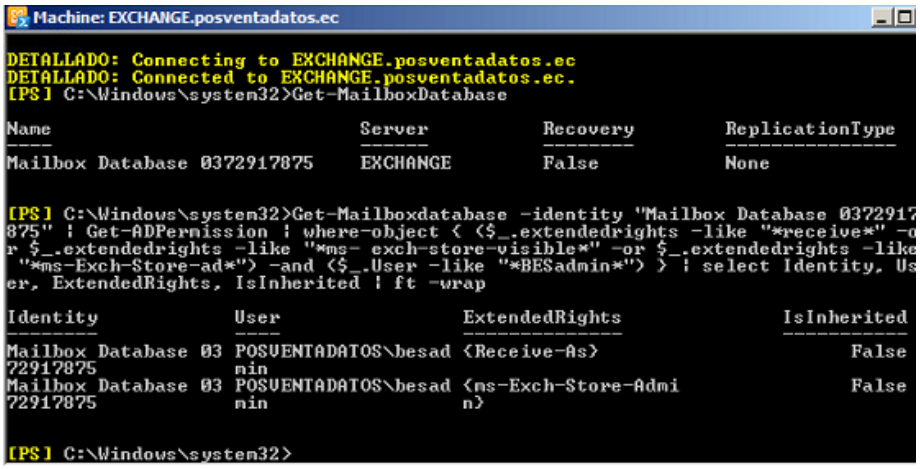


FIGURA V. 24 Verificación los permisos de EXCHANGE requeridos

Fuente: Elaboración propia

3. Es muy importante cambiar el nombre de mailbox al que se tiene existente

En la figura V.25 se ve el nombre que hay que cambiar.

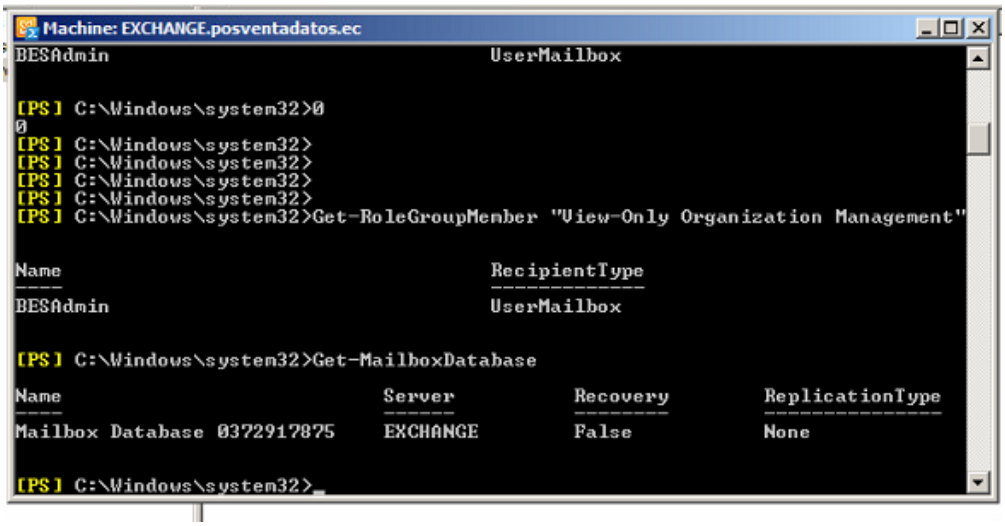


FIGURA V. 25Nombre del mailbox

Fuente: Elaboración propia

5.2.3.6. TAREA 6

En este caso, solamente se verifica que se haya asignado las políticas de servicios limitadas para la cuenta de servicio BES.

En la figura V.26 se muestra la verificación de las políticas de servicio.

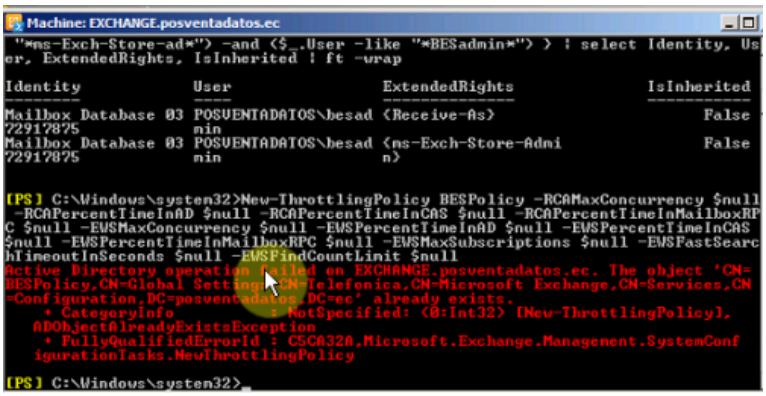


FIGURA V. 26 Verificación de asignación de las políticas de servicios limitadas para la cuenta de servicio BES

Fuente: Elaboración propia

5.3. INSTALACIÓN BES 10.1.1

El servidor BES 10 va a ser instalado en un servidor con las siguientes características:

- Procesador Quad-Core AMD Opteron(tm) de 2.70 Ghz
- Memoria RAM de 4 Gb
- Sistema Operativo Microsoft Windows Server 2008 x64 SP 2
- Disco Duro de 50 Gb

LA forma de trabajo en el servidor será de forma remota a través de la aplicación TeamViewer 8.0

5.3.1. PASOS PREVIOS A LA INSTALCIÓN

Como pasos previos a la instalación de BES se debe:

- Comprobar las matrices de compatibilidad que nos ofrece la documentación de BES 10
  - Sistemas Operativos solo X64
    - Windows Server 2008 SP2
    - Windows Server 2008 R2
    - Windows Server 2008 R2 SP1
    - Windows Server 2012
  - Servidores de Base de datos tanto X32 como X64
    - Microsoft SQL Server 2008 SP3
    - Microsoft SQL Server 2008 Express SP3

    - Microsoft SQL Server 2008 R2
    - Microsoft SQL Server 2008 R2 SP1
    - Microsoft SQL Server 2008 R2 SP2
    - Microsoft SQL Server 2008 R2 Express
    - Microsoft SQL Server 2008 R2 SP1 Express
    - Microsoft SQL Server 2008 R2 SP2 Express
    - Microsoft SQL Server 2012
    - Microsoft SQL Server 2012 SP1
- Microsoft .NET Framework
    - Microsoft .NET Framework 3.5 SP1
    - Microsoft .NET Framework 4.0
- Servidores Web
    - Microsoft IIS 7.0 y posteriors
- Navegadores Web
    - Internet Explorer 8.0 en adelante
    - Mozilla Firefox 10 en adelante
    - Google Chrome 12 en adelante
    - Safari 5 for MAC en adelante
- Sistemas Operativos de Dispositivos
    - BlackBerry 10 OS
    - BlackBerry Playbook 2.0 en adelante
    - IOS OS 5.0 en adelante excepto el OS 7.0
    - Android OS 2.3 en adelante
- Servidor de e-mail
    - Microsoft Exchange Server 2007 SP3 (Microsoft ActiveSync 12.1)
    - Microsoft Exchange Server 2010 (Microsoft ActiveSync 14.0)
    - Microsoft Exchange Server 2010 SP1 en adelante (Microsoft ActiveSync 14.1) [45].

➢ Se debe comprobar que el servidor este dentro del dominio correcto

La figura V.27 muestra las especificaciones de nuestro servidor:

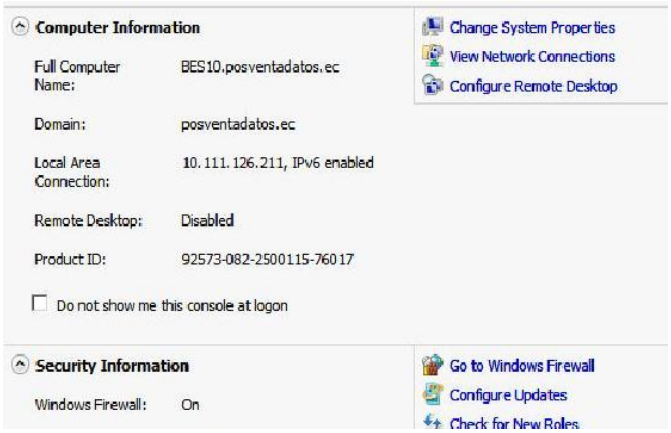


FIGURA V. 27 Propiedades del servidor BES10

Fuente: Elaboración propia

En este caso ell servidor ya pertenec3e al dominio posventadatos.ec y tiene una configuración IP similar a la del servidor Exchange

- Se Comprueba que el servidor tenga conectividad con el dominio ec.srp.BlackBerry.com perteneciente a BlackBerry

En la figura V.28 se muestra la prueba de compatibilidad hacia el dominio seguro de BlackBerry:

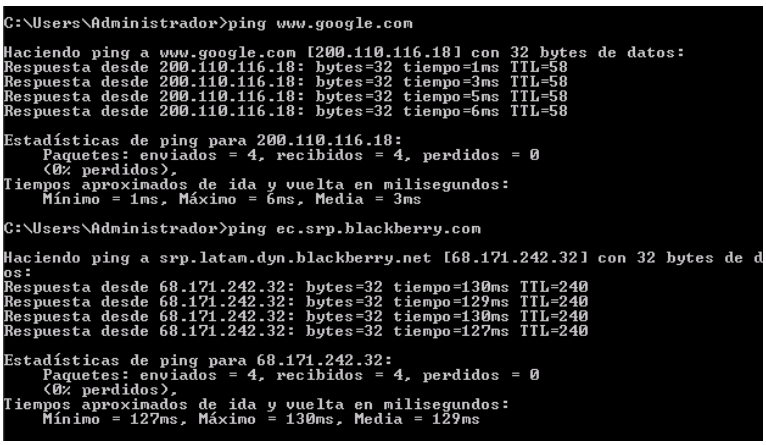


FIGURA V. 28 Propiedades del servidor BES10

Fuente: Elaboración propia

5.3.2. INSTALACIÓN BLACKBERRY ENTERPIRSE SERVICE 10.1.1

- Como primer paso se debe descargar la solución BES 10.1.1 de la página oficial de BlackBerry, la cual pide un registro de usuario, una vez llenado este registro la empresa RIM envía un correo hacia la cuenta, en

el cual se detalla un link para descargar el programa así como un documento en donde están las licencias que se usaran en BES 10.

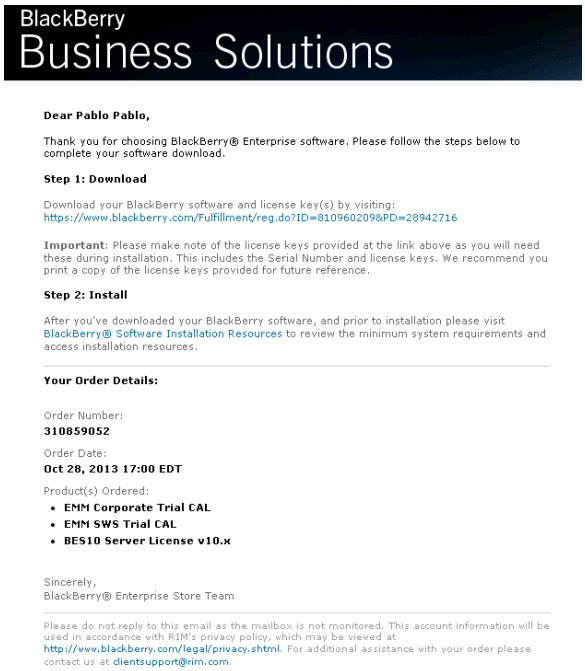
En la figura V.29 se indica la página de registro a RIM:

FIGURA V. 29 Hoja de registro de RIM

Fuente: Elaboración propia

- Llega a la cuenta un correo de BlackBerry en el cual aparece el link enviado para la descarga y el cual contiene las licencias, en este caso por ser una prueba se obtiene licencias de prueba por 60 días, periodo en el cual se debe probar la solución en post de la adquisición de licencias definitivas.

  La figura V.30 muestra los accesos para la descarga y para las licencias de BES10:



BlackBerry
Business Solutions

Dear Pablo Pablo,

Thank you for choosing BlackBerry® Enterprise software. Please follow the steps below to complete your software download.

Step 1: Download

Download your BlackBerry software and license key(s) by visiting:
https://www.blackberry.com/Fulfillment/reg.do?ID=8109602098PD=28942716

Important: Please make note of the license keys provided at the link above as you will need these during installation. This includes the Serial Number and license keys. We recommend you print a copy of the license keys provided for future reference.

Step 2: Install

After you've downloaded your BlackBerry software, and prior to installation please visit BlackBerry® Software Installation Resources to review the minimum system requirements and access installation resources.

Your Order Details:

Order Number:
310859052

Order Date:
Oct 28, 2013 17:00 EDT

Product(s) Ordered:

- **EMM Corporate Trial CAL**
- **EMM SWS Trial CAL**
- **BES10 Server License v10.x**

Sincerely,
BlackBerry® Enterprise Store Team

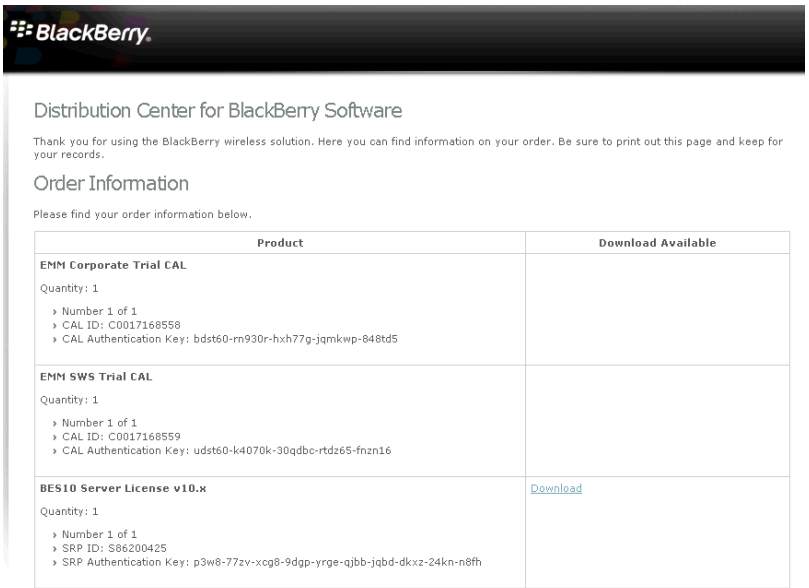
Please do not reply to this email as the mailbox is not monitored. This account information will be used in accordance with RIM's privacy policy, which may be viewed at http://www.blackberry.com/legal/privacy.shtml. For additional assistance with your order please contact us at clientsupport@rim.com.

FIGURA V. 30 Links de descarga proporcionados por RIM

Fuente: Elaboración propia

- Una vez dentro de la página a la que nos re direcciona el link se obtiene el programa así como las licencias para dispositivos BlackBerry y las licencias para dispositivos Android e IOS

  La figura V.31 muestra las licencias tanto para los dispositivos así como para el administrador BES10:



BlackBerry

Distribution Center for BlackBerry Software

Thank you for using the BlackBerry wireless solution. Here you can find information on your order. Be sure to print out this page and keep for your records.

Order Information

Please find your order information below.

Product	Download Available
EMM Corporate Trial CAL Quantity: 1 › Number 1 of 1 › CAL ID: C0017168558 › CAL Authentication Key: bdst60-rn930r-hxh77g-jqmkwp-848td5	
EMM SWS Trial CAL Quantity: 1 › Number 1 of 1 › CAL ID: C0017168559 › CAL Authentication Key: udst60-k4070k-30qdbc-rtdz65-fnzn16	
BES10 Server License v10.x Quantity: 1 › Number 1 of 1 › SRP ID: S86200425 › SRP Authentication Key: p3w8-77zv-xcg8-9dgp-yrge-qjbb-jqbd-dkxz-24kn-n8fh	Download

FIGURA V. 31 Licencias BES 10

Fuente: Elaboración propia

- Una vez descargado el software se procede a la instalación en el servidor
  - El primer paso es colocar el nombre, el de la organización y el país, luego de esto se debe aceptar las condiciones de uso.

    En la figura V.32 aparece la consola de instalación pidiendo el acuerdo de licencia con RIM:

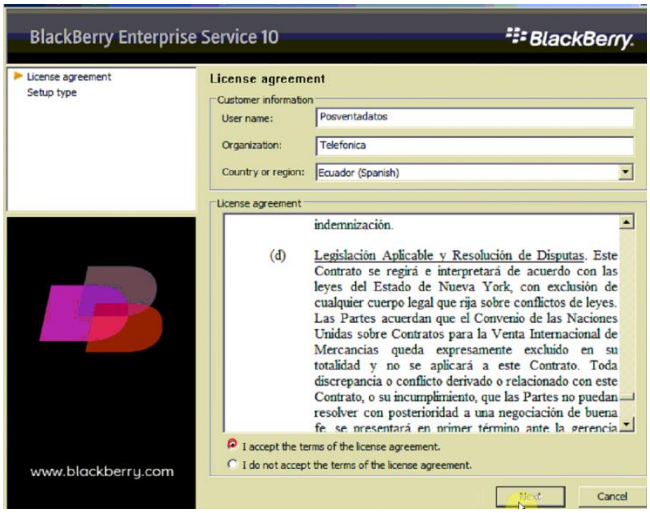


FIGURA V. 32 Acuerdo de Licencia BES10

Fuente: Elaboración propia

  - Como siguiente paso se pide el tipo de instalación en la cual ofrece crear una base de datos en el caso que no existiera una en la empresa, este es el caso ya que la base de datos no existe

    En la figura V.33 aparece la consola de instalación solicitando el tipo de instalación:

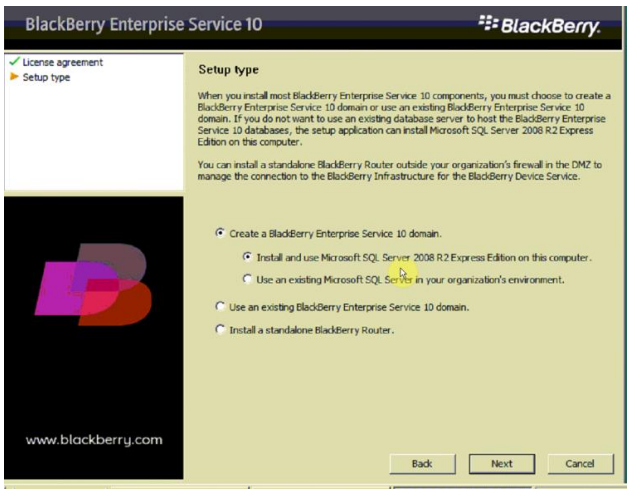


FIGURA V. 33 Tipo de instalación BES10

Fuente: Elaboración propia

- En la figura V.34 el programa de instalación comprueba los requisitos, si salen signos de pregunta esto quiere decir que el servidor no posee estos programas pero el instalador BES los va a instalar, si nos aparecen signos de admiración esto quiere decir que primero se debe instalar estos componentes antes de seguir con la instalación:

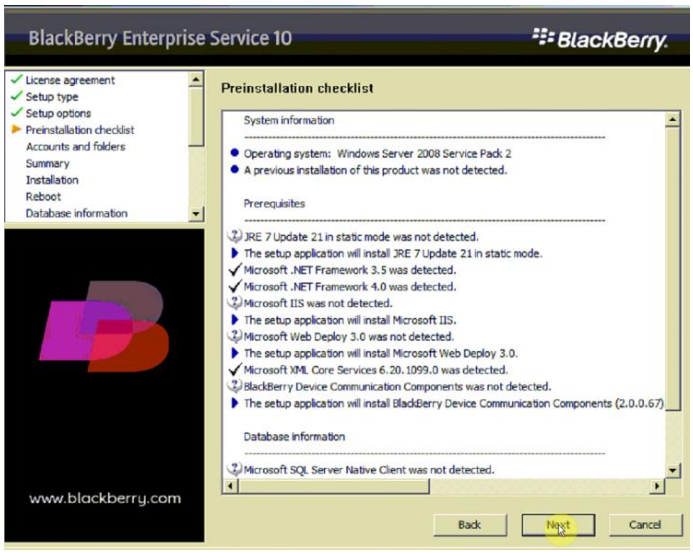


FIGURA V. 34 Check de verificación BES10

Fuente: Elaboración propia

- Como siguiente paso en la figura V.35 se comprueba la ubicación destino de los archivos así como requiere un password de administrador para permitir que el programa modifique el sistema

