ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UN MODELO PARA LA ADMINISTRACIÓN DE MOVILIDAD EMPRESARIAL, CONSIDERANDO SISTEMAS ANDROID, IOS Y WINDOWS PHONE"

INFORME DE MATERIA INTEGRADORA

Previa a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

RODRÍGUEZ BERNABÉ VERÓNICA MARÍA

QUIMÍ GONZÁLEZ JOSEPH EUGENIO

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTO

A Dios, que me concede salud, sabiduría, fortaleza en mi corazón para cumplir una de mis metas.

A mis padres que con su esfuerzo han ayudado a que tenga una formación profesional.

A la ESPOL, mi querida universidad por haberme permitido ser parte de ella, por brindarme sólidos conocimientos a través de los profesores y fomentar el crecimiento intelectual.

A mis tutores, Ing. Ronald Criollo, Ing. Robert Andrade Troya por su apoyo y motivación constante.

Joseph Quimí G.

AGRADECIMIENTO

Mi primordial agradecimiento es a Dios por la salud y las bendiciones recibidas constantemente.

A mi familia, especialmente a mi mamita la Sra. Dolores Bernabé por su amor, por creer en mis sueños, en mis aspiraciones y brindarme su apoyo incondicional en estos años de estudios.

Agradezco a mis maestros por compartir sus conocimientos e innumerables experiencias, sin lugar a dudas formarán parte de mi futuro éxito profesional.

A mi enamorado Joseph Quimí, que con amor y cariño me ha sabido guiar en el área académica, ha sido un pilar fundamental.

Verónica Rodríguez Bernabé

DEDICATORIA

El presente proyecto lo dedico a mis padres.

Joseph Quimí G.

DEDICATORIA

El presente proyecto lo dedico a mis padres.

Verónica Rodríguez B.

TRIBUNAL DE EVALUACIÓN

Ronald Criollo, MSIG.

PROFESOR EVALUADOR

Robert Andrade Troya., MSIG

PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Joseph Quimí G.

Verónica Rodríguez B.

RESUMEN

El presente trabajo se desarrolló con el fin de acceder a la información empresarial en los dispositivos móviles integrando múltiples plataformas y resolver el excesivo riesgo de seguridad que implica compartir los recursos en las redes móviles.

En el ambiente empresarial es muy importante la seguridad, proteger sus bienes inmuebles y salvaguardar la información, con la tendencia BYOD (Bring Your Own Device en español Trae Tu Propio Dispositivo) brinda la facilidad para trabajar en casa y la capacidad de tener todo al alcance de sus manos, la estrategia acogida es añadir el servicio de Google Apps disponible en la nube para complementar el acceso a los recursos de la red de forma segura.

La facilidad de eliminar los datos empresariales de forma remota, ha brindado resultados muy alentadores, separar los perfiles personal y corporativo fue el modelo exitoso, obtuvo una gran acogida por parte de los usuarios porque utilizan un sólo dispositivo y provee mayor confiabilidad e integridad de los datos.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1. EL PROBLEMA.

1.1. Descripción del problema.

CREASOFT ECUADOR es una empresa dedicada al diseño y desarrollo de aplicaciones, su objetivo es ayudar a empresas privadas de diferentes sectores económicos a trabajar de una manera más eficaz. En el día a día se intercambian archivos, almacenan versiones de los sistemas en sus servidores como principales actividades.

El uso de dispositivos móviles, como herramienta de trabajo. En CREASOFT ECUADOR o como en cualquier otro tipo de organización actualmente es muy usual, el hecho de proporcionar comodidad y desplazamiento, de un lugar a otro, hace que los empleados vean muy atractivo su uso, para realizar tareas cotidianas en la oficina.

Esta nueva tendencia tecnológica denominada BYOD (Bring Your Own Device, trae tu propio dispositivo), no consiste únicamente en andar por la oficina con los dispositivos personales tales como tabletas, teléfonos inteligentes y computadoras personales para realizar tareas que hace algunos años era exclusivo de los computadores de escritorio, sino que ha dado muchas implicaciones para la organización y el proceso de trabajo [1].

Los obstáculos que se encuentran en la utilización de los dispositivos ya mencionados, son tan habituales en cualquier tipo de organización, que han sido enmarcados en los siguientes cuatro puntos:

Primero: El problema principal es el riesgo de la seguridad, en la red corporativa, principalmente la amenaza latente de exposición de la información confidencial de la empresa. Por ejemplo, un empleado pierde su teléfono inteligente y no cuenta con una protección adecuada o un sistema de eliminación remota de datos, la persona que lo encuentre puede tener acceso a la información privada de la compañía.

Segundo: La pérdida de datos a través de la exposición de APPs(Término tecnológico que representa a las aplicaciones) no certificadas, Al tener una

gran diversidad de aplicaciones, el control de instalación de alguna de ellas se vuelve complejo, dado que depende de cada usuario, una infectada con malware puede ocasionar que se envié información a terceros.

Tercero: Múltiples plataformas y modelos de dispositivos, dentro de la organización se maneja una cantidad significativa de dispositivos con diversos sistemas operativos y versiones de los mismos, el tener diferentes plataformas hace que se complique aún más la seguridad, debido a la exposición de la infraestructura y confidencialidad de los datos.

Cuarto: Accesos no autorizados a través de redes Wi-Fi inseguras, el administrador debe prever limitaciones en las conexiones inalámbricas, especialmente las que no se encuentran dentro del área de trabajo.

Para resolver los problemas citados, se realiza una estrategia de movilidad y de gestión empresarial, que van de la mano de los objetivos específicos y que se enumerarán posteriormente.

1.2. Objetivos

Objetivo general

Implementar un modelo para la administración de movilidad empresarial en los sistemas multiplataforma en CREASOFT ECUADOR, para aumentar la productividad, la innovación y reducir el área de exposición frente a los problemas de seguridad.

Objetivos específicos

- Realizar investigación para conocer cualitativamente el nivel de productividad e innovación de los empleados.
- Conocer cualitativamente el grado de exposición de la información frente a los problemas de seguridad.
- Diseñar e implementar una solución óptima de protección de los dispositivos móviles.

- Fomentar la productividad laboral con el acceso a los servicios por medio de la red empresarial

1.3. Justificación

El entorno tecnológico en el que está envuelto CREASOFT ECUADOR, lleva a la necesidad de estar actualizado, pendientes de los últimos avances y tendencias, a través de estudios a grandes y medianas empresas. El BYOD se está afianzando y todo apunta a que se seguirá extendiendo.

Los dispositivos móviles seguirán creciendo, junto a sus características, capacidades y posibilidades de utilización, lo que hace necesario evaluar las políticas de seguridad que se ofrecen a estos dispositivos, así como también de medios de protección de la información que gestionan, dentro de los entornos de Tecnologías de la Información y las Comunicaciones (TIC).

Por lo tanto, se debe tomar criterios que garanticen accesos y usos de los recursos de la red empresarial, que permitan gestionar de forma adecuada la diversidad y el despliegue masivo, dinámico y a gran escala de dispositivos móviles en CREASOFT ECUADOR, con el enfoque orientado a incrementar la seguridad, y mejorar de forma paulatina la productividad del usuario final.

El factor desencadenante para la elección de la solución y que ésta sea la más idónea para la organización, es la de una solución multiplataforma, para que finalmente se complemente con la formación y concientización de los empleados en el buen uso de sus dispositivos dentro del área de trabajo.

A continuación, se presenta el estudio realizado en la empresa CREASOFT ECUADOR acerca de la utilización de dispositivos móviles.