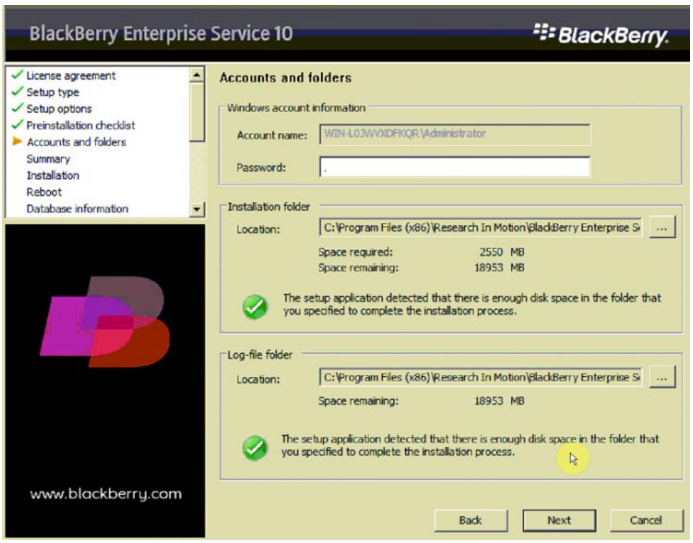


FIGURA V. 35 Password de administrador BES10

Fuente: Elaboración propia

- Como último paso en la figura V.36 comienza la instalación de los servicios de BES 10

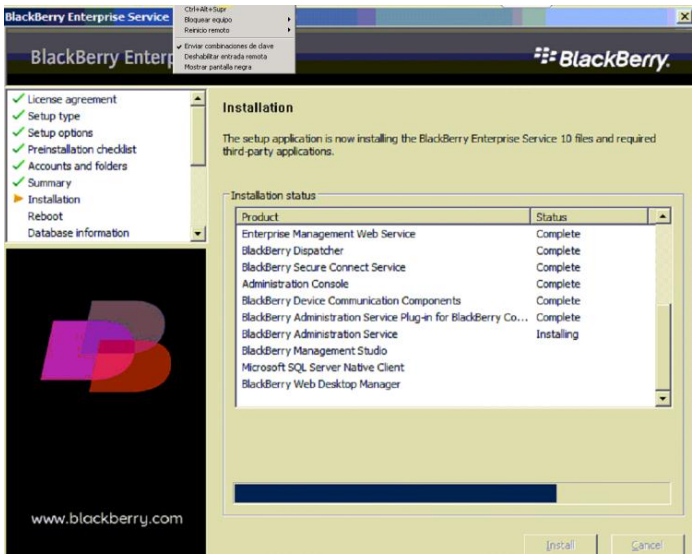


FIGURA V. 36 Ventana de instalación BES10

Fuente: Elaboración propia

- Una vez completada la instalación de los servicios, se procede a la creación de la base de datos SQL como muestra la figura V.37

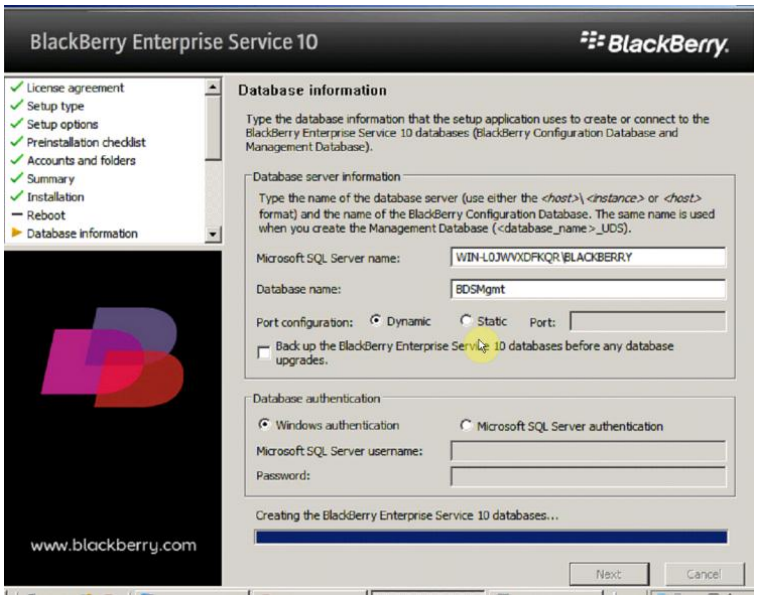


FIGURA V. 37 Creación de base de datos SQL en BES10

Fuente: Elaboración propia

- Una vez creada la base de datos, se abre una ventana de registro de licencia SRP de BES 10 como se muestra en la figura V.38, en la cual introducimos la licencia que se envió al correo.

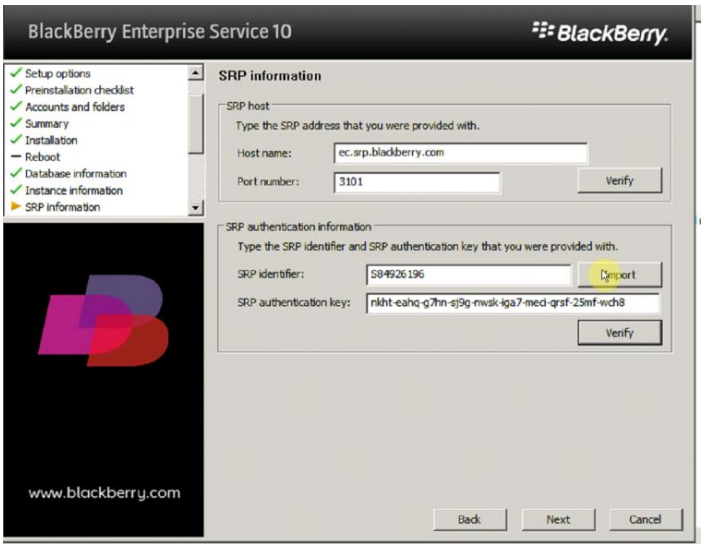


FIGURA V. 38 Verificación de licencias BES10

Fuente: Elaboración propia

- Como siguiente paso el programa hace una confirmación de contraseñas y de puertos activos tal como indica la figura V.39

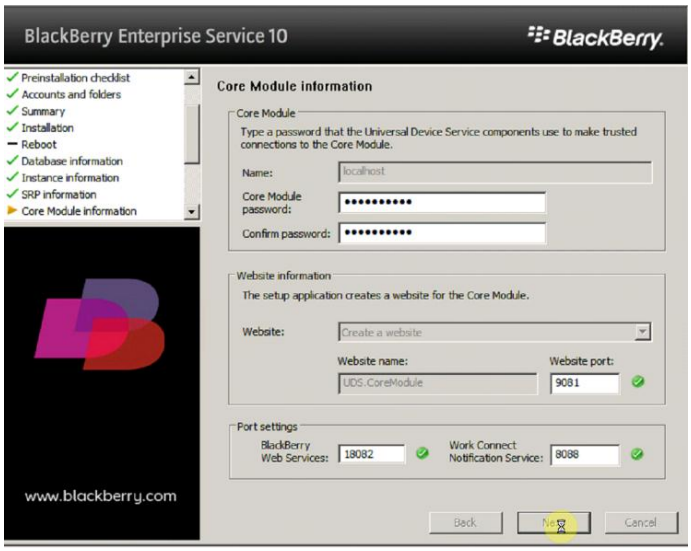


FIGURA V. 39 Confirmación de puertos activos BES10

Fuente: Elaboración propia

- Ahora se crea una cuenta por defecto y un password, el cual servirá para la administración mediante las consolas que BES 10 ofrece

  La figura V.40 muestra esta ventana:

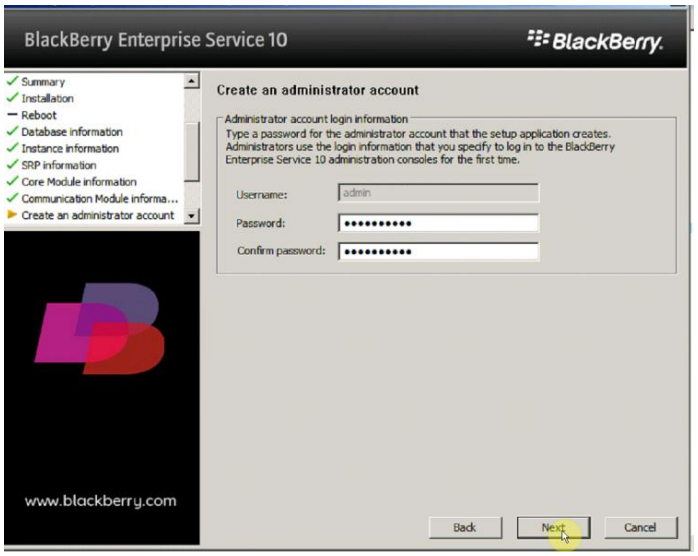


FIGURA V. 40 Contraseña para administrar BES10

Fuente: Elaboración propia

- Ahora en la figura V.41 se pide el ingreso del usuario de correo anteriormente creado en Exchange para ser administrador, el cual es BESAdmin y está en el dominio posventadatos.ec

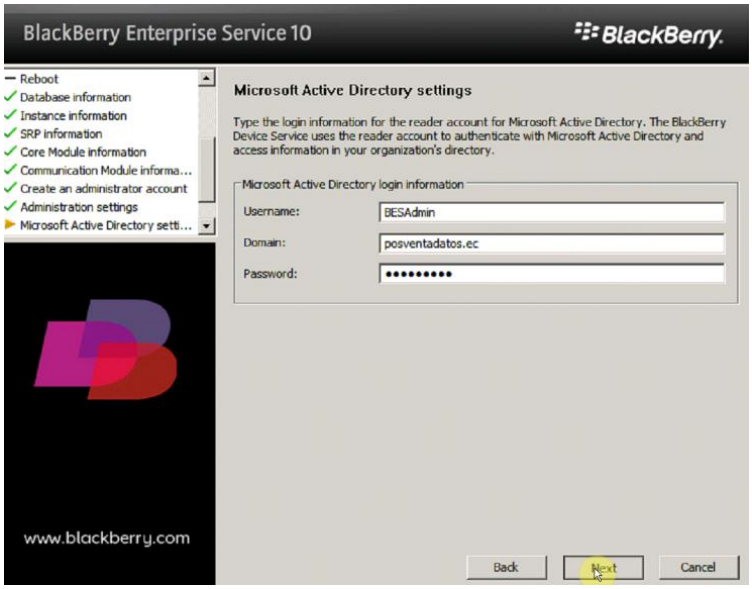


FIGURA V. 41 Requerimiento de datos de usuario BES10

Fuente: Elaboración propia

- Al final el programa inicializa todos los servicios de BES 10 como indica la figura V.42

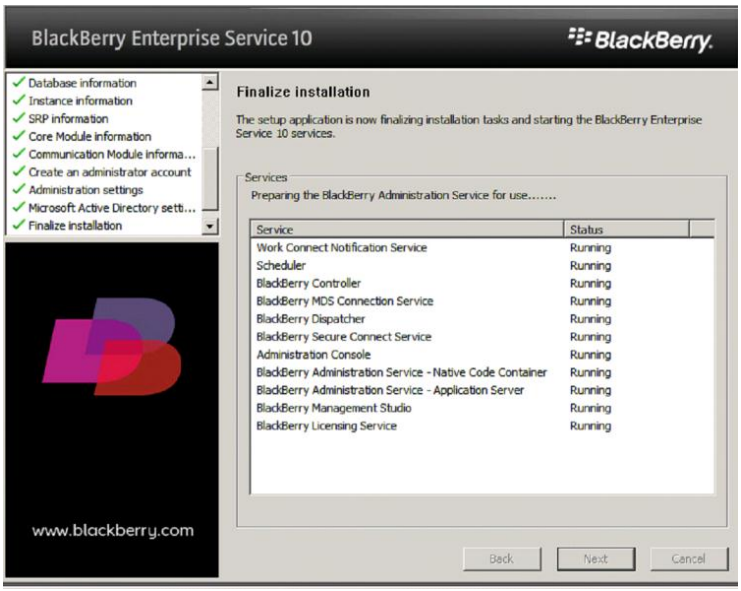


FIGURA V. 42 Inicialización de servicios en BES10

Fuente: Elaboración propia

5.3.3. ACTIVACIÓN DE LICENCIAS BES 10.1.1

- Una vez instalada la solución BES 10 se crea automáticamente un documento de texto en donde se obtiene los links de entrada a las consolas los cuales son:
  - **BlackBerry Management Studio address:**

    https://bes10.posventadatos.ec:7443

    En esta consola se debe activar las licencias de los dispositivos y los dispositivos como usuarios
  - **UDS address:**

    https://bes10.posventadatos.ec:6443

    En esta consola se administra los dispositivos IOS y Android
  - **BDS address:**

    https://bes10.posventadatos.ec:38443/webconsole/login

    En esta consola se administran los dispositivos BlackBerry y se administra las demás cuentas.
  - **BlackBerry Web Desktop Manager address:**

    https://bes10.posventadatos.ec:38443/webdesktop/login

    Tiene las mismas funcionalidades de BDS

  Estas consolas al ser ejecutadas van a tener errores en los certificados con los navegadores por lo cual se debe añadir certificados de BlackBerry.

- Para activar las licencias se debe ingresar a la consola BlackBerry Managment Studio a través del link https://bes10.posventadatos.ec:7443 y luego se debe ubicar la pestaña lísense, tal como muestra la figura V.43:

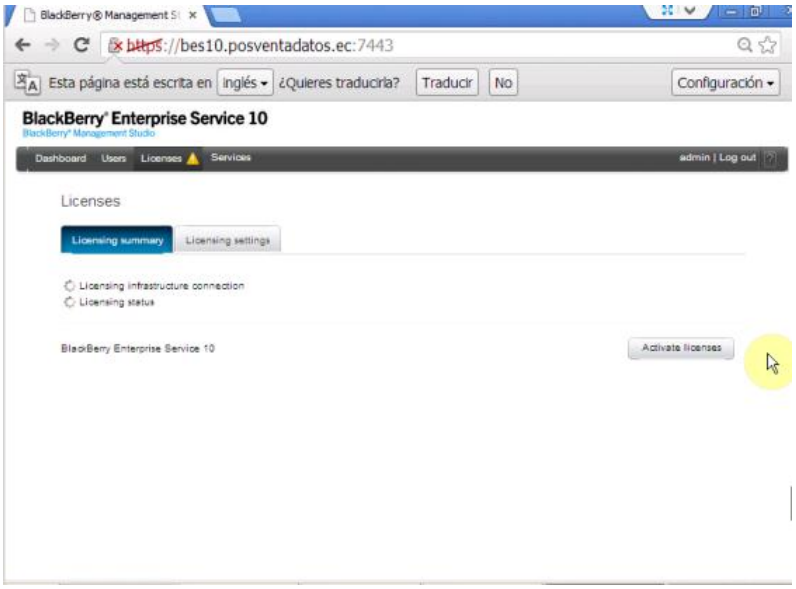


FIGURA V. 43 Activación de licencias en la consola BlackBerry Managment Studio

Fuente: Elaboración propia

- Se debe ingresar las licencias Cal que enviadas a la cuenta de correo y activarlas. LA figura V.44 indica la activación de licencias:

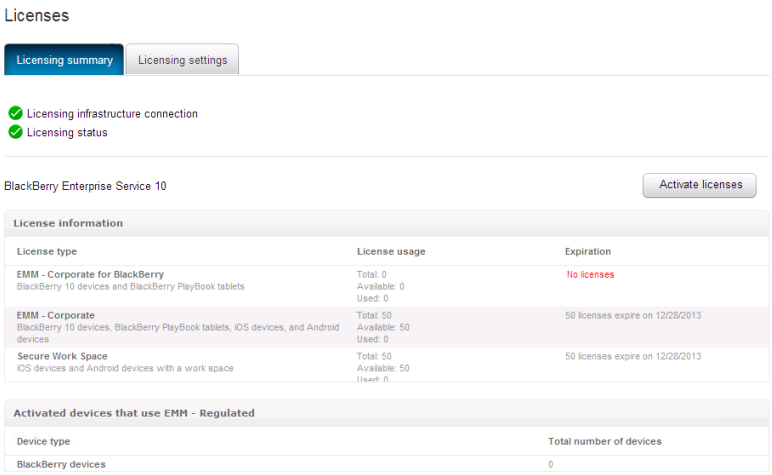


FIGURA V. 44 Activación de licencias CAL BES10

Fuente: Elaboración propia

Es así como se finaliza la instalación de la solución BES 10.1.1

5.4. Consolas de administración

Las consolas que BlackBerry Enterprise brinda para la administración son:

- BlackBerry Managment Studio
- UDS
- BAS Service
- BlackBerry Web Desktop Manager

5.4.1. BlackBerry Management Studio

Esta consola de administración permite entre varias funciones las siguientes:

- Activación de licencias CAL para dispositivos BlackBerry OS10
- Activación de licencias CAL para dispositivos Android e IOS
- Resumen de los dispositivos administrados
- Cuadro de funcionamiento de los dispositivos
- Obtención de certificados APN
- Obtención de certificados CA
- Resumen compacto de las demás consolas

5.4.2. UDS

Esta consola de administración permite entre varias funciones las siguientes:

- Creación de usuarios para dispositivos Android e IOS
- Manejo de usuarios
- Creación de perfiles para usuarios Android e IOS, los que pueden ser:
    - WI-FI
    - VPN
    - Correo
    - Proxy
- Manejos de los perfiles creados
- Creación de reglas de políticas IT
- Manejo de los usuarios a través de las políticas IT
- Administración de seguridad de usuarios Android e IOS

5.4.3. BAS

Esta consola de administración permite entre varias funciones las siguientes:

- Creación de usuarios para dispositivos BlackBerry OS10
- Manejo de usuarios
- Creación de perfiles para usuarios BlackBerry OS10, los que pueden ser:
    - WI-FI
    - VPN
    - Correo
    - Proxy
- Manejos de los perfiles creados
- Creación de reglas de políticas IT
- Manejo de los usuarios a través de las políticas IT
- Administración de seguridad de usuarios BlackBerry OS10

5.4.4. BlackBerry Web Desktop Manager

Esta consola ofrece las mismas funcionalidades de BAS pero para realizar la gestión desde una página web externa a la compañía.

CAPÍTULO VI

ADMINISTRACIÓN DE USUARIOS CORPORATIVOS

6.1. INTRODUCCIÓN

El presente capitulo detalla las pruebas realizadas en los dispositivos a través de la administración de la solución BES 10, así como la descripción de las políticas de seguridad presentes en cada plataforma

En primera instancia se detalla la creación de usuarios, la asignación del usuario corporativo y la administración a través de la solución de seguridad corporativa ya instalada

.

6.2. CREACIÓN DE USUARIOS BES 10

6.2.1. Usuarios BlackBerry

Para la creación de usuarios BLACKBERRY se realizó los siguientes pasos:

1. Se ingresa a la consola de BAS como muestra la figura VI.1

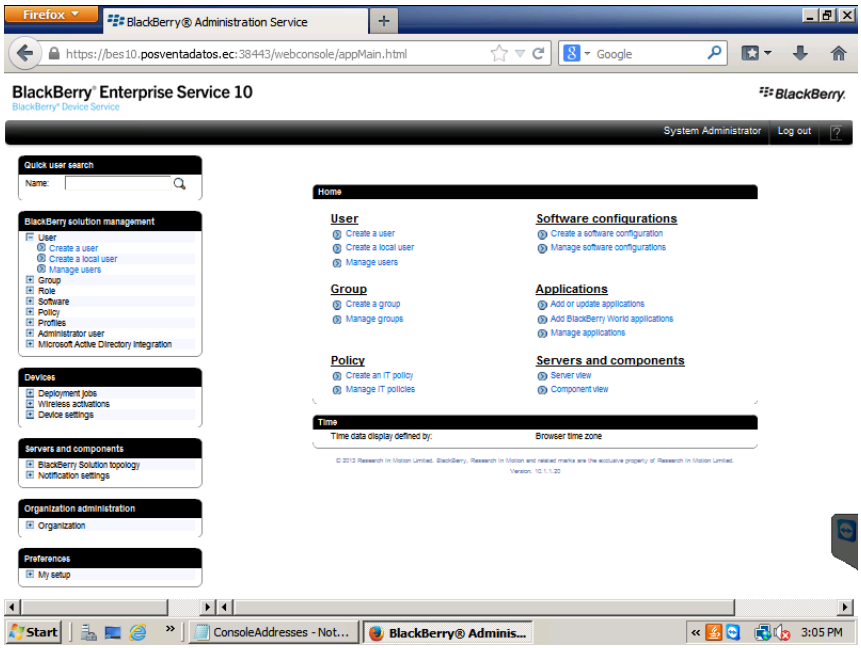


FIGURA VI. 1 Ingreso a la consola BAS

Fuente: Elaboración propia

2. Se selecciona la opción create user como muestra la figura VI.2

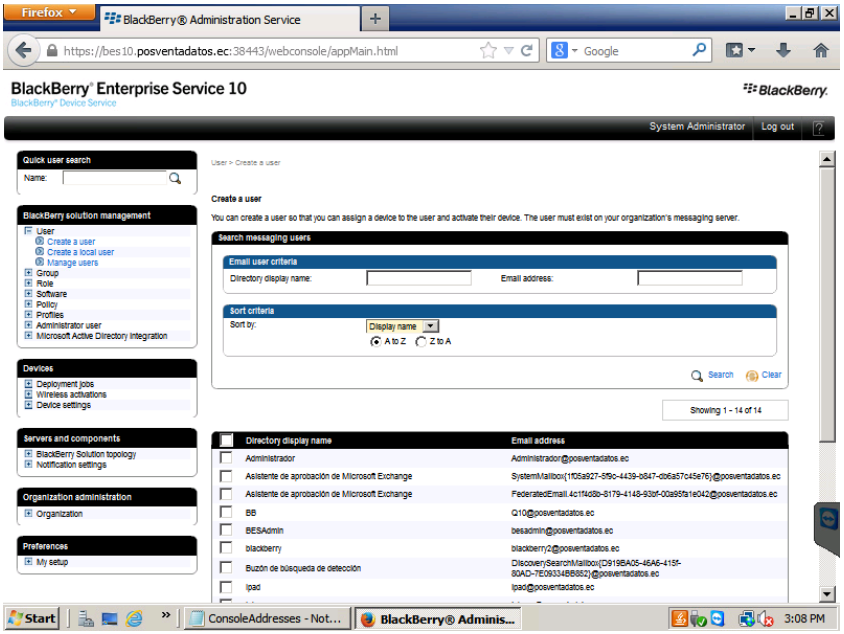


FIGURA VI. 2 Consola de creación de usuario

Fuente: Elaboración propia

3. Una vez desplegados los usuarios de la base de datos de Exchange se selecciona el usuario a crear como muestra la figura VI.3

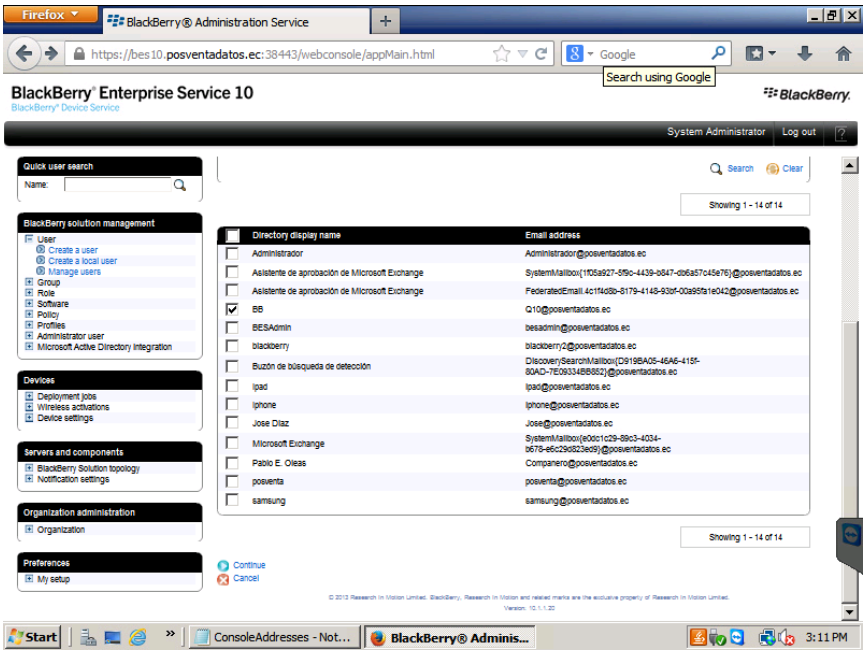


FIGURA VI. 3 Selección de usuario

Fuente: Elaboración propia

4. En el usuario se escogen las opciones tanto de grupo como de correo además el password de activación como lo indica la figura VI.4

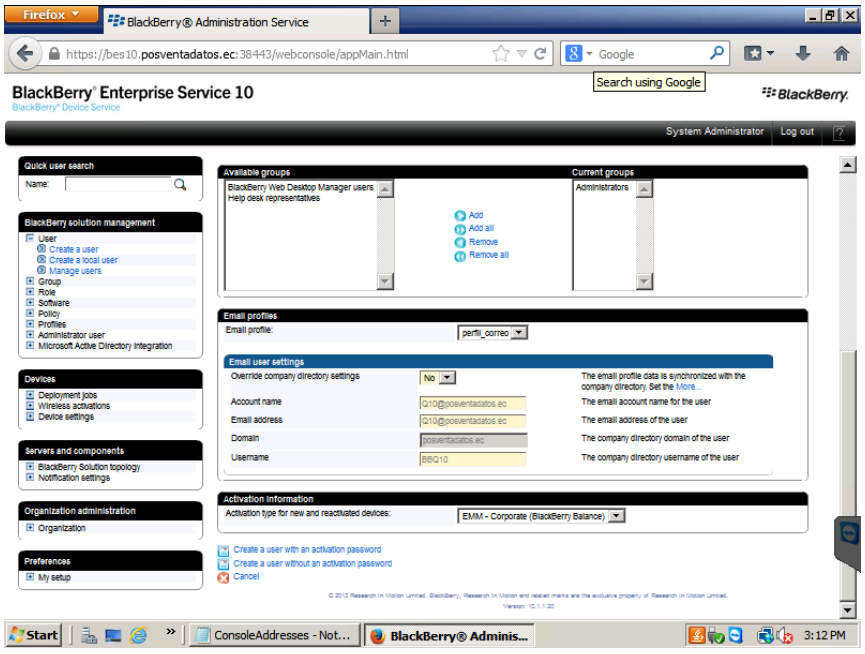


FIGURA VI. 4 Propiedades del usuario

Fuente: Elaboración propia

5. Se crea un password de activación y la expiración de la misma, esta debe ser ingresado por el usuario para la activación tal como lo muestra la figura VI.5

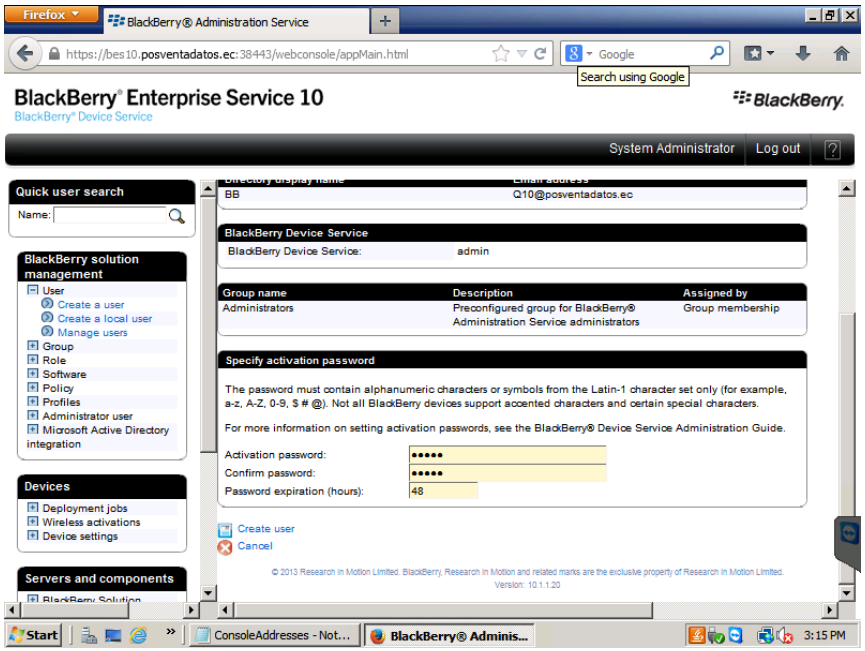


FIGURA VI. 5 Contraseña de activación

Fuente: Elaboración propia

6. El usuario ha sido satisfactoriamente creado como lo indica la figura VI.6

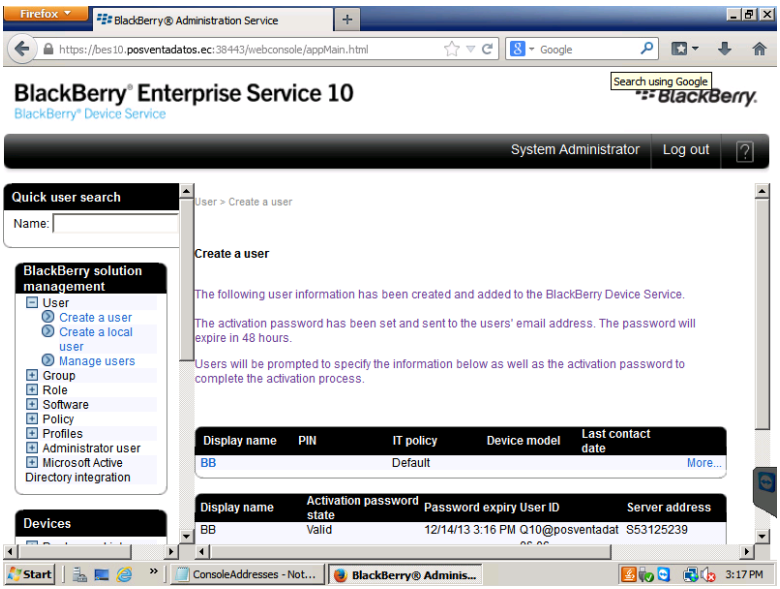


FIGURA VI. 6 Mensaje de creación de usuario

Fuente: Elaboración propia

6.1.2. Usuarios Android e IOS

La creación de usuarios Android e IOS puede ser realizada de manera semejante ya que los dos sistemas utilizan una misma consola de administración la cual es UDS, para la cual se siguen los siguientes pasos:

1. Ingresamos a la consola UDS la cual maneja la administración de dispositivos Android e IOS, la figura VI.7 muestra la consola UDS

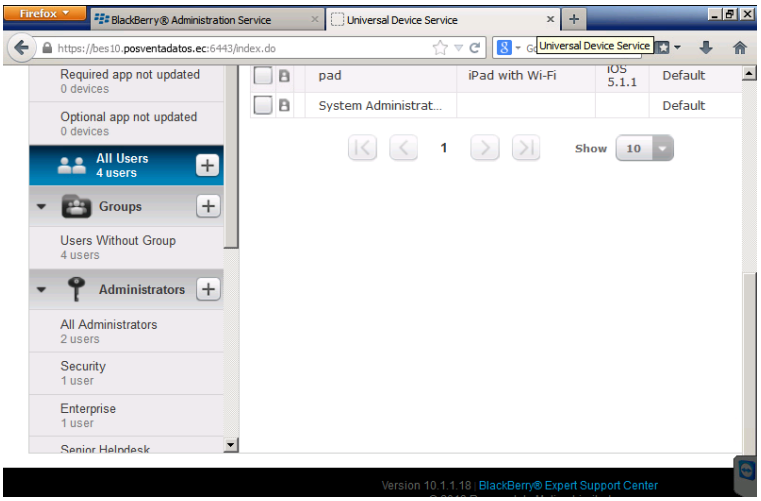


FIGURA VI. 7 Consola UDS

Fuente: Elaboración propia

2. En All Users se da click en el signo + con lo cual aparece una ventana emergente para la creación del usuario como se indica en la figura VI.8

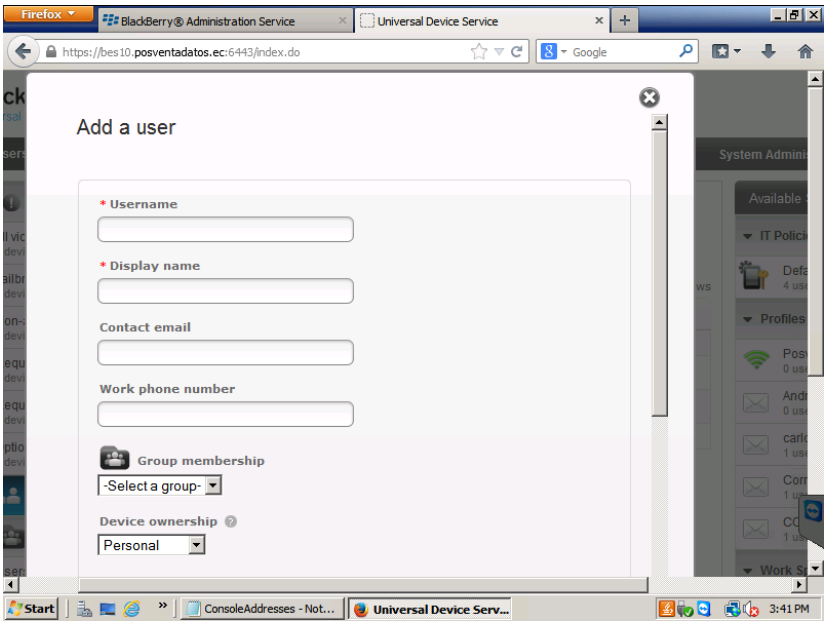


FIGURA VI. 8 Ventana de creación de usuario UDS

Fuente: Elaboración propia

3. Se ingresa los datos requeridos para la creación del usuario, como muestra la figura VI. 9, estos datos son:

- Datos del usuario
- Cuenta de administrador
- Opciones de activación

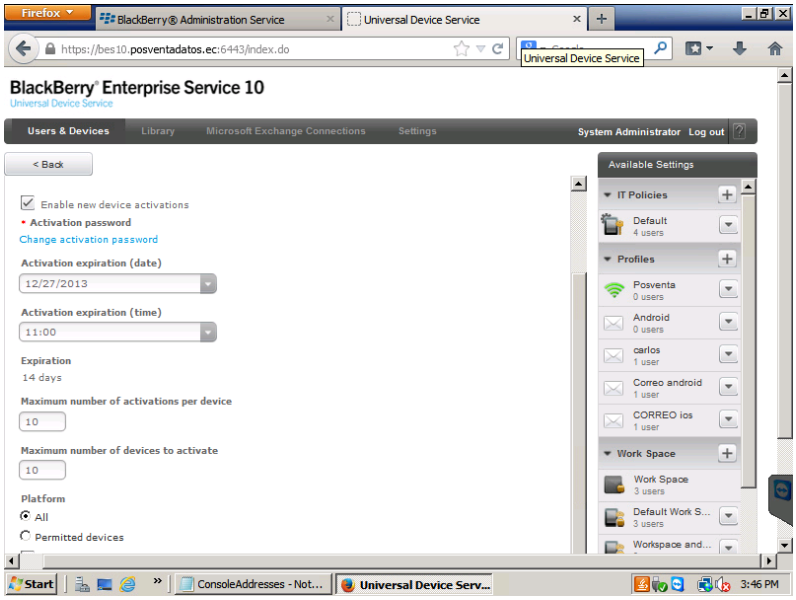


FIGURA VI. 9 Datos para la creación de usuarios

Fuente: Elaboración propia

4. Como punto final queda el usuario en espera de la activación como se muestra la figura VI.10

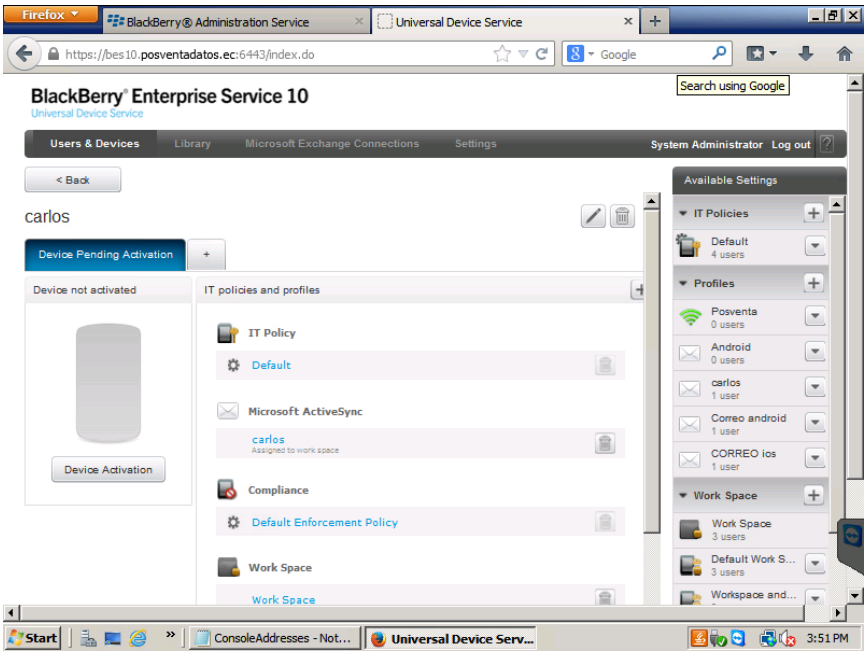


FIGURA VI. 10 Usuario pre activación

Fuente: Elaboración propia

6.3. Asociación de usuarios a la solución multiplataforma

6.3.1. Dispositivo BlackBerry

El usuario con sistema operativo BlackBerry OS10 posee un equipo BlackBerry Q10 el cual consta de las siguientes características:

- Nombre de dispositivo: BLACKBERRY-3D2B
- Modelo: BlackBerry Q10
- Numero de modelo: SQN100-1
- Versión de OS: 10.1.0.273
- Número de serie: 0720-9771-9560 (IMEI)

Este usuario es el primero en añadirse a la solución BES 10, para lo cual se realizó los siguientes pasos:

- En el dispositivo se añade una nueva cuenta de trabajo como lo indica la figura VI.11

FIGURA VI. 11 Creación de cuenta de trabajo

Fuente: Elaboración propia

- Los requisitos para crear esta cuenta son el ID de usuario, una contraseña de activación temporal y el SRPID de nuestro servidor como se muestra en la figura VI.12

FIGURA VI. 12 Requisitos cuenta de trabajo

Fuente: Elaboración propia

- En la comunicación con el servidor, el dispositivo muestra algunos mensajes como los que se muestra en la figura VI.13

FIGURA VI. 13 Mensajes de asociación BES 10

Fuente: Elaboración propia

- Una vez que el dispositivo se conecte con el servidor este asocia la cuenta de correo de la empresa para lo cual pide la contraseña de usuario que se creó en el servidor EXCHANGE como muestra la figura VI.14

FIGURA VI. 14 Mensajes de asociación BES 10

Fuente: Elaboración propia

- Una vez conectado con el servidor ya se ha creado el espacio de trabajo tal y como muestran las figuras VI.15 y VI.16

FIGURA VI. 15 Cuentas de usuario corporativo

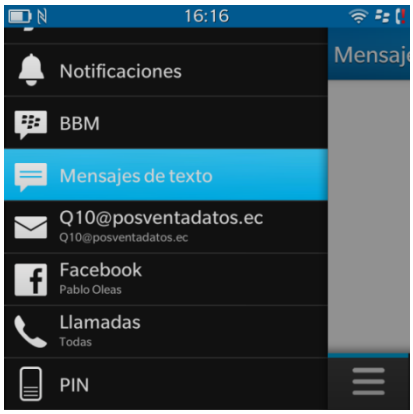


FIGURA VI. 16 Hub de usuario corporativo

Fuente: Elaboración propia

Una vez completados estos pasos la consola BlackBerry Managment Studio reconoce el dispositivo con todas sus características como muestra la figura VI.17

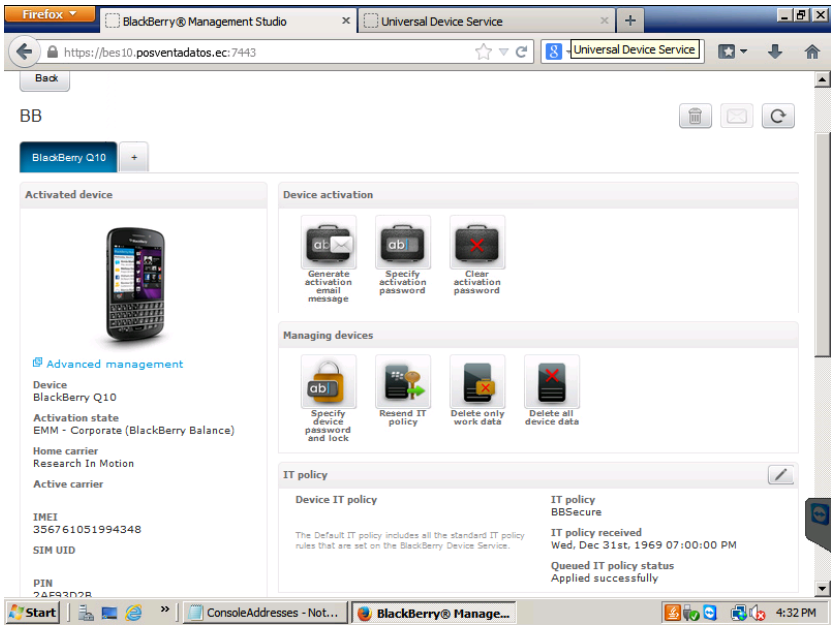


FIGURA VI. 17 Consola de administración rápida BDS

Fuente: Elaboración propia

6.3.2. Dispositivo iOS

6.3.2.1. Certificado APN

Para la creación de usuarios bajo sistema operativo IOS se necesita obtener un certificado firmado de Apple llamado certificado APN el cual es requisito para que exista comunicación entre la solución BES 10 y el dispositivo funcionando bajo IOS, cabe destacar que para dispositivos con sistema operativo Android no es necesario generar un certificado firmado diferente al que nos proporciona RIM ya que en su mayoría este sistema es libre por lo cual funciona con cualquier certificado de seguridad.