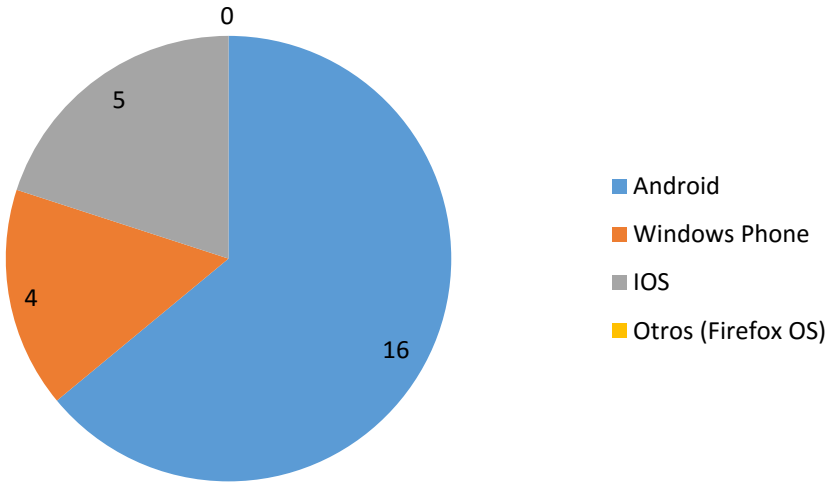

Figura 1.1: Sistemas operativos utilizados [2]

Como se aprecia en el gráfico, el uso de dispositivos móviles tiene una diversidad marcada por los sistemas operativos de tendencia actual.

CAPÍTULO 2

2. LA SOLUCIÓN.

En este capítulo se presenta a “Google Apps For Work” como modelo de administración de movilidad empresarial, además del funcionamiento como solución BYOD dentro de CREASOFT ECUADOR.

2.1. Descripción de la solución propuesta.

Con base a la experiencia en el manejo de “Google Apps For Work” en CREASOFT ECUADOR, se ha definido a la solución como un conjunto de herramientas para la productividad, la misma que está disponible en la nube que es un término para representar el almacenamiento en internet; al mismo tiempo, como objetivo dentro de la organización, se tiene el de establecer la conexión de los usuarios con sus dispositivos, para así poder realizar sus trabajos en cualquier lugar [3].

Su particularidad es la sencillez en su uso, la misma que brinda una nueva forma de trabajo como es la de un equipo online (no las típicas soluciones de correo electrónico y chat), ampliando de esta manera su enfoque a través de videoconferencias, medios sociales, colaboraciones en documentos en tiempo real y mucho más.

2.1.1. Gestión de las diversas plataformas móviles en “Google Apps For Work”.

Los teléfonos inteligentes, tabletas y computadores portátiles en CREASOFT ECUADOR que son gestionados, ahora toma el nombre de Administrador de dispositivos, el mismo que puede aplicar políticas de dispositivos en los mencionados equipos dentro de la organización, llevar a cabo acciones como el de eliminar de forma remota los datos de los dispositivos móviles y múltiples opciones.

Las opciones que se puede utilizar son:

- Establecer la configuración móvil en unidades organizativas, igual como se tiene en el diagrama jerárquico de CREASOFT ECUADOR.
- Controlar la conexión de dispositivos con la lista blanca de IP, la misma que es un registro de direcciones; además, se puede elegir que teléfono inteligente se habilita enlazar con los datos de Google Apps.
- Visualizar en tiempo real los dispositivos móviles de la organización y que equipos se conectan a través de los sincronizadores de información tales como Google Sync, Android Sync o iOS Sync.
- Ver todas las aplicaciones que acceden a los datos de Google Apps instaladas en los diferentes dispositivos de CREASOFT ECUADOR.

Gestión en dispositivos con sistemas operativos Android.

Los dispositivos con sistemas operativos Android, son gestionados a través de la APP denominada política de dispositivos. A continuación, se muestra una lista de políticas de seguridad que se pueden aplicar en los dispositivos de CREASOFT ECUADOR:

- Nivel de seguridad de la contraseña del dispositivo
- Longitud de la contraseña del dispositivo
- Número de contraseñas no válidas permitidas antes de eliminar los datos del dispositivo de forma remota
- Número de contraseñas caducadas recientemente que están bloqueadas
- Número de días que tardará en caducar la contraseña del dispositivo

- Tiempo de inactividad antes de que se bloquee un dispositivo de forma automática
- Auditoría de la aplicación
- Eliminación de la cuenta de un dispositivo de forma remota
- Eliminación de datos de un dispositivo de forma remota
- Requisitos de versión de la aplicación Política de dispositivos
- Número de días que el dispositivo no se sincroniza antes de eliminar los datos
- Bloqueo de dispositivos con seguridad comprometida.

Requisitos de Android

- Android 2.2 denominada “Froyo” o superior para instalar políticas de dispositivo para Android [4].
- Android 5.0 para desplegar Android For Work [5].
- Acceso en Google Play o un navegador
- Tener acceso a una cuenta corporativa

El administrador de sistemas de CREASOFT ECUADOR cumple varios roles, en los que desarrolla actividades relevantes como la aplicación de políticas de seguridad y la eliminación de datos, de manera remota.

Para aplicar políticas de seguridad se usa la página de configuración móvil en la Consola de Administración, se establece una contraseña en los dispositivos de los usuarios y se instaura los requisitos.

Arquitectura de gestión Android

Google proporciona un servicio a CREASOFT ECUADOR, denominado Google Cloud Messaging (GCM), la misma que se utiliza para el envío de mensajes desde los servidores de la solución

hacia los dispositivos móviles gestionados, en concreto hacia a la APP o agente de gestión de la solución y viceversa.

El cliente, es el agente o app de gestión que ejecuta el dispositivo móvil Android, que debe registrarse en GCM y recibir como resultado un identificador de registro. El servidor MDM, implementa el protocolo GCM y se comunica con la app instalada en el dispositivo móvil a través de los servidores de conexión GCM de Google; los servidores de conexión GCM se encargan de encolar, almacenar y reenviar (cuando el dispositivo móvil está disponible u online), en la siguiente figura se puede observar las notificaciones entre los servidores MDM y las apps.

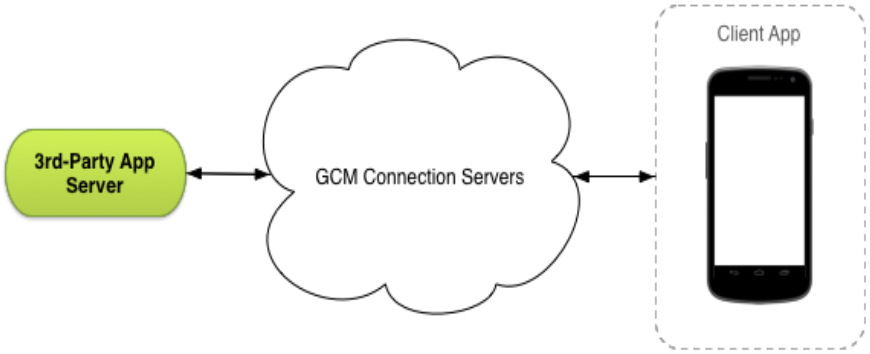

Figura 2.1: Proceso de notificación en Android [6]

Gestión en dispositivos con sistema operativo iOS.

La gestión y configuración avanzada de los dispositivos móviles iOS de CREASOFT ECUADOR, se realiza a través de perfiles de configuración, empleando ficheros XML, que aprovechan las capacidades de gestión de la API de iOS definidas por Apple.

La característica principal, es que no es necesario instalar una aplicación nueva para registrar el dispositivo, sólo es necesario configurar un certificado digital para establecer un canal seguro entre la solución y los dispositivos Apple.

Los perfiles de configuración, permiten establecer políticas de seguridad en los dispositivos móviles iOS, así como también habilitar restricciones en el uso de los mismos y ajustar diferentes parámetros de configuración. Se debe tomar en cuenta las siguientes opciones:

- **Habilitar iOS Sync:** Se utiliza la Consola de Administración de Google para habilitar iOS Sync, en los dispositivos actuales de Apple ya viene instalada de forma predeterminada, esto quiere decir, que cualquier usuario del dominio creasoftecuador.com puede utilizar la solución de Google Apps for Work en dispositivos iOS.
- **Aplicar políticas en dispositivos iOS:** La Consola de Administración se utiliza para aplicar políticas en los dispositivos iOS.
- **Una nota de relevancia:** Se debe configurar Apple Push Certificate, esto quiere decir básicamente, la configuración del certificado para el uso de administración.
- **Habilitar CalDAV:** Para poder usar Google Calendar, se configura los dispositivos iOS de los usuarios para que se sincronicen a través de CalDAV,
- **Incluir en lista blanca las aplicaciones de iOS:** La lista de aplicaciones disponibles para utilizar se considera lista blanca, las aplicaciones gratuitas de iOS que los usuarios pueden descargar, deben ser incluidas en la lista blanca, a través de la consola de administración, como aplicaciones administradas en el dispositivo iOS desde la aplicación Política de dispositivos.