Para obtener el certificado APN antes mencionado deben se sigue los pasos a continuación, los cuales permiten que RIM pida a Apple un certificado de funcionamiento en esta solución. Los pasos son:

1. Se ingresa a la consola de UDS y se selecciona el campo settings tal como nos muestra la figura VI.18

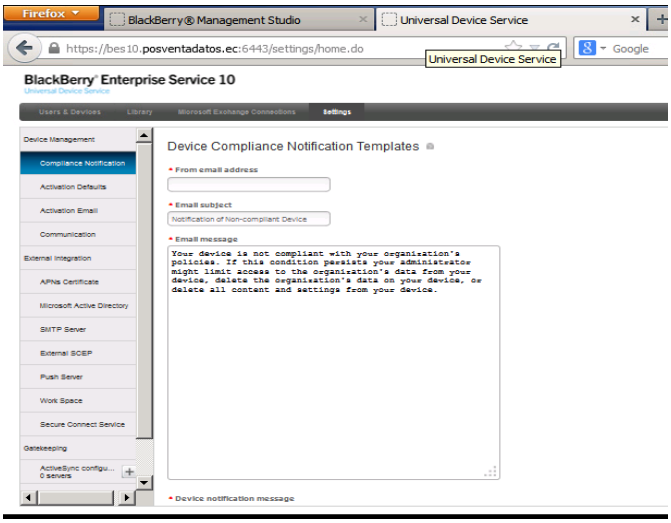


FIGURA VI. 18 Ventana settings de UDS

Fuente: Elaboración propia

2. Se ubica la opción APN Certificate en la cual se debe realizar la petición a RIM de un certificado firmado temporal, el cual Apple lo toma como garantía antes de aprobar el certificado tal como lo demuestra la figura VI.19

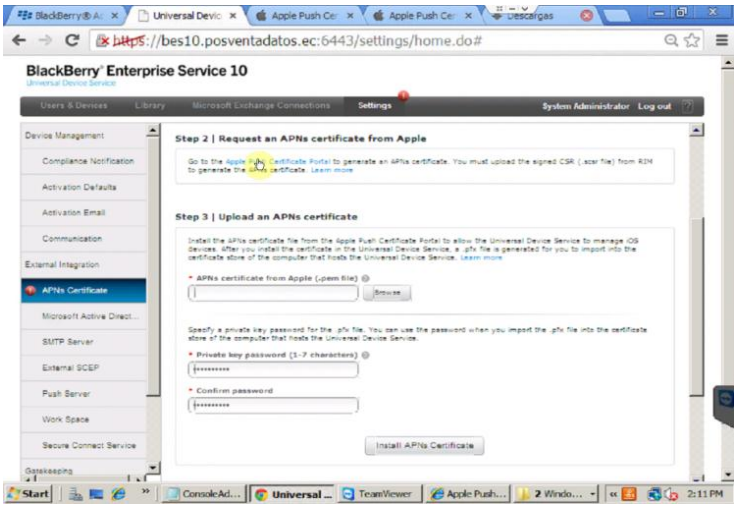


FIGURA VI. 19 Obtención de certificado firmado por RIM

Fuente: Elaboración propia

3. Cuando RIM envía al correo el certificado temporal firmado, se ingresa al portal de certificados de Apple cuya dirección es: https://identity.apple.com/pushcert/, en esta dirección creamos un certificado APN. La figura VI.20 muestra el portal de certificados de Apple

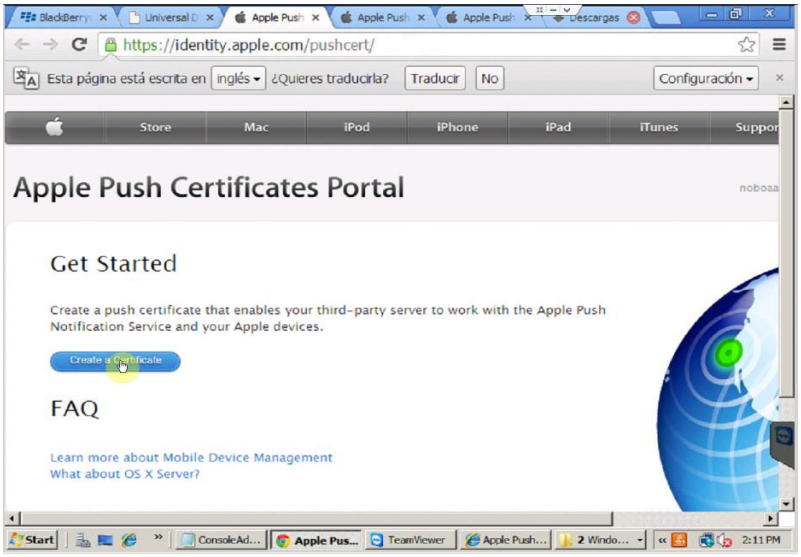


FIGURA VI. 20 Obtención de certificado firmado por RIM

Fuente: Elaboración propia

4. Se sube a esta página el certificado temporal que nos proporcionó RIM tal como muestra la figura VI.21

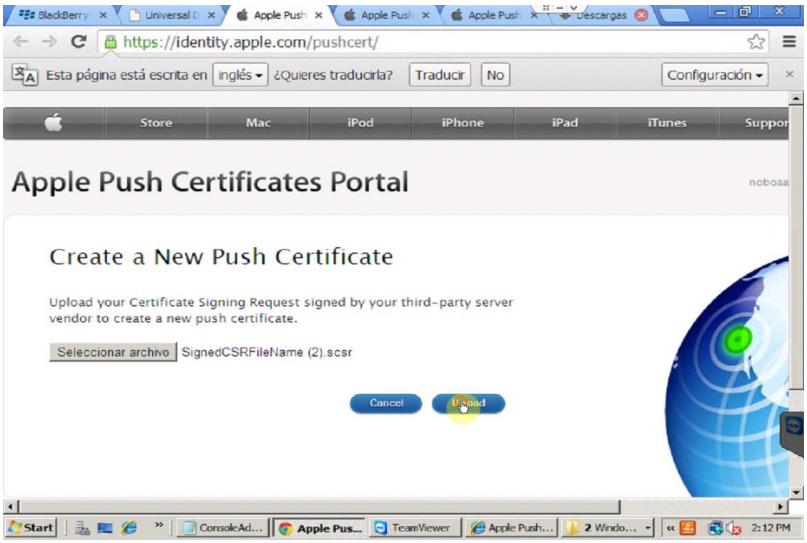


FIGURA VI. 21 Upload SignedCSR

Fuente: Elaboración propia

5. Una vez obtenido el password del certificado en la consola UDS se genera este certificado y se lo guarda en el equipo tal y como muestra la figura VI.22

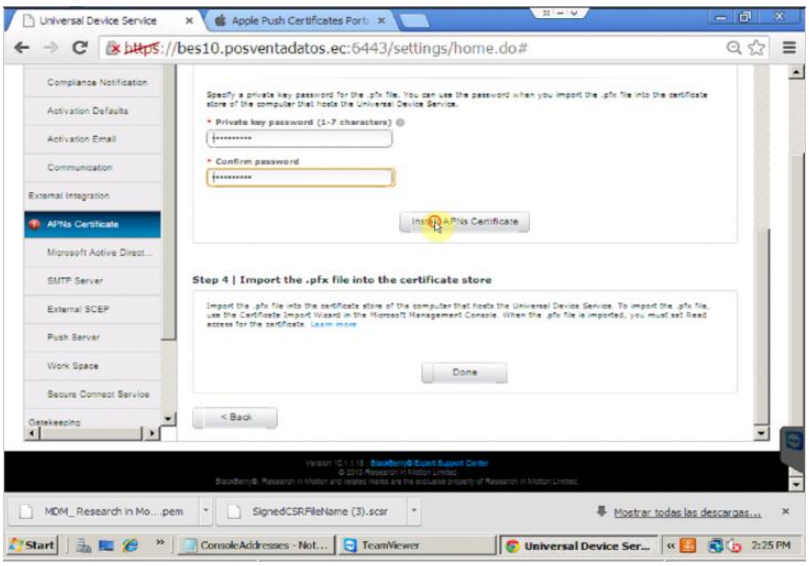


FIGURA VI. 22 Petición Certificado APN

Fuente: Elaboración propia

6. Como último paso se carga el certificado en el servidor con un proceso de administrador para que quede registrado en nuestro servidor, tal y como muestra la figura VI.23

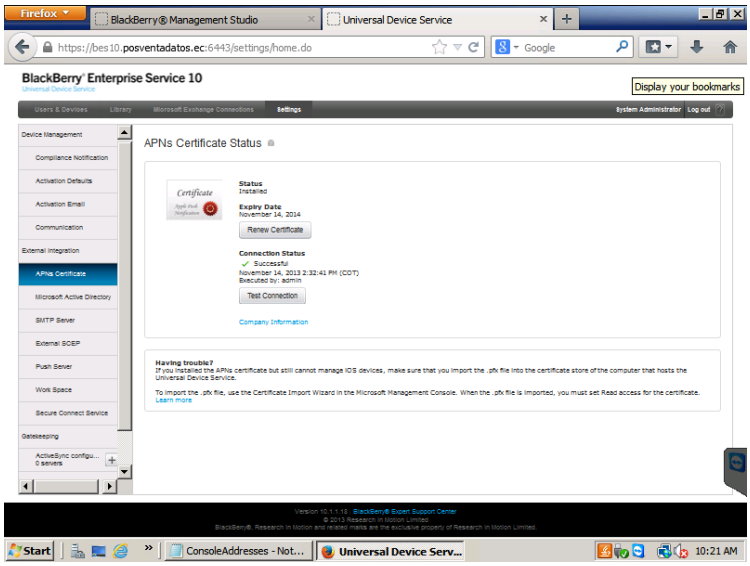


FIGURA VI. 23 Certificado APN

Fuente: Elaboración propia

6.2.2.2. Dispositivo IOS y Android

El usuario con sistema operativo iOS 6 posee un equipo iPhone 4 el cual consta de las siguientes características:

- Nombre de dispositivo: Iphone Andrés
- Modelo: Iphone 4
- Numero de modelo: MD128E/A
- Versión de OS: 6.1 (10B144)
- Número de serie: DNPKG93DP0N (IMEI)
-

El proceso para añadir usuarios es muy similar tanto para dispositivos IOS como para dispositivos Android por lo cual se detalla como uno solo y es el siguiente:

:

- En el dispositivo se descargó la aplicación BES10 Client, desde la App Store. En la siguiente figura VI.24 la cual mostró la interfaz de App Store.

FIGURA VI. 24 interfaz de App Store

Fuente: Elaboración propia

- Se ingresó a la aplicación, se eligió idioma. En las figuras VI.25 y VI.26 se muestra la interfaz de la aplicación en cero.

FIGURA VI. 25 Aplicación BES 10 client

FIGURA VI. 26 Idioma BES 10 client

Fuente: Elaboración propia

- El dispositivo tuvo que ser conectado al servidor UDS de acceso público en éste caso la dirección ec.bbsecure.com/s53125239. En las siguientes figuras VI.27 y VI.28 se mostró la interfaz de ingreso al servidor como el certificado para la comunicación.

FIGURA VI. 27 Interfaz de ingreso

FIGURA VI. 28Certificado APN

Fuente: Elaboración propia

- Previamente al ingreso de usuario éste debe estar creado en el servidor BES10 y también debe estar hecha la notificación de que es posible registrar usuario. En la siguiente figura VI.29 se mostró la interfaz de ingreso de credenciales.

FIGURA VI. 29 Ingreso de credenciales para activación

Fuente: Elaboración propia

- El asistente pide instalar un certificado, como previamente se instaló el certificado APN en el bes10, solamente se sigue el asistente. En las siguientes figuras VI.30, VI.31, VI.32, se mostraron las interfaces de activación.

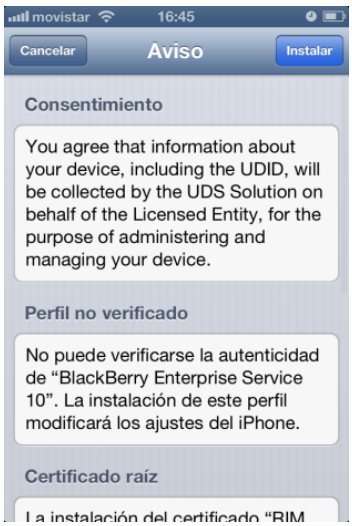


FIGURA VI. 30 **Aviso de activación**

FIGURA VI. 31 **Instalación de requisitos**

Fuente: Elaboración propia

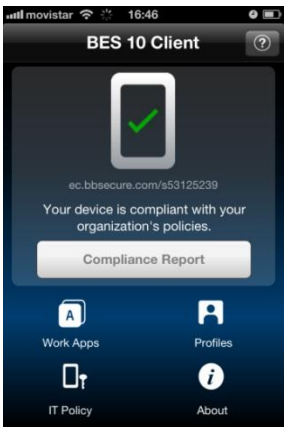


FIGURA VI. 32 **Entorno del servidor en IOS y Android**

Fuente: Elaboración propia

- En esta instancia el servidor empezó hacer cambios en el dispositivo con las políticas IT y de workspace por defecto. En las siguientes figuras VI.33, VI.34, VI.35, VI.36. se mostró las interfaces de los cambios que hace BES 10 en el dispositivo.

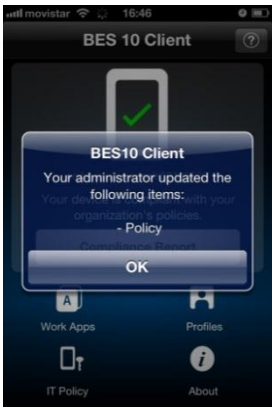


FIGURA VI. 33 Aviso de cambios de políticas

FIGURA VI. 34Políticas IT del usuario

Fuente: Elaboración propia

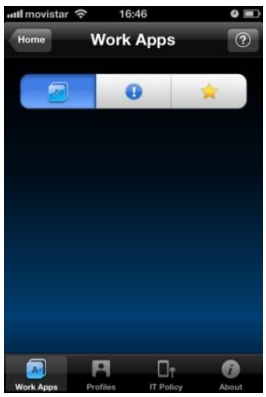


FIGURA VI. 35 Entorno de aplicaciones

FIGURA VI. 36 Entorno de Trabajo

Fuente: Elaboración propia

- Desde la consola se envía la petición de instalación de aplicaciones del workspace. En la figura V. se mostró la interfaz del workspace vacío. En las figuras VI.37 se mostró la instalación de aplicaciones del workspace.

FIGURA VI. 37Petición de instalación de aplicaciones en workspace

Fuente: Elaboración propia

- El servidor pidió ingresar una contraseña para el workspace. En la siguiente figura VI.38 se mostró la interfaz de ingreso de contraseña para el workspace.

FIGURA VI. 38 Ingreso de contraseña para el workspace

Fuente: Elaboración propia

- A continuación en las figuras VI.39, VI.40, VI.41, VI.42, se observa el ingreso del correo corporativo work connect, su configuración e interfaz.

FIGURA VI. 39 Ingreso de usuario de correo

FIGURA VI. 40 Ingreso de credenciales de correo

FIGURA VI. 41 Validación de usuario de correo

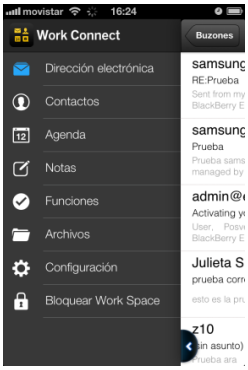


FIGURA VI. 42 Correo corporativo

Fuente: Elaboración propia

Una vez completados estos pasos la consola BlackBerry Managment Studio reconoce el dispositivo con todas sus características como muestra la figura VI.43

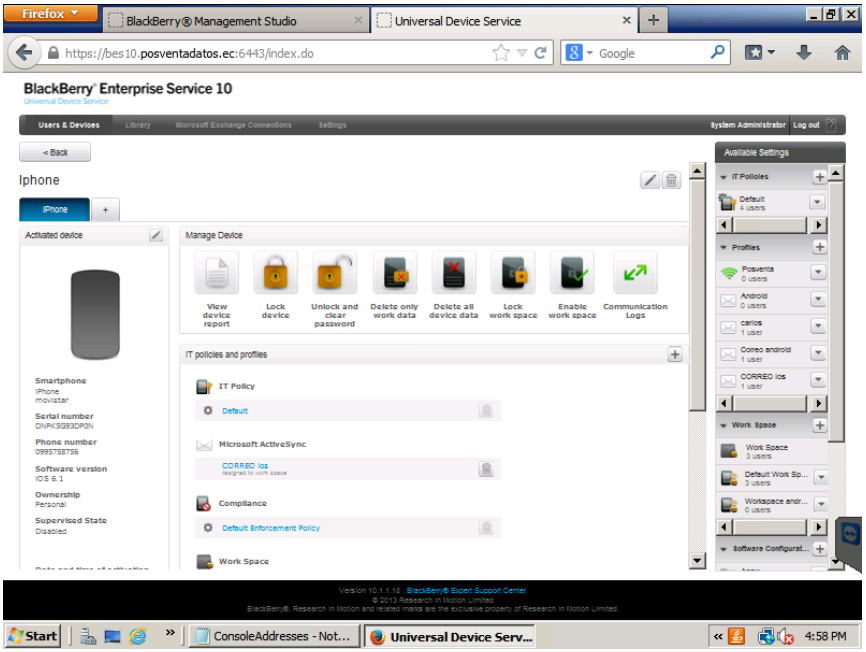


FIGURA VI. 43 Consola de administración rápida UDS

Fuente: Elaboración propia

6.4. Seguridad en entornos multiplataforma

Entre las diversas funcionalidades de la solución BES 10.1.1 se encuentra una alta cantidad de políticas que mejoran la seguridad en el entorno corporativo, estas políticas son asignadas a los usuarios en grupos llamados perfiles, los cuales comienzan a actuar luego de que sean asignados a un usuario.