La solución en iOS permite llevar a cabo tres tipos de tareas principales, tras su registro inicial en CREASOFT ECUADOR:

- Modificar y actualizar los ajustes de configuración de manera remota a través de la instalación, actualización y eliminación

de perfiles de configuración y aprovisionamiento. El conjunto de ajustes de configuración disponibles está definido por Apple en función de la versión de iOS.

- Monitorizar el cumplimiento de las políticas corporativas a través de la realización de consultas sobre el dispositivo móvil.
- Gestionar las apps y el propio dispositivo móvil.

Requisitos de iOS Sync

- Dispositivos iOS (iOS 7 o versiones superiores) [7].
- Usuario con una cuenta de Google Apps for Work, Educación o Gobierno.
- Los usuarios de CREASOFT ECUADOR deben utilizar la versión más reciente de una de estas aplicaciones: Gmail, Google Calendar, Google Drive, Documentos de Google o Presentaciones de Google.

Gestión en dispositivos Windows Phone

El uso de Microsoft Exchange ActiveSync es la recomendación esencial para la administración en este sistema operativo, puede sincronizar el correo de Google Apps, los contactos y calendarios en los teléfonos inteligentes y tabletas de CREASOFT ECUADOR.

Windows Phone 8, dispone por defecto de un agente de gestión, que permite comunicarse con el MDM de google y llevar a cabo el proceso de registro inicial en la solución (enrollment) mediante MS-XCEP; la instalación de una App permite el acceso al mercado de apps privado de la organización, la posterior instalación de nuevas Apps aprobadas por la organización, así como la consulta de información y configuración del dispositivo móvil según las políticas de seguridad corporativas [8].

Requisitos para Windows Phone

- Dispositivos Windows Phone 7.5 o superior [9].
- Usuario con cuenta en Google Apps for work.

Habilitar correos

Luego de habilitar el dispositivo con Google Sync, la plataforma le permite enviar y recibir correo empresarial con Microsoft Exchange.

2.1.2. Características y capacidades de Google Apps for Work.

Como puntos esenciales, para beneficio de CREASOFT ECUADOR se encuentra, una extensa documentación e implementación de operaciones con base a mejores prácticas, principalmente en torno a la seguridad y a la protección de los datos de usuarios. A continuación, se ofrecen características adicionales:

- **Modelo de licencias,** se utiliza 2 tipos de cuentas, la flexible que es una licencia que puede ser renovada periódicamente (mensualmente o anualmente) y una anual que tiene como beneficios un costo inferior [10].
- **El contrato de la solución**, es por usuario e independientemente del número de dispositivos de la organización [10].
- **Soporte y mantenimiento**, se establecen actualizaciones de seguridad y errores que se presenten, además del tipo de acceso al servicio de soporte (e-mail, teléfono, presencial, etc.), el horario de soporte son las 24 horas y los sietes días de la semana. [11].
- **Posibilidad de personalizar,** interfaz de usuario con el logo de CREASOFT ECUADOR, colores y otras preferencias de la organización [12].

- **La gestión y administración de los logs**, tanto de los terminales gestionados, como de la solución [13].
- **Capacidad de administración independiente,** se efectúa por cada departamento o ubicación, permitiendo la existencia de administradores independientes para cada grupo a gestionar. [14]

Desde el punto de vista técnico, la administración en CREASOFT ECUADOR, se realiza a través de una interfaz web, que se accede por medio de cualquier navegador soportado, como: IE, Firefox, Safari, Chrome, Opera, entre otros.

La gestión de los dispositivos móviles en la organización, es llevada por parte del administrador TIC en una consola de gestión, también denominado panel de control o dashboard de la solución, que permite la realización de consultas, ejecución de políticas de seguridad, así como también la visualización de alertas.

Registro de los dispositivos móviles

Uno de los pasos iniciales y fundamentales de CREASOFT ECUADOR en Google App for Work, es formular el registro de prueba por 30 días. Una vez activada la cuenta, se da lugar a los ajustes de configuración, restricciones y controles de acceso definidos con base a las políticas de seguridad de la organización.

En el entorno de CREASOFT ECUADOR, por motivos de escalabilidad, el usuario lleva a cabo el proceso de registro, Posterior a la configuración inicial de la solución, se lleva a cabo la aprobación y el registro de cada dispositivo móvil, con el objetivo de establecer comunicación entre la plataforma y el teléfono.

Finalmente, se proporcionan mecanismos que permiten al administrador de CREASOFT ECUADOR aprobar o rechazar, por lotes o grandes grupos de dispositivos móviles de una manera

sencilla, en otras palabras, el registro inicial de los dispositivos en la solución

A continuación, se detallan algunos puntos importantes en el registro dentro de CREASOFT ECUADOR:

- **Autenticación de usuario:** se validan las credenciales para establecer qué tanto usuario y dispositivo móvil se encuentran aprobados y autorizados en la solución.
- **Capacidad de integración con servidores LDAP,** tanto para la autenticación de usuarios como para permitir la aplicación de diferentes políticas de seguridad por usuario, grupo, unidad organizativa (OU) [15].
- **Opcionalmente**, la distribución y el registro de certificados digitales para la identificación del dispositivo móvil o el usuario por la arquitectura de la organización.

Políticas de Privacidad establecidas.

Uno de los puntos que se cataloga últimamente controversial, es el relacionado con la privacidad.

La cultura tecnológica adquiere un papel importante en las empresas como es el caso de CREASOFT ECUADOR, la sociedad moderna se acopla fácilmente a los cambios, no así las personas de mayor edad que se niegan al uso de la tecnología por su estilo de vida a la que están acostumbrados por muchos años. Existen numerosas implicaciones legales asociadas al uso de dispositivos móviles y los datos que éstos gestionan en entornos BYOD.

Objetivos de la privacidad [16]

- No se almacenan datos de la organización para uso de publicidad.
- Acceso exclusivo de los datos a los administradores y usuarios registrados dentro de la organización.

- Aplicaciones no recolectan información, ni imágenes, ni posiciones geográficas a través de GPS, tampoco fotos o datos.

Monitoreo y reportes.

Una característica relevante es poder monitorear el tráfico de la red en CREASOFT ECUADOR, inspeccionando comportamiento sospechoso, como la presencia de tráfico que podría indicar conexiones remotas no autorizadas.

Las capacidades de monitorización y búsqueda son establecidas considerando diferentes criterios, por grupos de usuarios (Ej. altos ejecutivos y responsables de departamento), por tipo de dispositivo o plataforma móvil (Ej. Android) o incluso por el operador de telecomunicaciones.

Finalmente, el rastreo de las aplicaciones en CREASOFT ECUADOR se puede elaborar dependiendo de parámetros tales como días, usos y usuarios que acceden y se vean reflejados en los informes.
Los informes que se proporcionan, tiene la opción de facilitar la auditoría dar un resumen de cualquier información con respecto a la administración, ajustes y estados, entre ellos [17]:

- Estado de verificación
- Estado de la cuenta
- Estado de la administración
- Las cuotas de almacenamiento
- La visibilidad de documentos
- Flujo de correo electrónico
- El recuento de archivos de unidad entre otros.

Los informes generan cuadros estadísticos y gráficos que muestran información para todos los usuarios en todos los dominios de Google Apps.