6.4.1. Políticas de seguridad de la información

6.4.1.1. Dispositivos BlackBerry

6.4.1.1.1. Grupo de Reglas generales

Regla	Descripción	Valores
Hotspot WPA2-Personal Security Type rule	Específica si un dispositivo debe utilizar seguridad WPA2-Personal para conectarse a un punto de acceso, configurada en sí el usuario no puede seleccionar un tipo de seguridad diferente para conectar el dispositivo a un punto de acceso.	• SI • NO
Mobile Hotspot Mode and Tethering rule	Especifica si se permite el modo de punto de acceso móvil, la inmovilización mediante la tecnología Bluetooth, y la inmovilización mediante un cable USB en un dispositivo.	• Permitir • No permitir
Roaming rule	Especifica si un dispositivo puede utilizar los servicios de datos mediante la red inalámbrica.	• Permitir • No permitir
Wireless Service Provider Billing	Especifica si un usuario del dispositivo puede comprar aplicaciones de pago de BBM WORLD, utilizando el plan de compras para el proveedor de servicios inalámbricos de su empresa.	• Permitir • No permitir

TABLA VI. I Reglas generales dispositivos BLACKBERRY

Fuente: Elaboración propia

6.4.1.1.2. Grupo de Reglas de Hardware

Regla	Descripción	Valores
Transfer Work Contacts Using Bluetooth	Especifica si un dispositivo puede enviar contactos de trabajo a otro dispositivo activado por Bluetooth. Si se configura esta regla a No permitir, los usuarios no pueden transferir los contactos de trabajo, también evita que los usuarios transfieran los mensajes del trabajo.	• Permitir • No permitir
Bluetooth rule	Especifica si un dispositivo puede utilizar la tecnología Bluetooth.	• Permitir • No permitir
Camera rule	Especifica si un dispositivo puede utilizar la cámara.	• Permitir • No permitir
HDMI rule	Especifica si un dispositivo puede utilizar el puerto HDMI.	• Permitir • No permitir
Location Services rule	Especifica si un dispositivo puede proporcionar su ubicación geográfica a las aplicaciones que se ejecutan en el dispositivo.	• Permitir • No permitir
Wi-Fi rule	Especifica si un dispositivo puede utilizar Wi-Fi	• Permitir • No permitir

TABLA VI. II Reglas de hardware dispositivos BlackBerry

Fuente: Elaboración propia

6.4.1.1.3. Grupo de Reglas de Password

Regla	Descripción	Valores

Maximum Password Age	Especifica el tiempo que puede transcurrir antes de que caduque una contraseña para el dispositivo, en el cual el usuario debe configurar una nueva contraseña.	De 0 a 65535 dias
Maximum Password Attempts	Especifica el número de veces que un usuario puede introducir una contraseña incorrecta antes de que un dispositivo elimine los datos en el espacio de trabajo o todos los datos del dispositivo.	De 3 a 10 veces
Maximum Password History	Especifica el número máximo de contraseñas anteriores que un dispositivo, comprueba para evitar que un usuario vuelva a utilizar una contraseña anterior.	De 0 a 15 contraseñas
Minimum Password Complexity	Especifica la complejidad mínima de la contraseña para el espacio de trabajo en un dispositivo.	Todas las restricciones
Minimum Password Length	Esta regla especifica la longitud mínima de la contraseña en el dispositivo. Si no se da un valor y no se requiere una contraseña de espacio de trabajo, la longitud mínima de la contraseña es de 4	De 4 a 32 caracteres
Security Timeout	Especifica el número máximo de minutos de inactividad del usuario para cerrar el espacio de trabajo.	De 5 a 60 minutos

TABLA VI. III Reglas de password dispositivos BlackBerry

Fuente: Elaboración propia

6.4.1.1.4. Grupo de Reglas de Seguridad

Regla	Descripción	Valores
BlackBerry Bridge	Especifica si un dispositivo BlackBerry 10 puede permitir a una tableta BlackBerry	• Permitir

rule	PlayBook, acceder a los datos de trabajo en el smartphone utilizando la aplicación BlackBerry Bridge.	• No permitir
Backup and Restore Device rule	Especifica si un usuario del dispositivo puede realizar copias de seguridad y restaurar las aplicaciones a través de BlackBerry Link.	• Permitir • No permitir
Computer Access to Device rule	Esta regla especifica si un ordenador puede acceder a contenido en un dispositivo a través de una conexión USB o la opción de compartir archivos con Wi-Fi.	• Permitir • No permitir
Media Card rule	Especifica si un dispositivo puede acceder a la tarjeta de memoria.	• Permitir • No permitir
Voice Dictation rule	Especifica si un usuario puede utilizar el dictado de voz en el dispositivo.	• Permitir • No permitir
Wipe the Device Without Network Connectivity rule	Especifica el tiempo en horas que deben transcurrir sin un dispositivo se conecta a la red de su organización antes de que el dispositivo elimine todos los datos del dispositivo.	De 2 a 8760 horas

TABLA VI. IV Reglas de seguridad dispositivos BlackBerry

Fuente: Elaboración propia

6.4.1.1.5. Grupo de Reglas de Software

Regla	Descripción	Valores

BBM rule	Especifica si BlackBerry Messenger está disponible en el dispositivo	• Permitir • No permitir
BlackBerry Maps rule	Especifica si un dispositivo puede utilizar la aplicación BlackBerry Maps.	• Permitir • No permitir
BlackBerry Protect rule	Especifica si un dispositivo puede utilizar la aplicación BlackBerry Protect.	• Permitir • No permitir
Hotspot Browser rule	Especifica si un dispositivo puede utilizar el navegador de BlackBerry para conectarse a un punto de acceso.	• Permitir • No permitir
Media Sharing rule	Especifica si un dispositivo puede compartir música, fotos y vídeos a través de una conexión Wi-Fi con dispositivos con certificación DLNA.	• Permitir • No permitir
Non-Email Accounts rule	Especifica si un usuario puede agregar cuentas de terceros para servicios, tales como Facebook, Twitter, LinkedIn, y Evernote al dispositivo.	• Permitir • No permitir
SMS/MMS rule	Esta regla especifica si un dispositivo puede enviar mensajes de texto SMS y mensajes MMS.	• Permitir • No permitir
User-Created VPN Profiles rule	Esta regla especifica si un usuario del dispositivo BlackBerry puede crear perfiles VPN en un dispositivo.	• Permitir • No permitir

TABLA VI. V Reglas de software dispositivos BlackBerry

Fuente: Elaboración propia

6.4.1.2. Dispositivos Android e IOS

6.4.1.2.1. Grupo de políticas del explorador.

Las reglas de este grupo de políticas especifican restricciones para el navegador por defecto en el dispositivo. Ëstas reglas aplican solamente en dispositivos iOS.

Política	Descripción	S.O mínimo
Hide the default web browser rule.	Al seleccionar esta regla, se desactiva el navegador Safari, y se remueve su ícono de la pantalla de inicio. Ésta regla también impide a los usuarios abrir clips web en los dispositivos.	iOS 4.0
Disable autofill in the default browser rule.	La selección de esta regla impide que el navegador Safari guarde las entradas de usuario pasadas en los formularios web para su uso posterior. (Ésta regla no es válida si la opción para ocultar el navegador web por defecto está activada).	iOS 4.0
Disable JavaScript in the default browser rule.	Al seleccionar esta regla desactiva JavaScript en el navegador Safari. El navegador ignora todo JavaScript en sitios web. (Ésta regla no es válida si la opción para ocultar el navegador web por defecto está activada).	iOS 4.0
Disable popups in the default browser rule.	Al seleccionar esta regla bloquea las ventanas pop-up en el navegador web Safari. (Ésta regla no es válida si la opción para ocultar el navegador web por defecto está activada).	iOS 4.0
Enable cookies	Ésta regla, especifica cómo el navegador web Safari manejará los cookies. Tiene 3	iOS 4.0

rule.	formas: *Siempre (always).- Los cookies será siempre aceptados* *De páginas visitadas (From visited websites).- Los cookies aceptados serán solamente los de las páginas que el usuario ha visitado directamente en el navegador, ésta regla está por defecto.* *Nunca (never).- los cookies bajo ningún motivo serán aceptados.*	
Force fraud warnings rule.	La selección de esta regla habilita advertencias de fraude en el navegador web Safari. El navegador intenta evitar que el usuario visite sitios web identificados como fraudulentos o comprometedores. (Ésta regla no es válida si la opción para ocultar el navegador web por defecto está activada).	iOS 4.0

TABLA VI. VI Políticas de explorador dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.2. Grupo de políticas de cámara y video.

Las reglas de éste grupo de políticas especifican restricciones para las cámaras y captura de pantallas de los dispositivos controlados. Todas aplican para iOS y solo una para Android.

Política	Descripción	S.O mínimo
Disable output rule.	La selección de ésta regla no permite que el dispositivo transmita videos o comparta pantallas a otros dispositivos, ésta regla impide también capturar pantallas del	iOS 4.0

	dispositivo.	
Disable screen capture rule.	Ésta regla impide capturar pantallas del dispositivo.	iOS 4.0
Hide the default camera application rule.	Ésta regla deshabilita la cámara del dispositivo, los usuarios no podrán tomar fotos ni videos.	iOS 4.0 Android OS 4.0
Hide the default video-conferencing application rule.	Ésta regla quita la aplicación Facetime de la pantalla de inicio del dispositivo, los usuarios no podrán hacer video llamadas.	iOS 4.0

TABLA VI. VII Políticas de cámara y video dispositivos IOS y Android

Fuente: Elaboración propia

6.4.1.2.3. Grupos de políticas de certificados

Las reglas de este grupo de políticas especifican parámetros para el uso de certificados en el dispositivo. Las normas se aplican sólo a los dispositivos iOS.

Política	Descripción	S.O mínimo
Disable untrusted certificates rule.	Ésta regla protege a los usuarios de certificados de confianza no verificados.	iOS 5.0
Disable untrusted certificates	Con ésta regla muestra un mensaje al usuario, cuando el dispositivo deshabilita un certificado que no puede ser verificado.	iOS 5.0

after prompt rule.		

TABLA VI. VIII Políticas de certificados dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.4. Grupo de políticas de servicios en la nube

Las reglas de este grupo de políticas especifican las restricciones para el uso de servicios en la nube en el dispositivo. Las normas se aplican sólo a los dispositivos iOS.

Política	Descripción	S.O mínimo
Disable cloud services rule.	La selección de esta regla impide el uso de todos los servicios de iCloud, incluyendo copia de seguridad, documentación y servicios de imagen.	iOS 5.0
Disable cloud backup service rule.	La selección de esta regla impide a los usuarios realizar copias de seguridad de sus datos del dispositivo a iCloud.	iOS 5.0
Disable cloud document services rule.	La selección de esta regla impide que los usuarios almacenen documentos en iCloud.	iOS 5.0
Disable cloud picture services rule.	La selección de esta regla impide que los usuarios utilicen Galería de fotos. El envío de esta regla a un dispositivo elimina Galería de fotos del dispositivo y evita que las fotos capturadas con la cámara sean enviadas a la Galería de fotos.	iOS 5.0

Dsable cloud picture sharing services rule.	La selección de esta regla impide que los usuarios compartan fotos en la nube. Para esto se necesita un UDS 6.1 MR2 o superior.	iOS 6.0

TABLA VI. IX Políticas de servicios en la nube dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.5. Grupo de políticas de conectividad.

Las reglas de este grupo de políticas especifican restricciones para la conectividad de red. Las normas se aplican sólo a los dispositivos iOS.

Política	Descripción	S.O mínimo
Disable network connectivity rule.	Esta regla no permite a los usuarios conectar el dispositivo a redes WI-FI o Wireless	iOS 4.0
Disable wireless connectivity rule.	Esta regla no permite a los usuarios conectar el dispositivo a redes Wireless. Ésta regla no es válida si la regla para desactivar conectividad a la red está activada.	iOS 4.0
Disable roaming rule.	Con ésta regla el usuario no podrá conectar el dispositivo a una red Wireless si el roaming está activado.	iOS 4.0
Disable data service when roaming rule.	Con ésta regla el usuario no podrá conectar el dispositivo a ninguna red si el roaming está activado. Para iOS 4.x ésta regla desactiva los servicios de segundo	iOS 4.0

	plano del dispositivo.	
Disable background data service when roaming rule.	Con ésta regla los servicios de sincronización automática se desactivarán y se harán solamente cuando el usuario lo requiera.	iOS 4.0
Disable voice service when roaming rule.	Con ésta regla se evita que el usuario haga llamadas de voz a través de la red Wireless mientras roaming esté activado.	iOS 5.0

TABLA VI. X Políticas de conectividad dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.6. Grupo de políticas de contenido.

Las reglas de este grupo de políticas especifican restricciones para la descarga de contenidos. Esto incluye ocultar el contenido explícito y el establecimiento de la calificación máxima permitida para aplicaciones, películas y programas de televisión.

Política	Descripción	S.O mínimo
Disable content rule.	Ésta regla evita que los usuarios descarguen videos de iTunes Store y aplicaciones de la App Store.	iOS 4.0
Hide explicit content rule.	Ésta regla evita que los usuarios descarguen cualquier contenido clasificado como explícito de iTunes Store y aplicaciones de la App Store.	iOS 4.0
Maximum allowed rating	Esta norma establece la calificación máxima permitida de contenido para las	iOS 4.0

for applications rule.	aplicaciones que los usuarios pueden descargar en el dispositivo de la App Store. La calificación va del 0 al 100 y el valor por defecto es el máximo.	
Maximum allowed rating for movies rule..	Esta norma establece la calificación máxima permitida de contenido de videos que los usuarios pueden descargar en el dispositivo de la App Store. La calificación va del 0 al 100 y el valor por defecto es el máximo.	iOS 4.0
Maximum allowed rating for TV shows rule.	Esta norma establece la calificación máxima permitida de contenido de programas de tv que los usuarios pueden descargar en el dispositivo de la App Store. La calificación va del 0 al 100 y el valor por defecto es el máximo.	iOS 4.0
Region that defines the rating restrictions rule.	Esta regla modifica la región o el país, para saber que calificación usan del contenido. Esta regla no es tan necesaria.	iOS 4.0

TABLA VI. XI Políticas de contenido dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.7. Grupo de políticas de diagnóstico y uso.

Las reglas en este grupo de políticas especifican restricciones, para enviar información sobre el diagnóstico del dispositivo hacia la empresa manufacturera. Éstas sólo funcionan para dispositivos iOS.

Política	Descripción	S.O mínimo
Disable submission of device diagnostic logs to device vendor rule.	Con ésta regla se evita enviar información de diagnóstico a APPLE.	iOS 5.0

TABLA VI. XII Políticas de diagnóstico y uso de dispositivos IOS

6.4.1.2.8. Grupo de políticas de encriptación

Las reglas de este grupo de políticas especifican los requisitos de cifrado para el espacio de almacenamiento del dispositivo. Las reglas sólo se aplican a los dispositivos Android.

Política	Descripción	S.O mínimo
Apply encryption rules rule.	Seleccionando ésta regla se encripta parte de la memoria interna del dispositivo.	Android OS 3.0
Encrypt internal device storage rule.	Al seleccionar esta regla cifra el almacenamiento de los datos del dispositivo.	Android OS 3.0

TABLA VI. XIII Políticas de encriptación dispositivos Android

Fuente: Elaboración propia

6.4.1.2.9. Grupo de políticas de mensajería.

Política	Descripción	S.O mínimo
Hide the default messaging application rule.	Con ésta regla no se permite usar a los usuarios iMessage.	iOS 5.0

TABLA VI. XIV Políticas de mensajería dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.10. Grupo de políticas de la tienda en línea.

Las reglas de este grupo de políticas especifican restricciones para las tiendas en línea disponibles en los dispositivos.

Política	Descripción	S.O mínimo
Disable online stores rule.	La selección de esta regla impide que los usuarios utilicen todos los almacenes de contenido en línea. Los usuarios no pueden hacer compras en la aplicación o utilizar la App Store y iTunes Store en el dispositivo.	iOS 4.0
Disable purchases in applications rule.	La selección de esta regla impide que los usuarios realicen compras en la aplicación.	iOS 4.0
Disable storage of online store password rule.	La selección de esta regla impide que la tienda en línea guarde la contraseña del usuario. Los usuarios deben introducir su contraseña para todas las compras de contenido.	iOS 5.0
Hide the default application store rule.	La selección de esta regla deshabilita la App Store y remueve su ícono de la pantalla de inicio del dispositivo.	iOS 4.0
Hide the default book store rule.	La selección de esta regla deshabilita la iBook Store y remueve su ícono de la pantalla de inicio del dispositivo.	iOS 6.0
Disable purchases from the default book store	La selección de esta regla no permite que los usuarios descarguen contenido clasificado como erótico desde el iBook Store.	iOS 6.0

Hide the default music store rule.	La selección de esta regla deshabilita la iTunes Store y remueve su ícono de la pantalla de inicio del dispositivo.	iOS 4.0

TABLA VI. XV Políticas de tienda en linea dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.11. Grupo de políticas de la aplicación Passbook.

La regla en este grupo de políticas especifica restricciones para Passbook. La regla sólo se aplica a los dispositivos iOS.

Política	Descripción	S.O mínimo
Disable Passbook notifications when device is locked rule.	La selección de esta regla impide que el dispositivo muestre las notificaciones de Passbook cuando el dispositivo está bloqueado.	iOS 6.0

TABLA VI. XVI Políticas de Passbook dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.12. Grupo de políticas de password.

Las reglas de este grupo de políticas especifican los requisitos de contraseña y las reglas para la creación de contraseñas. La mayoría de las normas se aplican tanto a los dispositivos iOS y Android.

Para algunos modelos de dispositivos Android y todos los dispositivos que ejecutan el sistema operativo Android 3.xx, si un usuario no tiene un contraseña previamente modificada, el usuario no puede establecer una contraseña.

Política	Descripción	S.O mínimo
Define password properties rule.	La selección de esta norma permite establecer parámetros que los usuarios deben seguir a la hora de configurar la contraseña del dispositivo.	iOS 4.0 Android OS 2.3
Avoid repetition and simple patterns rule.	La selección de esta regla impide que los usuarios utilicen caracteres secuenciales o repetidos en la contraseña del dispositivo. Esta es válida sólo si la primera regla está definida.	iOS 4.0
Require alphanumeric value rule.	Al seleccionar esta norma exige a los usuarios crear una contraseña para el dispositivo que contiene al menos una letra y un número.	iOS 4.0
Require letters rule.	Al seleccionar esta norma exige a los usuarios crear una contraseña para el dispositivo que contenga letras. Si selecciona esta regla y luego especificar el número mínimo de letras, el usuario debe crear una contraseña que incluya, al menos, el número de letras que usted especifique. Los valores puedes ser cualquiera mayor a 0. El valor por defecto es 1.	Android OS 2.3
Require lowercase letters rule.	Esta regla especifica el número mínimo de letras minúsculas necesarias para la contraseña del dispositivo. Si selecciona esta regla y luego se especifica el número mínimo de letras minúsculas, el usuario debe crear una contraseña que incluya, al menos, el número de letras minúsculas que especificó.	Android OS 3.0

	Los valores puedes ser cualquiera mayor a 0. El valor por defecto es 1.	
Require numbers rule.	Al seleccionar esta norma exige a los usuarios crear una contraseña para el dispositivo que contenga números. Si selecciona esta regla y luego especifica el número mínimo de números, el usuario debe crear una contraseña que incluya al menos la cantidad de números que especificó. Los valores puedes ser cualquiera mayor a 0. El valor por defecto es 1.	Android OS 2.3
Require special characters rule.	Esta regla especifica el número mínimo de caracteres especiales que se requieren en la contraseña del dispositivo. Si selecciona esta regla y luego especificar el número mínimo de caracteres especiales, el usuario debe crear una contraseña que incluye por lo menos el número de caracteres especiales que se especificó. Los valores puedes ser cualquiera mayor a 0. El valor por defecto es 1.	iOS 4.0 Android OS 3.0
Require uppercase letters rule.	Esta regla especifica el número mínimo de letras mayúsculas necesarias para la contraseña del dispositivo. Si selecciona esta regla y luego se especifica el número mínimo de letras mayúsculas, el usuario debe crear una contraseña que incluya, al menos, el número de letras mayúsculas que especificó.	Android OS 3.0

	Los valores puedes ser cualquiera mayor a 0. El valor por defecto es 1.	
Delete data and applications from the device after incorrect password attempts rule.	Al seleccionar esta regla especifica el número de veces que un usuario puede intentar una contraseña incorrecta antes de que el dispositivo elimine todos los datos de información del usuario y la aplicación. Para los dispositivos de Android, el dispositivo no reconoce un ingreso de menos de cuatro caracteres como contraseña. Si el usuario introduce una contraseña incorrecta de menos de cuatro caracteres, no se contará como un intento. Para iOS el valor puede ser en el rango de 4 y 10. Para Android el valor puede cualquiera mayor a 0. Valor por defecto es 1.	iOS 4.0 Android OS 2.3
Device password rule.	Al seleccionar esta regla requiere que los usuarios introduzcan la contraseña en el dispositivo después de un período de inactividad.	iOS 4.0 Android OS 2.3
Enable auto-lock rule.	Seleccione esta regla para especificar el período de inactividad tras el cual se bloquea el dispositivo. Se puede especificar cualquier número de días, horas, minutos o segundos. Los valores pueden ser cualquiera mayores a 0. Por defecto son 15 minutos.	iOS 4.0 Android OS 2.3
Time after a device locks that it can be unlocked	Seleccione esta regla para especificar el período de tiempo después de bloquear el dispositivo que el usuario puede desbloquear el dispositivo sin	iOS 4.0

without a password rule.	necesidad de contraseña. Se puede especificar cualquier número de días, horas, minutos o segundos. Los valores pueden ser cualquiera mayores a 0. Por defecto es el 1.	
Limit password age rule.	Al seleccionar esta regla le permite especificar el período de tiempo después que se establece una contraseña hasta que expire la contraseña en el dispositivo y el usuario debe configurar una nueva contraseña. Se puede especificar cualquier número de días, horas, minutos o segundos. Los valores pueden ser cualquiera mayores a 0. Por defecto son 90 días.	iOS 4.0 Android OS 3.0
Limit password history rule.	Al seleccionar esta regla le permite especificar el número de contraseñas anteriores que el dispositivo comprueba para evitar que un usuario vuelva a utilizar contraseñas. Los valores pueden ser cualquiera mayores a 0. Por defecto es 1.	iOS 4.0 Android OS 3.0
Restrict password length rule.	Al seleccionar esta norma restringe la longitud de la contraseña en el dispositivo.	iOS 4.0 Android OS 2.3
Minimum length for the device password that is allowed rule.	Al seleccionar esta regla le permite especificar los caracteres mínimos numéricos necesarios para la contraseña del dispositivo. Los valores pueden ser cualquiera mayores o iguales a 4.	iOS 4.0 Android OS 2.3

	Por defecto es 4.	

TABLA VI. XVII Políticas de Password dispositivos IOS y Android

Fuente: Elaboración propia

6.4.1.2.13. Grupo de políticas de teléfono y mensajería

Las reglas de este grupo de políticas especifican los restricciones para la aplicación de teléfono por defecto, se aplican en dispositivos iOS.

Política	Descripción	S.O mínimo
Disable voice dialing rule.	La selección de esta regla impide que el usuario realice llamadas usando Siri, los equipos soportados también deben ser desde el iphone 4s en adelante.	iOS 4.0

TABLA VI. XVIII Políticas de Teléfono y mensajería dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.14. Grupo de políticas de perfiles y certificados.

La reglas de este grupo de políticas no permite que se instalen perfiles y certificados en el dispositivo, se aplican en dispositivos iOS.

Política	Descripción	S.O mínimo
Disable interactive installation of profiles and certificates rule.	La selección de esta regla impide que el usuario instale perfiles y certificados en el dispositivo.	iOS 6.0

TABLA VI. XIX Políticas de perfiles y certificados dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.15. Grupo de políticas social.

Las reglas de este grupo de políticas especifica restricciones para aplicaciones sociales, éstas reglas aplican solo para iOS.

Política	Descripción	S.O mínimo
Hide the Game Center and YouTube apps rule.	Seleccionando ésta regla, de la aplicación del game center y la aplicación de youtube.	iOS 4.0
Hide the Game Center app (Supervised only) and disable game functionality rule.	Seleccionando ésta regla, deshabilita de la aplicación del game center.	iOS 4.0
Disable adding Game Center friends rule.	Seleccionando ésta regla, evita que el usuario agregue amigos a la aplicación del game center.	iOS 4.0
Disable multiplayer gaming rule.	Seleccionando ésta regla, evita que el usuario juegue a modo multijugador en la aplicación del game center.	iOS 4.0
Hide the Game Center app (Supervised only) rule.	Seleccionando ésta regla, deshabilita de la aplicación del game center, el ícono incluso es removido de la interfaz.	iOS 6.0
Hide the YouTube app rule.	Seleccionando ésta regla, deshabilita de la aplicación de youtube, el ícono incluso es removido de la interfaz.	iOS 4.0

TABLA VI. XX Políticas sociales dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.16. Grupo de políticas de almacenamiento y respaldos.

Las reglas de este grupo de políticas específica restricciones sobre el respaldar información en el dispositivo, se aplican en dispositivos iOS.

Política	Descripción	S.O mínimo
Require that the device backup data is encrypted rule.	Al seleccionar esta regla almacena todos los datos de copia de seguridad en un formato cifrado en el ordenador del usuario.	iOS 4.0

TABLA VI. XXI Políticas de almacenamiento y respaldo dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.17. Grupo de políticas de asistente de voz.

Éste grupo de reglas especifican restricciones sobre usar comandos de voz en el dispositivo, las reglas aplican a dispositivos iOS.

Política	Descripción	S.O mínimo
Disable the default voice assistant application rule.	Con ésta regla el usuario no puede usar Siri, comandos de voz o dictado en el dispositivo.	iOS 5.0
Disable voice assistant application when device is locked rule.	Con ésta regla se evita que el usuario use comandos Siri cuando el dispositivo esté bloqueado, y también evita habilitar el teléfono con comandos Siri, esto aplica solamente si el usuario tiene habilitado un password de desbloqueo.	iOS 5.0

TABLA VI. XXII Políticas de asistencia de voz dispositivos IOS

Fuente: Elaboración propia

6.4.1.2.18. Reglas de políticas para el espacio de trabajo

Las reglas del espacio de trabajo se aplican sólo a la zona de trabajo en el dispositivo.

Regla	Descripcion	S.O Minimo
Allow sequence and single character passwords rule	La selección de esta norma permite al usuario establecer una contraseña trabajo que utiliza un solo carácter, como 1111, o una secuencia de caracteres, como abcd.	iOS 5.0 and later Android OS 2.3 Android OS 4.0
Require letters rule	Esta regla especifica el número mínimo de letras necesarias en la contraseña del espacio de trabajo.	iOS 5.0 Android OS 2.3 Android OS 4.0
Require lowercase letters rule	Esta regla especifica el número mínimo de letras minúsculas necesarias en la contraseña del espacio de trabajo.	iOS 5.0 Android OS 2.3 Android OS 4.0
Require numbers rule	Esta regla especifica el número mínimo de números necesarios en la contraseña del espacio de trabajo.	iOS 5.0 Android OS 2.3 Android OS 4.0
Require special characters rule	Esta regla especifica el número mínimo de caracteres especiales que se requieren en la contraseña del espacio de trabajo.	iOS 5.0 Android OS 2.3 Android OS 4.0
Require uppercase letters	Esta regla especifica el número mínimo de letras mayusculas que se requieren en	iOS 5.0

rule	la contraseña del espacio de trabajo.	Android OS 2.3 Android OS 4.0
Restrict password length rule	Al seleccionar esta norma restringe la longitud de la contraseña del espacio de trabajo	iOS 5.0 Android OS 2.3 Android OS 4.0
Minimum and Maximun length for the work space password rule	Esta regla le permite especificar el número mínimo y máximo de caracteres necesarios en la contraseña del espacio de trabajo	iOS 5.0 Android OS 2.3 Android OS 4.0
Lock work space after inactivity rule	Ésta regla, especifica el período de inactividad después del cual se bloquea el espacio de trabajo. Se puede especificar cualquier número de días, horas, minutos o segundos.	iOS 5.0 Android OS 2.3 Android OS 4.0
Track incorrect password attempts rule	Al seleccionar esta regla se especifica el número de veces que un usuario puede intentar una contraseña incorrecta antes de la acción especificada	iOS 5.0 Android OS 2.3 Android OS 4.0
Action after maximum incorrect password attempts rule	Esta regla especifica qué sucede cuando el usuario introduce una contraseña incorrecta más del número de veces especificado en la regla. Si selecciona la opción Deshabilitar el espacio de trabajo, el espacio de trabajo se desactiva y sólo puede ser restaurado por un administrador. Si selecciona Desactivar y eliminar la opción de datos, el espacio de trabajo se	iOS 5.0 Android OS 2.3 Android OS 4.0

	desactiva y se borra todos los datos. Si selecciona Desactivar y después de N días elimina la opción de datos, también debe especificar un número de días. El espacio de trabajo se desactiva de inmediato y sólo puede ser restaurado por un administrador. Si el espacio de trabajo no se restaura antes del tiempo señalado, se borran todos los datos del espacio de trabajo.	
Delete Work Connect data after period of inactivity rule	Esta regla sirve para especificar el número de días en inactividad, después de lo cual los datos de trabajo, incluyendo mensajes de correo electrónico de trabajo y los datos del organizador, se eliminan.	iOS 5.0 Android OS 2.3 Android OS 4.0
Allow apps in the personal space to access files in the work space rule	Esta regla sirve para permitir aplicaciones en el espacio personal para acceder a los archivos en el espacio de trabajo.	iOS 5.0 Android OS 2.3 Android OS 4.0
Notification level rule	Esta regla especifica el nivel de notificaciones que ve el usuario para en el espacio de trabajo cuando este está bloqueado. Mute, el usuario no ve las notificaciones. Mostrar Nombre de la aplicación, el usuario sólo ve el nombre de la aplicación que cuenta con una notificación, por ejemplo, el calendario de espacio de trabajo. Mostrar título, el usuario ve el título de la notificación, por ejemplo, el título de la reunión en el calendario.	iOS 5.0 Android OS 2.3 Android OS 4.0

TABLA VI. XXIII Políticas de espacio de trabajo dispositivos IOS y Android

Fuente: Elaboración propia

6.5. Pruebas entornos de seguridad

A continuación se muestran pruebas que se realizaron a los tres dispositivos para demostrar como la administración multiplataforma de dispositivos a travez de la solución BES ayuda a mejorar la seguridad de la información en los entornos corporativos a través del manejo de políticas se seguridad de información, las cuales limitan el funcionamiento de los Smartphones de acuerdo a el rol que desempeña cada usuario en la empresa, logrando así que la información crítica de esta permanezca segura y confiable, evitando en su totalidad filtraciones y duplicados de los datos.

Prueba en dispositivo BlackBerry Q10 y Z10

Entre las varias pruebas realizadas con los dispositivos BlackBerry todas fueron satisfactorias en cuanto a seguridad de la información entre las principales realizadas se tiene:

6.5.1. Prueba en dispositivo BlackBerry Q10 y Z10

Entre las varias pruebas realizadas con los dispositivos BlackBerry todas fueron satisfactorias en cuanto a seguridad de la información entre las principales realizadas tenemos:

- **Prueba de restricción y petición de password mínimo**

En el perfil de política de password explica los requisitos mínimos para establecer la contraseña para el dispositivo ya que al establecer prerrequisitos para la contraseña el usuario debe obligadamente cumplirlos sino el dispositivo no le deja hacer uso de su equipo.

En la figura VI.42 se muestra como el servidor no permite el cambio de clave ya que no cumple los requisitos especificados.

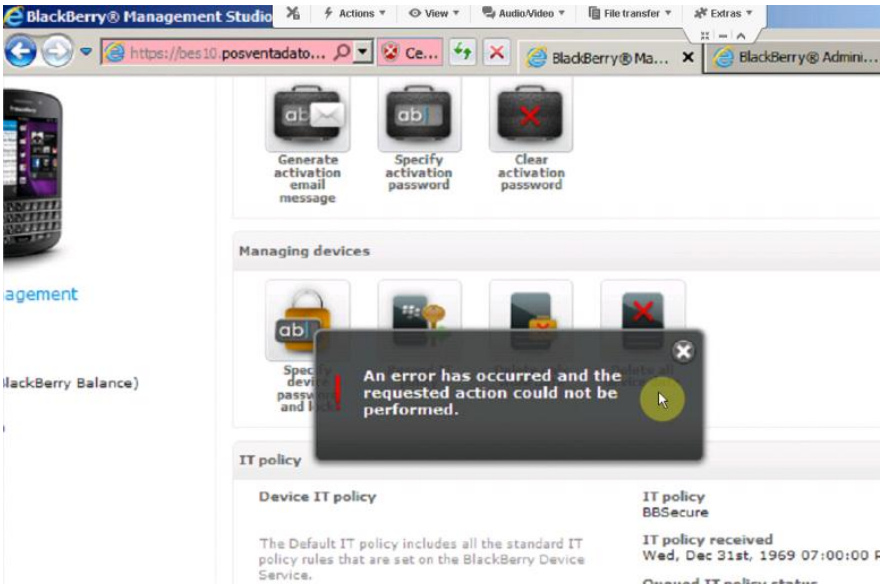


Figura VI. 44 Restricción del servidor por password

Fuente: Elaboración propia

La figura VI.45 y VI.46 muestra la restricción en el equipo

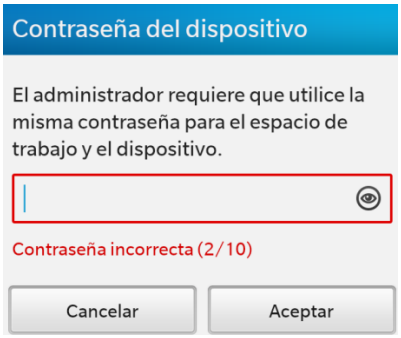


Figura VI. 45 Restricción del equipo

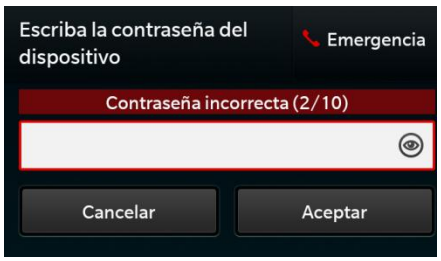


Figura VI. 46 Restricción del equipo (2)

Fuente: Elaboración propia

- **Prueba de bloque de bluetooth para transferencia de archivos desde el espacio de trabajo**

Otra política importante es el bloqueo de la transmisión de datos desde el entorno de trabajo al entorno corporativo, esta política bloquea los medios de envío y solo deja el correo de la empresa el cual es enviado solo a los usuarios que están registrados en la base de datos de la empresa.

La figura VI.47 muestra el espacio de trabajo antes de aplicar la regla de seguridad:

Figura VI. 47 Métodos de compartición de archivos en el workspace

Fuente: Elaboración propia

La figura VI.48 muestra el espacio de trabajo luego de aplicar la regla de seguridad:

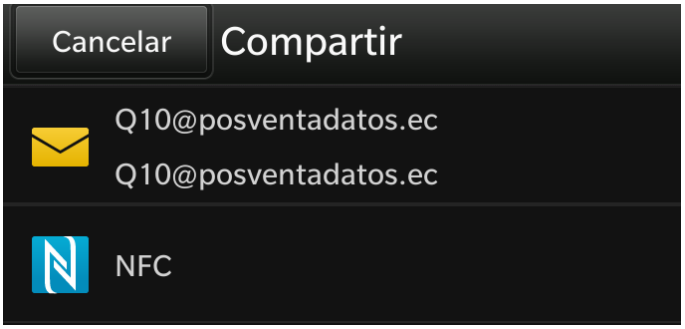


Figura VI. 48 Métodos de compartición de archivos en el workspace

- **Prueba de eliminación del espacio de trabajo para proteger el espacio de trabajo por pérdida o robo**

Esta opción es la de mayor utilidad y más que una política es una opción que da el servidor para proteger el entorno corporativo en caso de pérdida o robo, cabe destacar que aparte de esta opción existe la opción de borrar todo el dispositivo y bloquearle lo cual inhabilita el dispositivo, esta opción no se la realizo por ser un ambiente de prueba.

La figura VI.49 indica el entorno de trabajo normal de un usuario:

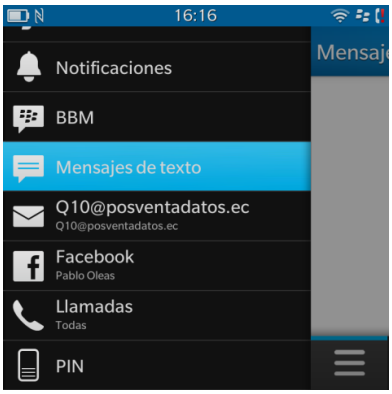


Figura VI. 49 Cuentas del entorno de trabajo

La figura VI.50 indica el equipo ya borrado el entorno de trabajo:

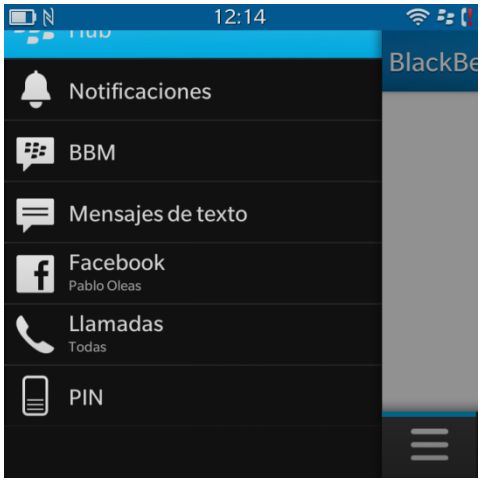


Figura VI. 50 Cuentas al borrar el entorno de trabajo

Estas son pocas de las prueba, entre las más importantes realizadas en el entorno de trabajo en el dispositivo BlackBerry, existen muchas pruebas las cuales son muy extensas y sirven para el mismo fin asegurar el entorno de trabajo de la empresa.

6.5.2. Prueba en dispositivo Samsung Galaxy S3 mini

Este dispositivo presentó complicaciones con el servidor ya que no aceptó todos los cambios en las políticas de seguridad; las pruebas que aceptó el dispositivo Android son pocas, pero estas de igual manera aseguran el entorno de trabajo ya que controlan las principales funciones que son:

- Restricción de Password
- Bloqueo del dispositivo

- Cambio de password
- Borrado del entorno y del equipo

- **Restricción y cambio de password**

En el dispositivo la regla de restricción de password solo toma efecto cuando se envía una petición de cambio de password, esto permite que el administrador controle todos los detalles que deben ser tomados en cuenta en el momento de poner un password.