2.2. Gestión de las políticas de seguridad en CREASOFT ECUADOR.

Las políticas de seguridad incluyen diversos ajustes de configuración que atañen a elementos y componentes del dispositivo móvil, como son: interfaces de comunicaciones, módulos de hardware y utilización de apps entre otros. Los detalles de configuración de los componentes son analizados, permiten llegar a una óptima utilización de la solución, sin violar la privacidad de los usuarios de CREASOFT ECUADOR.

El punto fundamental de la solución es la capacidad de configurar los dispositivos móviles a través de política de seguridad de forma remota, sin importar dónde se encuentren ubicados, esto se logra a través de comunicaciones inalámbricas que son las redes Wi-Fi o de telefonía móvil 2/3/4G. Por lo cual, se debe definir perfiles de configuración, según el tipo de dispositivo móvil, usuario y el nivel de acceso asociado (empleando el servidor LDAP)

2.2.1. Restricciones en el hardware y software del dispositivo móvil.

Se puede limitar con la mayor granularidad existente, es decir un nivel de detalle muy profundo, los diferentes módulos y componentes del hardware, especialmente en dispositivos Android que es el sistema operativo predominante en CREASOFT ECUADOR. Por ejemplo, se deshabilitan elementos que permitan obtener información y datos, como la cámara, el módulo de localización, la tarjeta de almacenamiento externa: igualmente, se puede deshabilitar todas las interfaces de comunicaciones existentes en el dispositivo móvil, tanto cableados como inalámbricos, como el puerto USB o los interfaces NFC, Bluetooth, Wi-Fi, telefonía móvil 2/3/4G, etc.

Complementariamente se logra deshabilitar el acceso a las Apps o elementos software que hacen uso del hardware descrito.

Protección remota

El administrador de CREASOFT ECUADOR, con el objetivo de minimizar recursos TIC, establece a través de políticas de seguridad de la organización que el usuario final, también pueda usar la protección remota, como por ejemplo, localización del dispositivo móvil y el borrado remoto de sus datos.

Gestión y borrado de datos remotos

Una de las características que tiene relación directa con la protección remota del dispositivo móvil, es la de permitir el borrado remoto parcial o completo del dispositivo. La operación de borrado completo, restaura en el dispositivo los ajustes de fábrica y elimina todos los datos existentes.

Se determinan los siguientes pasos frente a un dispositivo móvil perdido o robado para proteger los datos de CREASOFT ECUADOR:

- Intentar localizar la ubicación física del dispositivo móvil a través de la solución.
- Bloquear el dispositivo móvil remotamente para no permitir el acceso no autorizado al mismo.
- Llamar al número de teléfono del dispositivo, o forzar de forma remota al dispositivo móvil a emitir un sonido (a través de las capacidades de gestión) que permita su localización.
- Llevar a cabo el borrado de datos remoto, selectivo o completo, del dispositivo móvil.

Servicios de localización.

Una de las funcionalidades de los dispositivos móviles que se encuentran en las instalaciones de CREASOFT ECUADOR, es la disponibilidad de múltiples capacidades o servicios de localización,

que permiten obtener su ubicación física con mayor o menor exactitud, dependiendo de las condiciones y los métodos empleados.

Las plataformas móviles, que disponen los empleados de CREASOFT ECUADOR son de dos tipos de mecanismos de localización, que permiten obtener su ubicación actual:

- Localización de mayor precisión, en el exterior y/o espacios abiertos, a través del módulo GPS del dispositivo móvil y de los satélites GPS.
- Localización de menor precisión, pero que funciona incluso en recintos cerrados y en el interior del edifico, a través de las torres de telefonía móvil y redes WiFi cercanas.

La solución no sólo permite localizar la ubicación de un dispositivo móvil en un momento dado, por ejemplo si éste ha sido perdido o robado, sino que también permite realizar un seguimiento detallado de la ubicación del dispositivo de manera periódica o permanente (*tracking*), rastreando así la ubicación y el desplazamiento del dispositivo móvil a lo largo del día.

2.2.2. Gestión de los datos almacenados en el dispositivo móvil.

Adicionalmente, a las capacidades de borrado remoto de datos y de la protección del acceso a los dispositivos móviles que se cuenta en CREASOFT ECUADOR, se tiene capacidades de cifrado de los datos que almacenan. Las plataformas móviles actuales disponen de capacidades nativas, para el cifrado completo del dispositivo móvil y funcionalidad asociada normalmente a la existencia de un código de acceso.

Gestión de certificados digitales.

Al evaluar, la gestión de certificados digitales de la solución en CREASOFT ECUADOR, se define como mínimo dos repositorios para el almacenamiento de certificados:

- Certificados digitales personales: permiten almacenar los certificados propios del dispositivo móvil y/o usuario que pueden ser utilizados como mecanismos de autenticación.
- Certificados digitales de las autoridades certificadoras (CA's) de confianza: permiten establecer qué CA's serán consideradas de confianza por el dispositivo móvil, incluyendo tanto CA's raíz como intermedias. La lista de CA's de confianza existente por defecto es establecida por el fabricante de la plataforma móvil.

Se dispone de capacidades de gestión de certificados digitales, tanto para los certificados personales como de nuevas CA's propias de CREASOFT ECUADOR para las siguientes funcionalidades de conexión:

- Redes Wi-Fi
- Redes VPN
- Navegación web (SharePoint, aplicaciones web, etc.)
- Correo electrónico (e-mail) y S/MIME
- Cuentas de Microsoft Exchange ActiveSync (EAS)
- Comunicación con la solución MDM

2.2.3. Gestión de apps.

Uno de los elementos fundamentales a considerar en las plataformas móviles modernas, y motivo principal por el que a los terminales móviles actuales se les referencia con el término *smartphones*, es la posibilidad de instalar aplicaciones móviles o Apps.

Las Apps son clasificadas en diferentes categorías, por ejemplo, desde Apps profesionales de productividad, ampliamente utilizadas en entornos corporativos, pasando por Apps de acceso a servicios en Internet (como redes sociales, portales web, servicios "en la nube", etc.),

Uno de los objetivos fundamentales de la gestión de aplicaciones empresarial (MAM) es poder proporcionar a los usuarios de CREASOFT ECUADOR un conjunto de apps necesario para su trabajo.

Gestión de los mercados públicos de Apps.

La solución permite gestionar la instalación de Apps desde los mercados públicos oficiales, disponibles en internet para cada una de las plataformas móviles, como Google Play (Android), Apple's App Store (iOS) o Microsoft Windows Phone Store, además de la instalación de Apps a través del mercado corporativo de Apps de CREASOFT ECUADOR.

Gestión en la distribución de las Apps.

La solución admite la distribución de Apps mediante la recepción automática (notificaciones push) por parte del usuario, un mensaje le indica la existencia de una nueva App, una nueva versión de Apps para su instalación o actualización [18].

En CREASOFT ECUADOR, es de gran utilidad las Apps gestionadas dado que no se necesita la intervención del usuario.

2.2.4. Gestión de las comunicaciones.

En CREASOFT ECUADOR, la solución otorga mecanismos de conectividad, disponibilidad y estado de las diferentes interfaces de comunicaciones inalámbricas del dispositivo móvil, como NFC (Near Field Communications), Bluetooth, WiFi, telefonía móvil 2/3/4G, etc.

Al desplegar la solución, se requiere un mayor control sobre todas las comunicaciones de datos, originadas desde el dispositivo móvil, por ejemplo, forzando el establecimiento y la utilización de una conexión VPN cifrada antes de enviar algún tipo de tráfico, asegurando la utilización de mecanismos de autenticación mutua antes de transmitir

ningún tráfico, o seleccionando la interfaz de comunicaciones a emplear en cada momento Wi-Fi o telefonía móvil 2/3/4G [19].

Los siguientes apartados proporcionan ejemplos del tipo de capacidades de gestión de las comunicaciones móviles que se encuentran en CREASOFT ECUADOR requeridas en las soluciones MDM, pero sin ser completamente detallados.

NFC Near Field Comunication. Tecnología de comunicación inalámbrica cercana.

Las opciones de configuración disponibles para soporte NFC son muy limitadas, solo permite habilitar o deshabilitar el interfaz.

Bluetooth.

La solución, permite al dispositivo móvil configurarse de forma permanente como no visible u oculto, siendo necesario que durante los emparejamientos sea el otro dispositivo Bluetooth el que esté visible. Esta es la configuración recomendada desde el punto de vista de seguridad.

WI-FI.

Por ser una tecnología de comunicación muy popular, tiene capacidades avanzadas de gestión. En primer lugar, se define con qué tipo de redes Wi-Fi, se permite al dispositivo móvil establecer una conexión. Al mismo tiempo, en temas de políticas de seguridad, se define como muy restrictiva, al establecer listas de redes Wi-Fi permitidas denominadas listas blancas, a las que pueden conectarse los dispositivos móviles gestionados.

La opción recomendada, es tener una configuración Wi-Fi restrictiva, que sólo permita al dispositivo móvil conectarse a la red Wi-Fi corporativa y que se prohíba establecer conexiones con cualquier otra red, especialmente las redes Wi-Fi públicas que no cuentan con mecanismo de protección. La seguridad de la red Wi-Fi corporativa debería emplear WPA2 Empresarial, y los clientes deben

configurarse adecuadamente para verificar su identidad a través de los parámetros y certificados digitales correspondientes.

TELEFONÍA MÓVIL 2/3/4G.

Respecto a las comunicaciones móviles, es posible habilitar o deshabilitar de forma independiente las comunicaciones de voz (y SMS/MSM) y las comunicaciones de datos (2/3/4G).

La solución MDM permite gestionar las capacidades de compartición de la conexión de datos con otros dispositivos (conocidas como tethering), incluyendo la aplicación de restricciones sobre los métodos de tethering permitidos (Bluetooth, Wi-Fi y/o USB) y los ajustes de seguridad de las redes de comunicaciones asociadas.

2.2.5. Gestión de VPN.

La solución aprueba la gestión de dispositivos móviles con un nivel de seguridad alto. Las conexiones hacia la oficina de CREASOFT ECUADOR desde una zona fuera de la intranet son proporcionadas por VPNs, que es un túnel privado con credenciales y claves secretas precompartidas y asociadas a la cuenta de usuario, para establecer la conexión segura hacia los servidores.

La posibilidad de establecer una conexión VPNs por App (o VPNs selectivas) permite proteger con más granularidad la transferencia de datos corporativos, minimizando colateralmente el consumo de batería y reduciendo el tráfico de red. Las Apps personales no son asociadas y la transferencia no tiene porqué ser protegida necesariamente [20].

Las VPNs para CREASOFT ECUADOR son configuradas por el Superadministrador en el Administrador de dispositivos, se configura por usuario y los ajustes se aplican a los dispositivos móviles, se agrega la configuración VPN por L2TP u OpenVPN que viene integrada, más detalles en el Anexo A, manual de usuario.

Configuración del dispositivo de Redes Privadas Virtuales. Además, se utiliza para comunicar los servidores de la empresa en la ciudad de Guayaquil con los servidores de la solución en Google.

VPN de hardware.

La VPN por hardware se limita al router Cisco RV320 de CREASOFT, las características de 25 túneles IPsec de sitio a sitio para conectividad de sucursales, 25 túneles VPN IPsec a través del cliente VPN de Cisco y clientes de terceros para la conectividad VPN de acceso remoto. Asimismo, utiliza una línea alquilada para la conexión a internet y requiere que el router tenga conexión a internet de manera permanente, lo que le hace ser persistente.

Una ventaja es que son rápidas comparadas con las basadas en software.

VPN con L2TP.

L2TP es económico, compatible con Windows Phone, Android y iOS, combinando con IPSec para proporcionar seguridad a la conexión de redes locales remotas y proteger la información en los sitios. Con IPSec se utiliza una clave precompartida. Para hacer la configuración en los puntos usa el nombre de la VPN vpncreasoft con L2TP/IPSec.

VPN con OpenVPN.

OpenVPN implementa las VPN en los clientes, los dispositivos con sistema operativo iOS localizan y descargan el programa en tienda de aplicaciones Apple Store, en Android está ubicado en Play Store.

El siguiente cuadro compara los protocolos que se pueden emplear para la conexión.

	L2TP/IPSec	OpenVPN
CIFRADO	256-bit	160 bits 256-bit
SEGURIDAD VPN	Optimo cifrado. Comprueba la integridad de los datos y encapsula los datos dos veces.	Optimo cifrado. Autentifica los datos con certificados digitales.
VELOCIDAD DE VPN	Necesita más proceso de la CPU para encapsular los datos dos veces.	Rendimiento y velocidades elevadas, probado en alta latencia y conexiones de grandes distancias.
ESTABILIDAD	Compatible con dispositivos NAT.	Muy confiable utilizando routers inalámbricos con puntos de acceso Wi-Fi.

Tabla 1: Características de los tipos de VPNs [21]

2.2.6. Ancho de banda

El ancho de banda necesario para el funcionamiento correcto es de 9Mbps para los 20 empleados. La solución Google Apps For Work

garantiza que 15 empleados tengan comunicación exitosa en videoconferencia con aplicación Hangouts, cada usuario consume 512kbps ancho de banda, con video de alta calidad.

Nota. El ancho de banda mínimo es de 300 kbps de entrada y salida.

Aplicaciones	Usuarios recurrentes	Ancho de banda garantizado	Subtotal
Streaming de video	15	512Kbps	7680 kbps
Correo y otros	5	256Kbps	1280 kbps
Total			8960Kbps

Tabla 2: Ancho de banda requerido

CREASOFT ECUADOR garantiza 512 Mbps para los 15 usuarios recurrentes y que puedan utilizar videoconferencias, el límite de ancho de banda por día para clientes web es de 1250 MB de descarga y de 500 MB de subida [22].

2.3. Diagrama de la solución.

La empresa cuenta con infraestructura propia, un espacio para un cuarto de telecomunicaciones, utilizado para la integración de la solución con el servidor Active Directory, se procede con la configuración a través de herramientas de sincronización denominada GADS Google Apps Directory Sync. En la siguiente Figura 2.2. Se puede observar el diagrama que establece la comunicación entre la solución de Google Apps For Work y los recursos de la empresa CREASOFT ECUADOR, es una arquitectura cliente–servidor, el cliente es el agente o App de gestión que se ejecuta en el dispositivo móvil, el mismo debe disponer de una cuenta de Google previamente activada.

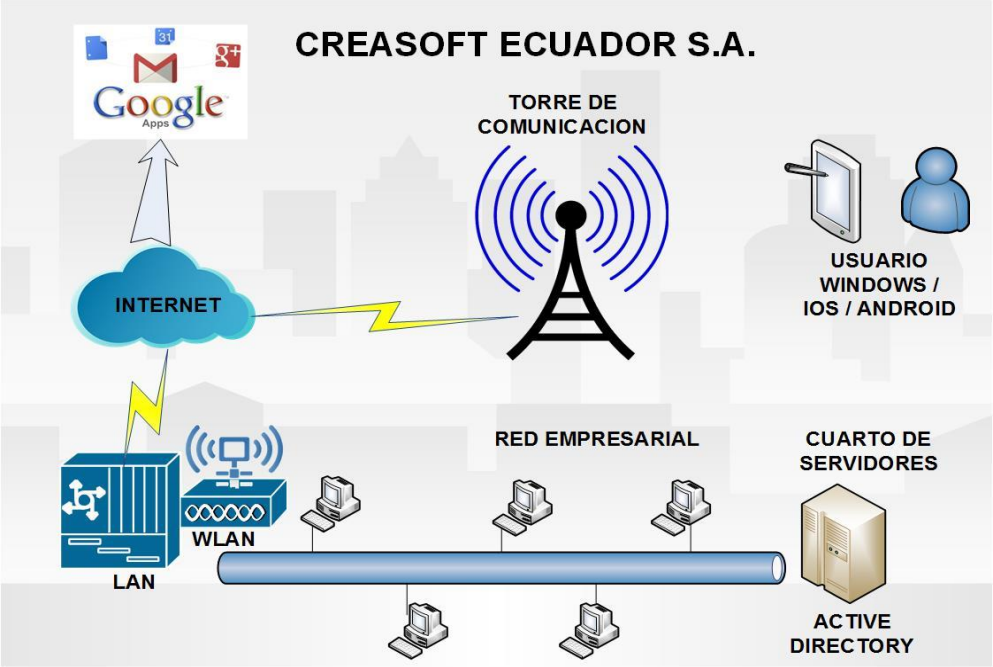

Figura 2.2: Diagrama de la Solución.