La figura VI.51 muestra la consola de administración para realizar los cambios desde el servidor UDS

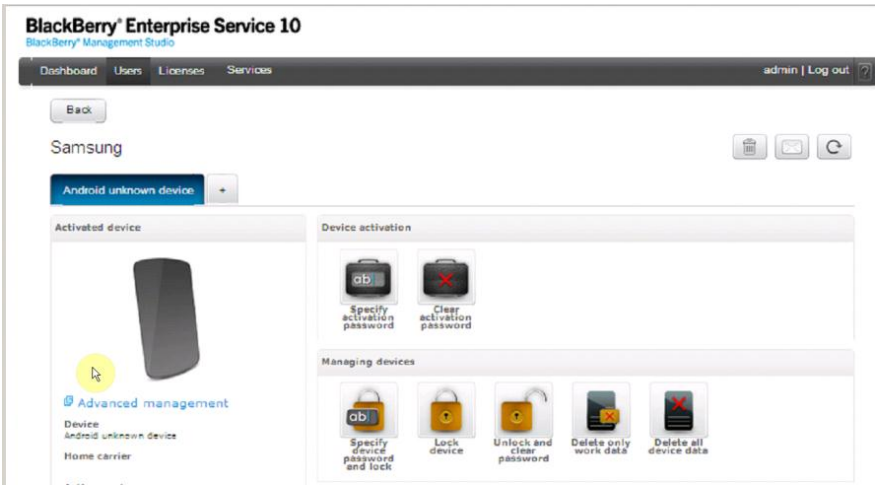


Figura VI. 51 Envió de desbloqueo y borrado de password

Fuente: Elaboración propia

La figura VI.52 muestra el dispositivo luego de enviar este comando:

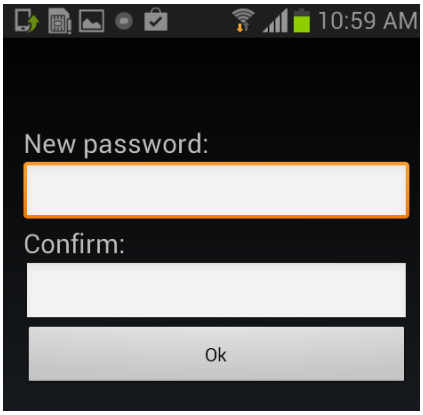


Figura VI. 52 Dispositivo luego de la petición

Fuente: Elaboración propia

- **Bloqueo del dispositivo**

Este comando bloquea el dispositivo, para volverlo a usar pide una contraseña antes ya designada

La figura VI.53 indica el entorno de trabajo0 de Samsung bloqueado:

Figura VI. 53 Entorno de trabajo Android bloqueado

Fuente: Elaboración propia

- **Borrado del entorno y del equipo**

Esta opción permite al administrador borrar el entorno de trabajo y del equipo inutilizándolo en este caso se probó el borrado del espacio de trabajo, para lo cual el equipo avisa que ya comienza a desinstalar todos los componentes.

La figura VI.54 muestra el aviso de desinstalación, la figura VI.55 indica el entorno desinstalado y la figura VI.56 muestra la aplicación BES 10 client reiniciada:

Figura VI. 54 Borrado del entorno de trabajo Android

Fuente: Elaboración propia

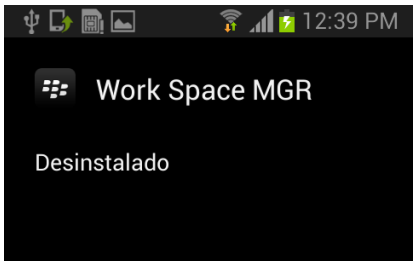


Figura VI. 55 Workspace Android eliminado

Fuente: Elaboración propia

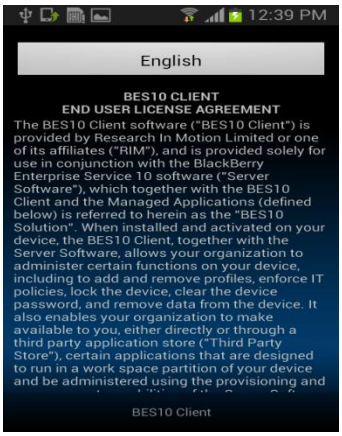


Figura VI. 56 BES 10 client reiniciado

Fuente: Elaboración propia

Una aclaración muy importante es que estas funciones actúan de manera igual en dispositivos IOS por lo cual esta parte sirve para las dos plataformas.

6.5.3. Prueba en dispositivo IPhone 4

Esta es el gran avance que muestra BES 10 ya que tiene una excelente comunicación con los dispositivos IOS y la mayoría de las políticas son aplicables y exitosas, bajo esta plataforma el servidor funciona perfectamente en este dispositivo debido a su amplia gama de posibilidades de seguridad se exploró algunas como:

Grupo de políticas del explorador

- **Hide the default web browser rule**
  - En la siguiente figura VI.57 se observó que el navegador por defecto (safari) está presente.

Figura VI. 57 Navegador por defecto

Fuente: Elaboración propia

- En la siguiente figura VI.58 Se observa que cuando se aplicó la política el navegador se deshabilita completamente.

Figura VI. 58 Navegador safari se deshabilitó.

Fuente: Elaboración propia

- **Disable autofill in the default browser rule**
  - En la siguiente figura VI.59 se observa cómo se deshabilita el autocompletado al momento de introducir una dirección.

Figura VI. 59 Función auto completar deshabilitada

Fuente: Elaboración propia

- **Disable JavaScript in the default browser rule.**
  - En la siguiente figura VI.60 se observa cómo se deshabilita javascript en el navegador.

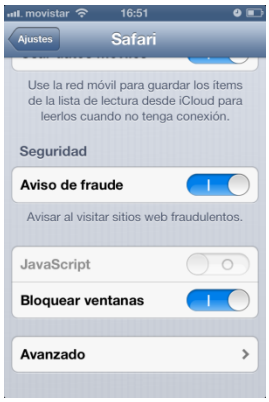


Figura VI. 60 Javascript deshabilitado

Fuente: Elaboración propia

Grupo de políticas de cámara y video

- **Hide the default camera application rule**
  - En la siguiente figura VI.61 se observa que la cámara estuvo presente antes de aplicar la política.

Figura VI. 61 La cámara está presente

Fuente: Elaboración propia

- En la siguiente figura VI.62 se observa que la cámara no estuvo presente.

Figura VI. 62 La cámara no está presente

Fuente: Elaboración propia

- **Hide the default video-conferencing application rule**
  - En la siguiente figura VI.63 se observa que la aplicación para video conferencia FACETIME está presente

Figura VI. 63 FACETIME está presente

Fuente: Elaboración propia

- En la siguiente figura VI.64 se observa que la aplicación para video conferencia FACETIME ha desaparecido aplicando la política.

Figura VI. 64 FACETIME se deshabilita

Fuente: Elaboración propia

Grupo de políticas de servicios en la nube

- **Disable cloud services rule**

- En las siguiente figuras VI.65, VI.66 se observa como el servicio icloud estuvo habilitado

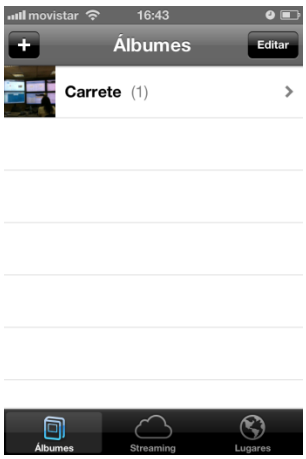


Figura VI. 65 iCloud

Figura VI. 66 iCloud (2)

Fuente: Elaboración propia

- En las siguiente figuras VI.67, VI.68 se observa como iCloud fue deshabilitado

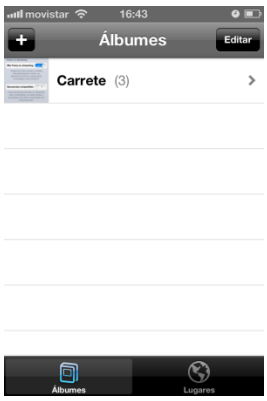


Figura VI. 67 iCloud deshabilitado

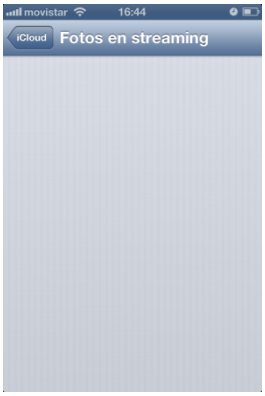


Figura VI. 68 iCloud deshabilitado (2)

Fuente: Elaboración propia

Grupo de políticas de contenido

- **Disable content rule**
  - En las figuras VI.69, VI.70, VI.71 Se observa que todo el contenido está disponible sin restricciones.

Figura VI. 69 Contenido

Figura VI. 70 Contenido (2)

Figura VI. 71 Aplicación

Fuente: Elaboración propia

- En las figuras VI.72, VI.73, VI.74 Se observa que aplicada la regla según los parámetros es el contenido mostrado y que ya no es posible descargarse una app de App Store.

Figura VI. 72 Contenido restringido

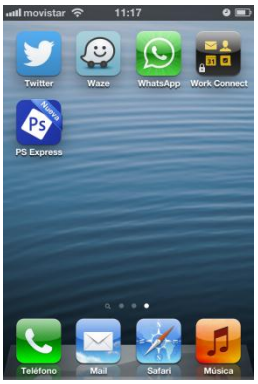


Figura VI. 73 Contenido restringido (2)

Figura VI. 74 Descarga deshabilitada

Fuente: Elaboración propia

Grupo de políticas de diagnóstico y uso

- **Disable submission of device diagnostic logs to device vendor rule**

  - En la siguiente figura VI.75 se observa que los informes de diagnóstico están habilitados.

Figura VI. 75 Diagnóstico y uso

Fuente: Elaboración propia

  - En la siguiente figura VI.76 se observa que los informes de diagnóstico se han deshabilitados.

Figura VI. 76 Diagnóstico y uso deshabilitado

Fuente: Elaboración propia

Grupo de políticas de tienda en línea

- **Disable online stores rule**

    - En las siguientes figuras VI.77, VI.78 se observa que las tiendas en línea App Store e iTunes están habilitadas.

Figura VI. 77 Tiendas online habilitadas

Figura VI. 78 Tiendas online deshabilitadas

Fuente: Elaboración propia

Grupo de políticas de contraseñas

- **Define password properties rule**

    - En las siguientes figuras VI.79, VI.80 se observa la interfaz de contraseña y que se puede restringir.

Figura VI. 79 Contraseña del equipo

Figura VI. 80 Interfaz código

Fuente: Elaboración propia

Grupo de políticas de almacenamiento y respaldos

- **Require that the device backup data is encrypted rule**

  - En las siguientes figuras VI.81, VI.82 Se muestra como aplicando la política y conectando el equipo a iTunes automáticamente se empieza hacer una copia de seguridad encriptada.

Figura VI. 81 Sincronización del equipo con iTunes

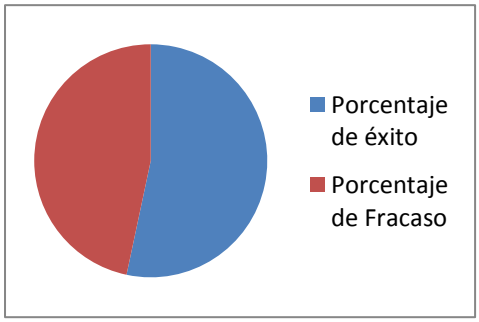
Figura VI. 82 Copia de seguridad

6.6. Análisis de resultados

Luego de simulados los entornos corporativos de trabajo en los cuales se realizaron las pruebas de seguridad se obtuvo que:

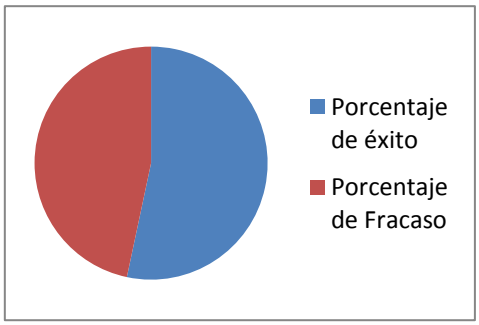
Al realizar las pruebas en Blackberry se obtuvo lo siguiente:

Políticas Disponibles	Políticas exitosas	Porcentaje de éxito	Porcentaje de Fracaso
211	211	100,00%	0,00%



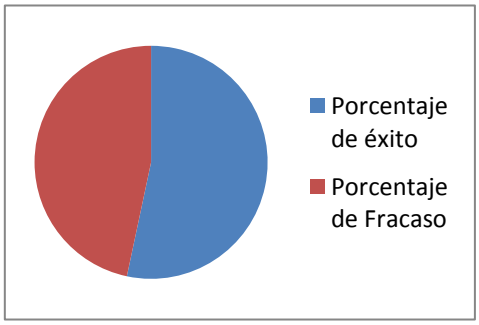
Al realizar las pruebas en iOS se obtuvo lo siguiente:

Políticas Disponibles	Políticas exitosas	Porcentaje de éxito	Porcentaje de Fracaso
84	59	70,24%	29,76%



Al realizar las pruebas en Android se obtuvo lo siguiente:

Políticas Disponibles	Políticas exitosas	Porcentaje de éxito	Porcentaje de Fracaso
30	16	53,33%	46,67%



Como se observa, en el dispositivo BlackBerry Z10 se obtuvo éxito al 100%, en el dispositivo iOS un 70,73%, y en el dispositivo ANDROID un 53,33%. Todo esto guiándonos en la misma documentación proporcionada por RIM.se acepta la hipótesis planteada ya que al administrar la solución BES mediante uso de políticas de seguridad nos brinda un entorno seguro para el manejo de la información en entornos corporativos.

CONCLUSIONES

- La solución BES 10.1, es capaz de administrar equipos con diferentes sistemas operativos los cuales son IOS, BlackBerry, y Android, brindando un entono seguro para el manejo de la información corporativa, mostrando porcentajes en blackberry del 100%, en iOS 70.73% y en Android un53.33%
- Para distinguir entre la información personal de la corporativa se utilizan las herramientas BlackBerry Balance y Secure Work Space, las cuales aseguran que la información personal y de trabajo se mantengan separadas y bien clasificadas en los dispositivos, manejando una infraestructura diferente para administrar cada plataforma.
- Al simular un espacio de comunicación móvil, la solución BES brinda seguridad en entornos de punta a punta de su arquitectura y sus políticas IT.
- Esta solución a pesar de su considerable costo, brinda muchas bondades a empresas que deseen implementar el servicio o a su vez empresas que deseen ofertar la misma, como la empresa telefónica.

RECOMENDACIONES

- Para realizar la instalación es necesario que el servidor tanto de correo como el del BES 10 estén en ingles ya que la solución no soporta otros idiomas.
- Para una correcta instalación y administración, se debe mantener un caso abierto con la empresa RIM, la cual es la dueña de la solución.
- Se deber tener muy en cuenta las versiones de los sistemas operativos de los equipos comprobando las matrices de compatibilidad.
- Se debe tener en cuenta todos los equipos externos a la solución en especial los firewalls, ya que se debe aplicar los permisos necesarios para que la solución se desarrolle con normalidad.
- La asistencia al usuario se la debe realizar a través de un código abierto con RIM por medio de una cuenta de e-mail.

RESUMEN

La investigación tuvo como finalidad evaluar los niveles de seguridad brindados por varios dispositivos multiplataforma Android, iOS, BlackBerry bajo una solución diseñada para entornos corporativos destinado al departamento Posventa-Datos empresa Telefónica-Quito.

Esta investigación se realizó mediante el método inductivo, comenzando por observación luego medición del número de políticas IT funcionando correctamente en cada plataforma divididas mediante grupos; seguridad respecto a password, seguridad de aplicaciones, aislamiento de entornos; luego ordenamos y analizamos las pruebas obteniendo las conclusiones requeridas.

Los materiales usados fueron: servidor Exchange para crear cuentas de correo, tres smartphones para pruebas directas y el servidor BlackBerry Enterprise Service como solución para lograr movilidad empresarial segura; evaluamos las políticas disponibles para cada plataforma, midiendo seguridad y confiabilidad brindada en entornos corporativos móviles punta a punta. Con los resultados analizamos el nivel de confianza presente por plataforma.

Como resultado obtuvimos: primer lugar a BlackBerry el cual ofrece seguridad al 100%, iOS segundo lugar logrando 73.73%, Con Android obtuvimos apenas 53.33%, basado en un numero de políticas fijo existente para cada sistema.

Se concluye que administrar dispositivos multiplataforma asegura toda información empresarial crítica en entornos móviles punta a punta, tanto aplicando políticas de seguridad como separando entornos de trabajo, sea personal o corporativo.

Se recomienda que empresas ofertantes de servicios móviles corporativos adopten esta solución segura debiendo elegir correctamente equipos soportados, además revisar todos los requerimientos previos para obtener beneficios óptimos en soluciones multiplataforma.

ABSTRACT

The research aimed to evaluate the levels of security provided by various Android, Ios and BlackBerry multi-plataform devices under one solution designed for corporate environments.

This research was performed by the inductive method, starting with observation after measuring the number of IT policies working correctly in each group divided by plataform; regarding passwordsecurity, application security, isolation security, then ordered the test and analyse the findings obtained required.

The materials used were: Exchange server to créate email accounts, three smartphones for direct evidence and the Blackberry Enterprise Server as a Service solution for archieving secure enterprise mobility evaluate policies available for each plataform, measuring security and reliability in mobile corporate environments provied tip to end. Whit the results we analize the confidence level for this plataform.

As a result we obtained: Firstly BlackBerry wich offers 100% security, secondly iOS achieves 73.73%, whit Android we got just 53.33%, base don a fixed number of existing policies for each system.

We conclude that manage multiplataform devices ensures all critical bussines information in mobile environment end to end, both applying security policies as separating work environments, whether personal or corporate.

It is recommended that vendors corporate mobile services companies adop this safe solution must correctly choose suported teams also review all prerequisites for optimum benefits un multi-plataform devices solutions.

ANEXOS

HOJA ESPECIFICACIONES SAMSUNG GALAXY S3 MINI

CARACTERISTICAS

El GALAXY SIII mini materializa el alto rendimiento, el uso intuitivo y el diseño inspirado en la naturaleza del GALAXY SIII en un smartphone elegante y compacto con una pantalla de 4,0 pulgadas. Puede ser una excelente opción para los clientes que están buscando smartphones más prácticos.

Diseño

El diseño del GALAXY SIII mini se parece al diseño minimalista y orgánico inspirado en la naturaleza del GALAXY SIII. Su naturaleza centrada en el ser humano ofrece una experiencia ergonómica y cómoda, con una mayor facilidad de uso. Su diseño se siente sencillamente natural, con su cómodo agarre y sus sutiles curvas.

Pantalla AMOLED de 4,0"

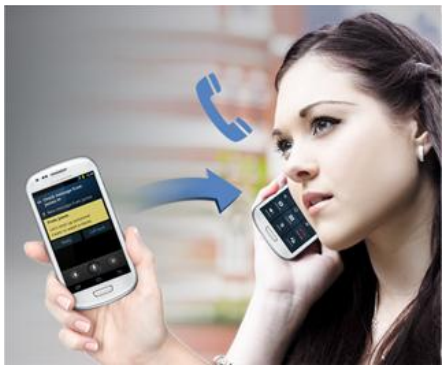
A esto lo llamamos ver la realidad. La hermosa pantalla Super AMOLED de 4,0 pulgadas ofrece una experiencia visual generosa, que te permite ver contenido Web y multimedia con nitidez y en colores brillantes.

Sistema operativo Jelly Bean

Cuenta con Android™ 4.1 (Jelly Bean), la versión más actual del sistema operativo para smartphones más popular del mundo. Jelly Bean posee gráficos rápidos, fluidos y homogéneos junto con una nueva experiencia de Google Search™, con Google Now™, que te ofrece la información correcta incluso antes de pedirla.

Ventanas de reproducción emergentes

Las ventanas de reproducción emergentes te permiten enviar mensajes de texto mientras ves un video. Es compacto, pero de todas maneras puedes hacer cosas al mismo tiempo. No te pierdas nada de lo que ocurre.

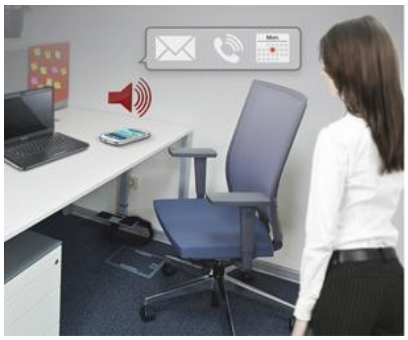


Llamada directa

El Samsung GALAXY SIII mini incluso sabe cuándo quieres hablar. Cuando le estás enviando un mensaje a alguien y decides que es mejor llamarlo, sencillamente lleva el teléfono al oído y Llamada directa marcará su número. Olvídate de desplazarte hacia arriba y abajo por los registros de llamadas o listas de contactos. Deja que el Samsung GALAXY SIII mini se encargue de eso.

S Voice

Con el software de reconocimiento de idioma avanzado de Samsung puedes usar la voz para desbloquear el teléfono con sencillos comandos personalizados, o puedes reproducir tus canciones favoritas, subir o bajar el volumen, organizar tu agenda o iniciar automáticamente la cámara y comenzar a tomar fotografías.



Smart Alert

Cuando tomas el teléfono, ¿no sería genial que te hiciera saber lo que ha ocurrido desde la última vez que lo usaste? El Samsung GALAXY SIII mini sabe que regresaste y te avisa con una breve vibración sobre las llamadas perdidas y los nuevos mensajes. ¿No te parece considerado de su parte?

HOJA ESPECIFICACIONES IPHONE 4

Color

Blanco

Negro

Capacidad

8 GB

Tamaño y peso

Alto: 115.2 mm (4.5 pulgadas)

Ancho: 58.6 mm (2.31 pulgadas)

Profundidad: 9.3 mm (0.37 pulgadas)

Peso: 140 gramos (4.9 onzas)

9.3 mm 0.37 pulgadas
115.2 mm 4.5 pulgadas
58.6 mm 2.31 pulgadas

Chip

Chip A5

Tecnología celular y wireless

Teléfono universal

UMTS/HSDPA/HSUPA (850, 900, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz); CDMA EV-DO Rev. A (800, 1900 MHz)[3]

Wi-Fi 802.11b/g/n (sólo 802.11n de 2.4 GHz)

Tecnología wireless Bluetooth 4.0

Lugar

GLONASS y GPS asistido

Brújula digital

Wi-Fi

Tecnología celular

Pantalla

Pantalla Retina

Pantalla widescreen Multi-Touch de 3.5 pulgadas (diagonal)

Resolución de 960 x 640 pixeles a 326 ppi

Relación de contraste 800:1 (normal)

Brillo máximo de 500 cd/m2 (normal)

Revestimiento oleofóbico resistente a marcas dactilares al frente y en la parte posterior

Soporte para mostrar varios idiomas y caracteres simultáneamente

Cámara iSight

8 megapixeles

Apertura ƒ/2.4

Flash LED

Sensor de iluminación posterior

Lente de cinco elementos

Filtro híbrido IR

Autoenfoque

Toque para enfocar

Detección de rostros

Función panorámica

Geoetiquetado de fotos

Grabación de videos

Grabación de video en HD de 1080p

30 cps

Luz LED

Estabilización de video

Toque para enfocar

Detección de rostros

Geoetiquetado de videos

Cámara FaceTime

Fotos con resolución VGA

Grabación de video con resolución VGA

[4] Videollamada

FaceTime

Desde iPhone 4s a cualquier dispositivo con FaceTime a través de Wi-Fi o red celular

Haz videollamadas por HSPA, 3G y 2G

Llamadas por Wi-Fi con resolución HVGA (480 por 320)

[4]Llamada de audio

FaceTime

Desde iPhone 4s a cualquier dispositivo con FaceTime a través de Wi-Fi o red celular

Reproducción de audio

Frecuencia de respuesta: 20 Hz a 20,000 Hz

Formatos de audio compatibles: AAC (8 a 320 Kbps), AAC protegida (del iTunes Store), HE-AAC, MP3 (8 a 320 Kbps), MP3 VBR, Audible (formatos 2, 3, 4, Audible Enhanced Audio, AAX y AAX+), Apple Lossless, AIFF y WAV

Límite de volumen máximo configurable por el usuario

TV y video

La función de duplicación AirPlay es compatible con el Apple TV a 720p

Transmisión de videos de AirPlay al Apple TV (tercera generación) de hasta 1080p y al Apple TV (segunda generación) de hasta 720p

Video en espejo y soporte de salida de video: hasta 1080p con Adaptador AV Digital de Apple o Adaptador VGA de Apple (los adaptadores se venden por separado)

Soporte para salida de video a 576p y 480p con el cable AV componente de Apple; 576i y 480i con el cable AV compuesto de Apple (los cables se venden por separado)

Formatos de video compatibles: video H.264 de hasta 1080p, 30 cuadros por segundo, Main Profile nivel 4.1 con audio AAC-LC de hasta 160 Kbps, 48 kHz, audio estéreo en formatos de archivo .m4v, .mp4 y .mov; video MPEG-4, de hasta 2.5 Mbps, 640 por 480 pixeles, 30 cuadros por segundo, Simple Profile con audio AAC-LC de hasta 160 Kbps por canal, 48 kHz, audio estéreo en formatos de archivo .m4v, .mp4 y .mov; Motion JPEG (M-JPEG) de hasta 35 Mbps, 1280 por 720 pixeles, 30 cuadros por segundo, audio en ulaw, audio estéreo PCM en formato de archivo .avi

Botones y conectores externos

Botones y controles externos

Encender/apagar
Reposo/despertar
Timbre/silencioso
Control de volumen
Inicio

Conectores y entradas/salidas

Puerto para conector dock

Micrófono

Bocina integrada

Minijack para audífonos
estéreo de 3.5 mm

[5]Energía y batería

Batería de litio-ion recargable integrada

Carga vía USB a una computadora o a un adaptador de corriente

Tiempo de conversación: hasta 8 horas con 3G

Tiempo en standby: hasta 200 horas

Uso de Internet: hasta 6 horas en 3G; hasta 9 horas en Wi-Fi

Reproducción de video: hasta 10 horas

Reproducción de audio: hasta 40 horas

Sensores

Giroscopio de tres ejes

Acelerómetro

Sensor de proximidad

Sensor de luz ambiental

Sistema operativo

iOS 7

Con un nuevo diseño y nuevas funcionalidades, iOS 7 es el sistema operativo móvil más avanzado del mundo en su versión más avanzada. Más información sobre iOS 7

iOS 7 incluye

AirDrop

AirPlay

AirPrint

Centro de control

Centro de notificaciones

Búsqueda Spotlight

Integración con Facebook

Integración con Twitter

iCloud

Llavero de iCloud

Multitarea

Passbook

Auriculares

Audífonos Apple con control remoto y micrófono
Frecuencia de respuesta: 20 Hz a 20,000 Hz

Tarjeta SIM

Connector

30 pin

Soporte para archivos adjuntos

Tipos de documentos visualizables

.jpg, .tiff, .gif (imágenes); .doc y .docx (Microsoft Word); .htm y .html (páginas web); .key (Keynote); .numbers (Numbers); .pages (Pages); .pdf (Vista Previa y Adobe Acrobat); .ppt y .pptx (Microsoft PowerPoint); .txt (texto); .rtf (formato de texto enriquecido); .vcf (datos de contactos); .xls y .xlsx (Microsoft Excel); .zip; .ics

Requerimientos del sistema

ID de Apple (requerido para algunas funcionalidades)

Acceso a Internet[7].

La sincronización con iTunes en una Mac o PC requiere:

Mac: OS X v10.6.8 o posterior

PC: Windows 8, Windows 7, Windows Vista o Windows XP Home o Professional con Service Pack 3 o posterior

iTunes 11.1 o posterior (descarga gratis en www.apple.com/la/itunes/download)

Requisitos ambientales

Temperatura operativa: 0 a 35 ºC (32 a 95 ºF)

Temperatura no operativa: –20 a 45 ºC (–4 a 113 ºF)

Humedad relativa: 5% a 95% sin condensación

Altitud máxima de funcionamiento: 3,000 m (10,000 pies)

Idiomas

Soporte para idiomas

Alemán, árabe, catalán, checo, chino (simplificado), chino (tradicional), coreano, croata, danés, eslovaco, español, finés, francés, griego, hebreo, holandés, húngaro, indonesio, inglés (Estados Unidos), inglés (Reino Unido), italiano, japonés, malayo, noruego, polaco, portugués, portugués (Brasil), rumano, ruso, sueco, tailandés, turco, ucraniano, vietnamita

Soporte de teclado

Alemán (Alemania), alemán (Suiza), árabe, búlgaro, catalán, checo, cherokee, chino simplificado (escrito, pinyin, pincelado), chino tradicional (escrito, pinyin, zhuyin, cangjie, wubihua, pincelado), coreano, croata, danés, emoji, eslovaco, español, estonio, finés, flamenco, francés (Canadá), francés (Francia), francés (Suiza), griego, hawaiano, hebreo, hindi, holandés, húngaro, indonesio, inglés (Australia), inglés (Canadá), inglés (Estados Unidos), inglés (Reino Unido), islandés, italiano, japonés (romaji, kana), letón, lituano, macedonio, malayo, noruego, polaco, portugués (Brasil),

portugués (Portugal), rumano, ruso, serbio (cirílico/latino), sueco, tailandés, tamil, tibetano, turco, ucraniano, vietnamita

Soporte de diccionario (permite el texto predictivo y la autocorrección)

Alemán, árabe, catalán, checo, cherokee, chino (simplificado), chino (tradicional), coreano, croata, danés, eslovaco, español, estonio, finés, flamenco, francés (Canadá), francés (Francia), francés (Suiza), griego, hawaiano, hebreo, hindi, holandés, húngaro, indonesio, inglés (Australia), inglés (Canadá), inglés (Estados Unidos), inglés (Reino Unido), italiano, japonés (romaji, kana), letón, lituano, malayo, noruego, polaco, portugués (Brasil), portugués (Portugal), rumano, ruso, sueco, tailandés, tamil, turco, ucraniano, vietnamita

Idiomas de Siri
Alemán (Alemania, Suiza), cantonés (Hong Kong), coreano, español (Estados Unidos, México, España), francés (Francia, Canadá, Suiza), inglés (Estados Unidos, Reino Unido, Canadá, Australia), italiano (Italia, Suiza), japonés, mandarín (China continental, Taiwán)

En la caja

iPhone 4s

Audífonos Apple con control remoto y micrófono

Cable de conector Dock a USB

Adaptador de corriente USB
Documentación

HOJA DE ESPECIFICACIONES BACKBERRY Z10

GENERAL	**Red**	GSM 850 / 900 / 1800 / 1900 - HSDPA 800 / 850 / 900 / 1900 / 2100 - LTE 800 / 900 / 1800 / 2600 o LTE 700 / 850 / 1700 / 1900
	Anunciado	2013, Enero
	Status	Pronto
TAMAÑO	**Dimensiones**	130 x 65.6 x 9 mm

	Peso	135 g
DISPLAY	**Tipo**	LCD touchscreen capacitivo, 16M colores
	Tamaño	768 x 1280 pixels, 4.2 pulgadas
		- Soporte multitouch - Sensor acelerómetro para auto rotación - Sensor de proximidad para auto apagado - Sensor giroscópico
RINGTONES	**Tipo**	Polifónico, MP3, WAV
	Customización	Descargas
	Vibración	Si
		- Conector de audio 3.5 mm
MEMORIA	**Agenda telefónica**	Entradas y campos prácticamente ilimitados, Foto de llamada
	Registro de llamadas	Prácticamente ilimitado
	Slot de tarjeta	microSD hasta 32GB
		- 16GB memoria interna, 2GB RAM - Procesador Qualcomm MSM8960 Snapdragon dual-core 1.5 GHz, GPU Adreno 225
CARACTERÍSTICAS	**GPRS**	Si
	Velocidad de datos	
	OS	BlackBerry 10 OS
	Mensajería	SMS, MMS, Email, IM, BBM
	Navegador	HTML5
	Reloj	Si
	Alarma	Si
	Puerto infrarrojo	No
	Juegos	Si
	Colores	Blanco, Negro
	Cámara	8 MP, 3264x2448 pixels, autofocus, flash LED, geo-tagging, detección de rostro y sonrisa, foco táctil, estabilizador de imagen, video 1080p@30fps, cámara frontal 2MP 720p@30fps

		- GPS con soporte A-GPS - Brújula digital - EDGE - 3G HSDPA 21Mbps / HSUPA 5.76Mbps - 4G LTE - Wi-Fi 802.11 a/b/g/n; banda dual - Bluetooth v4.0 A2DP - microUSB 2.0 - Integración con redes sociales - NFC - Puerto HDMI - Mapas BlackBerry - Reproductor de video DivX/XviD/MP4/WMV/H.263/H.264 - Reproductor de audio MP3/WAV/eAAC+/AC3/FLAC - Organizador - Editor de imagen/video - Editor de documentos (Word, Excel, PowerPoint, PDF) - Memo/comandos/discado de voz - Manoslibres incorporado - Java MIDP 2.1 - Ingreso predictivo de texto
BATERÍA		Standard, Li-Ion 1800 mAh
	Stand-by	Hasta 305 h (3G) / Hasta 316 h (2G)
	Tiempo de conversación	Hasta 10 h

BIBLIOGRAFÍA

[19]. SAMANIEGO,D., Comunicaciones celulares GSM., Escuela Superior Politécnica de Chimborazo., Riobamba-Ecuador., FIEE IETR., 2013., Pp6

[10]. FLORES N.J., SISTEMAS DE COMUNICACIÓN INALÁMBRICA DE MÚLTIPLES ENTRADAS Y MÚLTIPLES SALIDAS (MIMO)., Escuela Politécnica Nacional., Ingeniería Electrónica y Telecomunicaciones., Escuela de Ingeniería., Quito-Ecuador., TESIS., 2005., Pp29.

E-Book http://bibdigital.epn.edu.ec/bitstream/15000/5080/1/T2455.pdf

[1]. More Smartphones Were Shipped in Q1 2013 Than Feature Phones, An Industry First According to ID

http://www.idc.com/getdoc.jsp?containerId=prUS24085413

12-07-2013

[2]. El mercado IT de América Latina tendrá el mayor crecimiento a nivel mundial durante 2013

http://www.latamtechnews.com/el-mercado-it-de-america-latina-tendra-el-crecimiento-mas-rapido-a-nivel-mundial-durante-2013.html

13-07-2013

[3]. Smartphones a pasos inteligentes

http://www.vistazo.com/impresa/vidamoderna/imprimir.php?Vistazo.com&id=3760

13-07-2013

[4]. El Blackberry BBM viene para Android y iPhone este año

http://www.eliax.com/index.cfm?post_id=10385

15-07-2013

[5]. Android vs Blackberry: El 40% del tráfico web empresarial móvil a nivel mundial viene de Android

http://www.androidpit.es/Android-vs-Blackberry-El-40-del-trafico-web-empresarial-movil-a-nivel-mundial-

17-07-2013

[6]. Evolución de la telefonía celular.

http://masterandrade.wikispaces.com/EVOLUCION+DE+LA+TELEFONIA+CELULAR

07-10-2013

[7]. StarTAC: a 15 años del celular que revolucionó la telefonía móvil.

http://www.conexionbrando.com/1342831

07-10-2013

[8]. La evolución del celular.

http://unmundomovil.blogspot.com/2010/08/la-evolucion-del-celular-con-imagenes.html

07-10-2013

[9]. Telefonía celular cómo funcionan las comunicaciones con los teléfonos celulares.

http://isczacatepec.webege.com/telecom/1)%20Telefon%C3%ADa%20Celular.pdf

08-10-2013

[11]. Sistema AMPS

http://www.spw.cl/05mar07_mobile/Material_moviles/amps.pdf

09-10-2013

[12]. AMPS DAMPS

https://www.ucursos.cl/ingenieria/2004/2/EL65G/1/material_docente/bajar?id_material=52717

09-10-2013

[13]. Las generaciones de la telefonía inalámbrica

http://telefoniaunicolmayor.galeon.com/aficiones2336545.html

10-10-2013

[14]. Tecnologías GSM, CDMA, TDMA, GPRS, EDGE, UMTS

http://www.monografias.com/trabajos75/tecnologias-gsm-cdma-tdma-gprs/tecnologias-gsm-cdma-tdma-gprs.shtml

10-10-2013

[15]. HSCSD

http://www.gsmspain.com/info_tecnica/hscsd/

11-10-2013

[16]. Telefonía móvil 3g

http://www.ecured.cu/index.php/Telefon%C3%ADa_m%C3%B3vil_3G

11-10-2013

[17]. Comunicaciones móviles

http://profesores.usfq.edu.ec/renej/Contenidos%20Comunicaciones%20Moviles/Exposiciones%202008/Telefon%EDa%20m%F3vil%204G.pdf

13-10-2013

[18]. Tecnologías móviles

http://200.110.171.173/tecnologia/intranetp/tecnologiasmoviles.pdf

13-10-2013

[20]. Historia del sistema Android

http://android.cix.pe/lecciones/la-historia-de-android/

15-10-2013

[21]. Etimologia Android

http://www.unocero.com/2013/09/23/la-historia-de-android/

15-10-2013

[22]. Características de Android

http://www.configurarequipos.com/doc1107.html

15-10-2013

[23]. Logo de Android

http://blog.zerobytesystems.com/2012/09/porque-el-logo-de-android.html

15-10-2013

[24]. Ventajas y Desventajas de Android

http://scoello12.wordpress.com/ventajas-y-desventajas/

15-10-2013

[25]. Versiones de Android

http://www.androidcurso.com/index.php/tutoriales-android/31-unidad-1-vision-general-y-entorno-de-desarrollo/146-las-versiones-de-android-y-niveles-de-api

15-10-2013

[26]. Generalidades de IOS

http://luxstevejobs.comxa.com/obra1.html

17-10-2013

[27]. Versiones de IOS

http://www.applesfera.com/ios/la-evolucion-de-ios-desde-2007-hasta-la-actualidad-especial-historia-wwdc

17-10-2013

[28]. IOS OS7

http://www.infinittonews.com/index.php/tecnologia/internet/2459-apple-llega-el-nuevo-ios-7-como-un-nuevo-punto-de-partida

17-10-2013

[29]. Nueva versión IOS OS7

https://www.apple.com/es/ipad/ios/

17-10-2013

[30]. Inicio y Evolución de Blackberry

http://www.bberryblog.com/los-inicios-y-evolucion-de-blackberry/

21-07-2013

[31]. Historia de Blackberry

http://www.xatakamovil.com/blackberry/blackberry-un-poco-de-historia

21-07-2013

[32]. Evolución de Blackberry

http://www.bb-pr.net/la-historia-de-blackberry-el-comienzo-de-la-evolucion/

21-07-2013

[33]. Comparacion entre Blackberry los y Android

http://www.xatakandroid.com/mercado/las-10-caracteristicas-de-android-que-le-faltan-a-iphone

[34]. Movilidad empresarial

http://mundocontact.com/la-movilidad-empresarial-el-futuro-de-los-negocios/

21-07-2013

[35]. Visión Estratégica y entendiendo blackberry 10

http://www.blackberry.com

21-07-2013

[36]. Soluciones de Movilidad

http://www.sap.com/spain/solutions/mobility/index.epx

21-07-2013

[37]. Blackberry Device Service Advanced Administration guide

http://docs.blackberry.com

24-10-2013

[38]. BlackBerry Enterprise Service 10:BlackBerry Device Service SolutionVersion: 10.1

http://docs.blackberry.com

24-10-2013

[39]. BES10_v.10.1.3_Security_Note_SWS_EN

http://docs.blackberry.com

28-10-2013

[40]. BES10_v10.1.3_Licensing_Guide_en

http://docs.blackberry.com

31-1032013

[41]. BES10_v10.1.3_BDS_Advanced_Admin_Guide_en

http://docs.blackberry.com

04-11-2013

[42]. BES10_v10.1.3_BDS_Policy_and_Profile_Reference_Guide

http://docs.blackberry.com

05-11-2013

[43]. BlackBerry_Enterprise_Server_5.0.4_and_BlackBerry_7.1_Security_Technical_Overview_en

http://docs.blackberry.c…

06-11-2013

[44]. Pasos previos a la instalación de Microsoft Exchange Server 2010

http://www.microsoft.com/exchange/2010/es/es/system-requirements.aspx

06-11-2013

[45]. Compatibility Matrix Blackberry Enterprise Service 10and Mobile Device OS

http://docs.blackberry.com/en/admin/deliverables/55583/BES10_and_Mobile_Device_OS_Compatibility_Matrix_en.pdf

06-11-2013