Asimismo se instaura la utilización de una conexión VPN cifrada antes de enviar algún tipo de tráfico, asegurando la utilización de mecanismos de autenticación mutua antes de transmitir, seleccionando la interfaz de comunicaciones a emplear en cada momento, Wi-Fi o telefonía móvil 3/4G.

La siguiente Figura 2.3 muestra la descripción de la estructura organizativa de la empresa, la misma que es aplicada en la solución planteada, utilizando contenedores que son unidades organizativas.

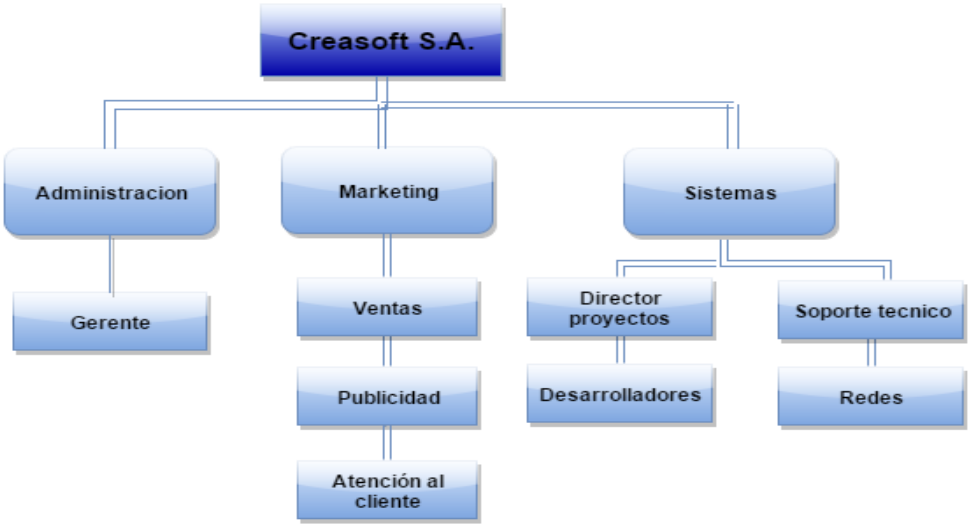

Figura 2.3: Estructura organizativa de CREASOFT ECUADOR

Cada unidad organizativa, representa los departamentos en CREASOFT ECUADOR, donde se establece la creación de cuentas de usuarios, con su respectiva dirección de correo electrónico para el uso de la solución

Descripción técnica.

Cuenta con un servidor, que se encuentra en funcionamiento con el servicio de Active Directory y de un Router Cisco VPN con WAN Gigabit dual RV320.

Para obtener y establecer acceso seguro, se utiliza un router Cisco® Small Business de la serie R. que tiene como nombre comercial router Cisco VPN con WAN Gigabit dual RV320 (ver Anexo B. Datasheet"), en el que se detallan características y ventajas en el ámbito de seguridad

.

Descripción	Especificación
VPN	
Seguridad IP (IPsec)	25 túneles IPsec de sitio a sitio para conectividad de sucursales 25 túneles VPN IPsec a través del cliente VPN de Cisco y clientes de terceros como “The GreenBow”para la conectividad VPN de acceso remoto
VPN con SSL	10 túneles VPN con SSL para acceso remoto de clientes
PPTP	10 túneles PPTP para acceso remoto
Cifrado	Estándar de cifrado de datos (DES) ● Estándar de triple cifrado de datos (3DES) Cifrado con norma de cifrado avanzado (AES): AES-128, AES-192, AES-256

Tabla 3: Características del Router

2.4. Implementación de la Herramienta.

Para implementar la solución, se cuenta con los servidores de CREASOFT ECUADOR, la ejecución de servicio de directorio se realiza en un servidor con sistema operativo Windows Server 2012, se selecciona el dominio de autenticación para sincronizarla y conectarla con la solución de Google. A continuación se señalan los puntos importantes en el proceso de implementación.

2.4.1. Planificación.

En esta etapa, se prepara a la organización con varias actividades en la que se gestiona la migración a la plataforma de Google Apps y la realización de reuniones de trabajo, donde se elabora un plan de acción para el proceso de implementación y migración de

CREASOFT ECUADOR (ver Anexo C. Diagrama de Gantt), considerando mejores prácticas.

El diagrama muestra el orden recomendado y las tareas a realizar durante cada fase de transición de Google Apps.

Fase inicial, exclusiva del equipo de IT.

Sólo los miembros del equipo de IT de CREASOFT ECUADOR, comienzan a utilizar la solución durante la fase inicial. Esto brinda al equipo la oportunidad de familiarizarse y planificar las próximas dos fases.

Se empieza a enviar correo en Google Apps con el dominio creasoftecuador.com, aunque ninguna migración de datos heredados ocurre aun en esta fase. (ver Anexo D. modelo de correo electrónico).

Fase de adopción.

El propósito de esta fase es llevar a cabo una transición, pero a pequeña escala, como una prueba de concepto. Aproximadamente el 10 por ciento de los miembros de CREASOFT ECUADOR fueron seleccionados, para poder comenzar a utilizar Google Apps. Estos son los primeros en adoptar una sección transversal de la solución, que incluye una mayor cantidad de funciones con respecto a la fase inicial.

El comienzo de la migración de datos del antiguo sistema, incluyendo las cuentas de usuarios, correos y datos del calendario se realiza en esta fase.

Fase Final.

Como fase final, todo CREASOFT ECUADOR está utilizando la solución de Google. La tarea principal en esta etapa es solucionar problemas que surgen, mientras el resto de los usuarios se aclimata a su nuevo flujo de trabajo. Para ayudar a facilitar la transición, el

equipo IT tiene horas de oficina extendida y sus primeros usuarios pueden servir como guías de Google, responder a las preguntas básicas de sus pares y dirigir las preguntas más avanzadas a su equipo de TI.

2.4.2. Configuración.

Una vez, efectuada la etapa de planificación, se realizan una serie de validaciones y acciones técnicas que servirán como base a la integración de la infraestructura de CREASOFT ECUADOR con la nube de Google. Se establecen las herramientas para este proceso a continuación.

Integración de la infraestructura.

Para establecer la comunicación entre Google Apps y Active Directory se utiliza Google Apps Directory Sync (GADS). Otro punto de la integración es sincronizar las contraseñas, para eso se usa Google Apps Password Sync. Para los diversos dispositivos Android y Windows Phone se usa Google Sync, en dispositivos iOS se emplea iOS Sync.

Observaciones de GADS.

Se realiza una sincronización unidireccional, los datos del servidor LDAP no se actualizan ni se modifican nunca, se ejecuta como una utilidad en tu entorno de servidor y no es posible acceder a los datos del servidor del directorio LDAP fuera del área de la empresa [23].

Acerca Google Apps Password Sync (GAPS).

Se sincroniza automáticamente las contraseñas, los usuarios de Google Apps con las cuentas de Microsoft Active Directory de CREASOFT ECUADOR.

GAPS tiene como objetivo nunca cambiar la contraseña de Active Directory de un usuario, al momento que Active Directory cambia las contraseñas, GAPS lo sincroniza.

Acerca de Google Sync.

Google Sync utiliza Microsoft Exchange Active Sync, cumple con la función de aplicar políticas de seguridad, sincronizar el calendario, lista de direcciones, correos actualizados cada minuto, además permite importar datos de correo de CREASOFT ECUADOR [24].

2.4.3. Gestión del cambio.

El objetivo de esta etapa es facilitar la migración y minimizar el impacto a nivel de usuario, es la fase con mayor duración del proceso de implementación, depende de la disponibilidad de los usuarios para involucrarse con las distintas herramientas que se dispone. (ver Figura 1. Manual de usuario).

2.4.4. Despliegue.

Finalizada esta etapa, CREASOFT ECUADOR está conectada con la nube de Google y utiliza Google Apps como herramienta de comunicación, colaboración y productividad. La tarea principal en esta etapa es asegurar la aclimatación de los usuarios a su nuevo flujo de trabajo.

Apoyo y soporte al usuario.

La ayuda a los usuarios tiene breves guías, muchas de estas pautas ya están incluidas en el Centro de Aprendizaje de Google, pero también se puede enviar una de estas guías independientes para los usuarios de CREASOFT ECUADOR cada semana, con contenidos de:

- Información sobre Google Apps para móviles y cómo los usuarios pueden recibir su correo electrónico desde cualquier lugar.

- Actualizaciones de Producto, se puede ver las nuevas características de Google Apps y los cambios visitando .
- Recursos y recomendaciones están disponibles en línea.
- Recursos localizados Vídeos de formación: videos a propio ritmo que cubren los conceptos básicos de correo electrónico, Calendario y Docs

2.5. Recursos financieros.

Se detalla los planes que se muestran en google [25], [26].

	Plan flexible	**Plan anual**
Compromiso	Ninguno	Servicio durante un año completo para las licencias de usuario que tengas al iniciar el contrato
Ciclo de facturación	Mensual	Mensual
Pago mensual	Google Apps for Work: $5 por usuario Google Apps Unlimited: $10 por usuario	Google Apps for Work: $4,34 por licencia de usuario
Total anual	Google Apps for Work: $ 52.13 por usuario Google Apps Unlimited: $ 104.27 por usuario	Google Apps for Work: $ 43.92 por licencia de usuario
Añadir a usuarios	En cualquier momento por un coste mensual adicional	En cualquier momento por un coste mensual adicional
Eliminar a usuarios	En cualquier momento (reduce el coste mensual)	Eliminas las licencias de usuario solo al renovar el contrato anual. Hasta ese momento pagas por todas las licencias adquiridas.
Cancelar el servicio	En cualquier momento sin penalización	Debes pagar el compromiso anual (incluso si lo cancelas antes).

Tabla 4: Planes de Google Apps For Work

Debido a que CREASOFT ECUADOR se considera una empresa con muchos cambios en su personal, se toma la decisión de seleccionar un Plan denominado flexible, el mismo que se factura mensualmente por cada cuenta de usuario.

También tiene varios criterios que son apropiados, como son el añadir y eliminar cuentas en cualquier momento, y pagar cuentas que se utiliza durante ese mes. Igualmente permite cancelar el servicio en cualquier momento sin ninguna penalización.
Los valores para el despliegue de la solución se detallan de forma anual e incluye todos los trabajadores de la empresa.

COSTO DE IMPLEMENTACIÓN	
Licenciamiento anual con correo empresarial, llamadas de voz y videos, 30 Gb de almacenamiento	$50.00
Número de usuarios	20
Total	$1000.00

Tabla 5: Costo de la implementación.

Forma de pago principal

Se determina que la forma más óptima es cancelar con tarjeta de crédito debitando mensualmente, ya que las suscripciones de la cuenta de facturación señalan que existen problemas con cuentas bancarias en países sudamericanos.

En la facturación, las opciones de números de usuarios, detalle de facturación, información de usuarios activos y forma de pago se encuentra en la ventana factura.

CAPÍTULO 3

3. ANÁLISIS Y PRUEBAS

En este capítulo, se realizan pruebas en varios escenarios para demostrar que el uso de la solución contrarresta las amenazas tecnológicas más comunes y expone los beneficios que brindan a CREASOFT ECUADOR.

La información almacenada en el teléfono de cada empleado es personal y los datos de la empresa no deben mezclarse, conjuntamente cifra el contenido almacenado, las pruebas que garantizan la integridad de los datos son:

- Acceso físico no autorizado del dispositivo móvil, protección mediante contraseña.
- Eliminación de cuenta de usuario de la empresa.
- Instalación automática y acceso a las aplicaciones autorizadas.
- Separación de aplicaciones del usuario y la de trabajo.
- Registro no autorizado de dispositivos, acceso de credenciales por ingeniería social.
- Auditoria mediante los informes.
- Protección contra la manipulación de la información transmitida: Ataques de hombre en medio (MitM, Man-in-the-Middle).

3.1. Prueba número uno, acceso físico no autorizado del dispositivo móvil

Como escenario se tiene que una persona no autorizada, tiene acceso a un teléfono de CREASOFT ECUADOR. Al momento de ingresar diez veces la contraseña sin éxito, el teléfono muestra un mensaje de alerta indicando que los datos empresariales se eliminarán del teléfono, entonces alcanza el objetivo de mantener segura la información del dispositivo ante la pérdida o robo. De acuerdo a pruebas realizadas por los autores del documento, se puede observar los intentos de bloqueos de la pantalla además de controlar los intentos en la siguiente tabla.

Numero de intentos	Resultado
1-5	Al usuario le pide ingresar la contraseña
5-9	Al usuario le pide ingresar la contraseña.
10	El usuario depende de la función del administrador. El administrador puede reiniciar un nuevo PIN, llamar al dispositivo, bloquear remotamente el dispositivo, ubicar el dispositivo en Google Maps, limpiar el dispositivo o eliminar la cuenta empresarial automáticamente.

Tabla 6: Intentos de desbloqueo de pantalla.

3.2. Prueba número dos, eliminación de una cuenta empresarial.

Cuando un dispositivo se ha extraviado o robado dentro de CREASOFT ECUADOR, es un escenario común para que se establezca, que existe un gran riesgo de acceso físico no autorizado; como parámetro adicional, el delincuente toma la medida de desactivar la conexión de datos móviles y el retiro de la tarjeta SIM.

Aunque la solución, elimine los datos del dispositivo y lo restaure a valores de fábrica, es necesario aclarar que los datos estarán disponibles iniciando sesión a través de un navegador. En la siguiente figura se puede observar el mensaje de advertencia para eliminar la cuenta.

Figura 3.1: Mensaje de Advertencia al eliminar cuenta

De comprobarse que el teléfono se ha extraviado se puede optar la opción de borrado parcial. En la siguiente figura se puede observar el mensaje de advertencia para la eliminación remota de la cuenta especificando el modelo del dispositivo, el sistema operativo y el nombre del propietario de la cuenta.

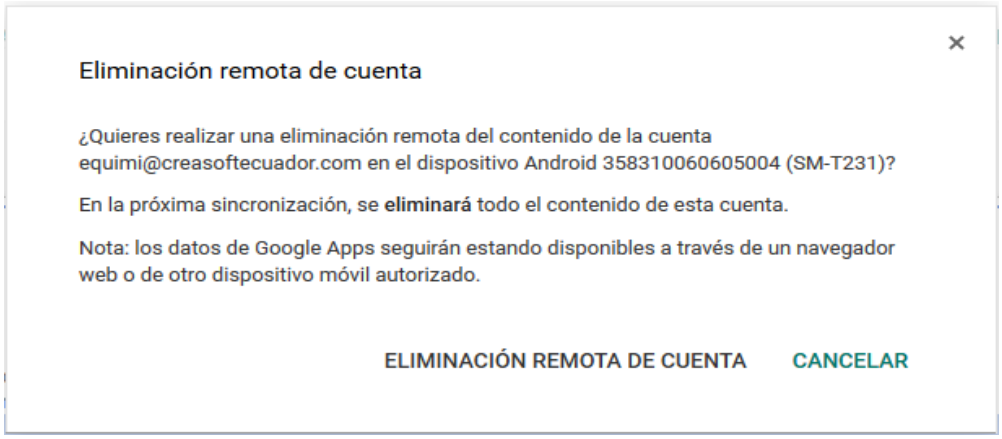

Figura 3.1: Mensaje de Advertencia borrado parcial.

Las políticas aplicadas por el administrador de CREASOFT ECUADOR establecen, que en caso de robo se debe borrar totalmente la información del dispositivo, dejándolo como un dispositivo de fábrica; y, en caso de extraviar el dispositivo se puede optar por un borrado parcial o el borrado total. En la siguiente figura se puede observar, en el estado de los dispositivos administrados se ha eliminado la cuenta de forma remota al usuario equimi@creasoftecuador.com, en el teléfono con modelo SM-T231.

Correo	Modelo	SO	Tipo	Última sincronización	Estado
equimi@creasoftecuador.com	SM-T231	Android 4.4.2	Android	16/1/16	Eliminación remota de la cuenta
verrodri@creasoftecuador.com	Windows Phone 8	Windows Phone 8	Google Sync	15/1/16	Aprobado

Figura 3.2: Lista de Dispositivos Administrados

3.3. Prueba número tres, instalación de apps no aprobados.

Es usual, que los dueños de los dispositivos instalen aplicaciones, sin observar los tipos de permisos que se aceptan sin leerlas primero. En la siguiente figura se puede observar el intento de instalar aplicaciones como Youtube y Cisco Packet Tracer Movile dando como resultado, un mensaje informativo que indica que el administrador de CREASOFT ECUADOR no ha concedido acceso a este elemento en el perfil empresarial.

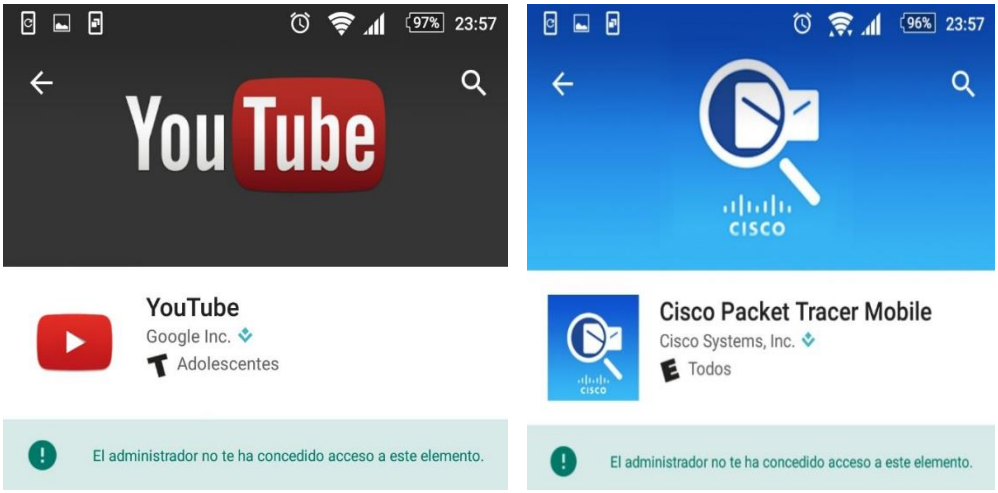

Figura 3.3: Aplicaciones no autorizadas.

3.4. Prueba número cuatro, separación de aplicaciones a través de Perfiles de Trabajo

Como escenario, el administrador permite la instalación de Evernote pero en el dispositivo ya tiene instalado una versión. En la siguiente figura se puede observar que obtiene una aplicación de forma personal y la segunda de modo empresarial, se diferencia porque posee el logo de Google Apps for Work.

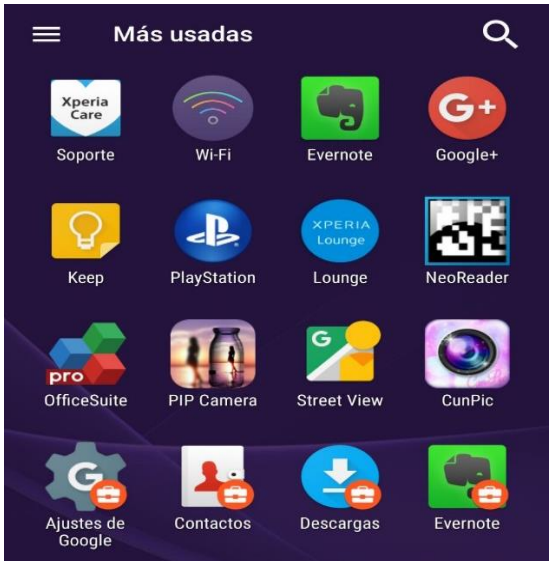

Figura 3.4: Vista de Aplicaciones

3.5. Prueba número cinco, registro no autorizado de dispositivos, acceso de credenciales por ingeniería social.

El atacante obtuvo las credenciales de un usuario del dominio de CREASOFT ECUADOR e intenta registrar su dispositivo para tener acceso a la plataforma y así tener información empresarial, en la siguiente figura se puede observar que el administrador gestiona el acceso, deja pendiente o bloquea el acceso porque no forma parte de los dispositivos de la empresa.

Figura 3.5: Dispositivo Pendiente de aprobación

Se da a conocer al administrador las características del dispositivo, que sirve para tomar la decisión de aprobar o no el equipo. A continuación en la figura se muestra el modelo, el tipo de cuenta, Dirección Mac del Wifi entre otras opciones.

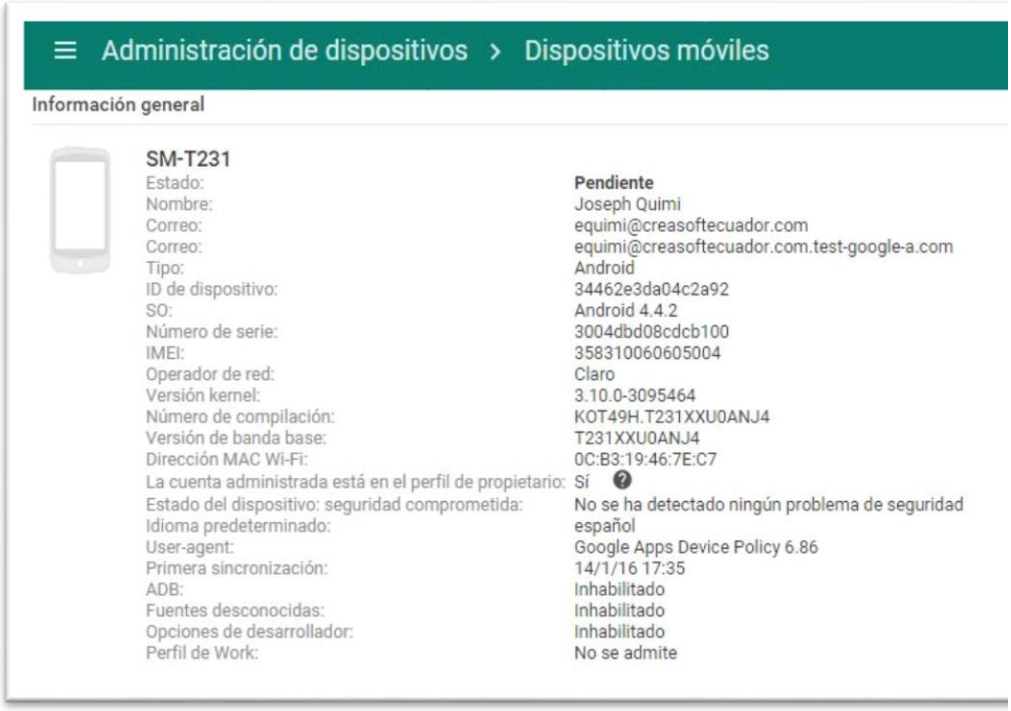

Figura 3.6: Características del dispositivo

En la siguiente figura se puede observar que los dispositivos que intenten acceder a la plataforma, son gestionados por las políticas locales de la aplicación y no globales de la solución, por lo tanto el registro está en manos del administrador de CREASOFT ECUADOR.

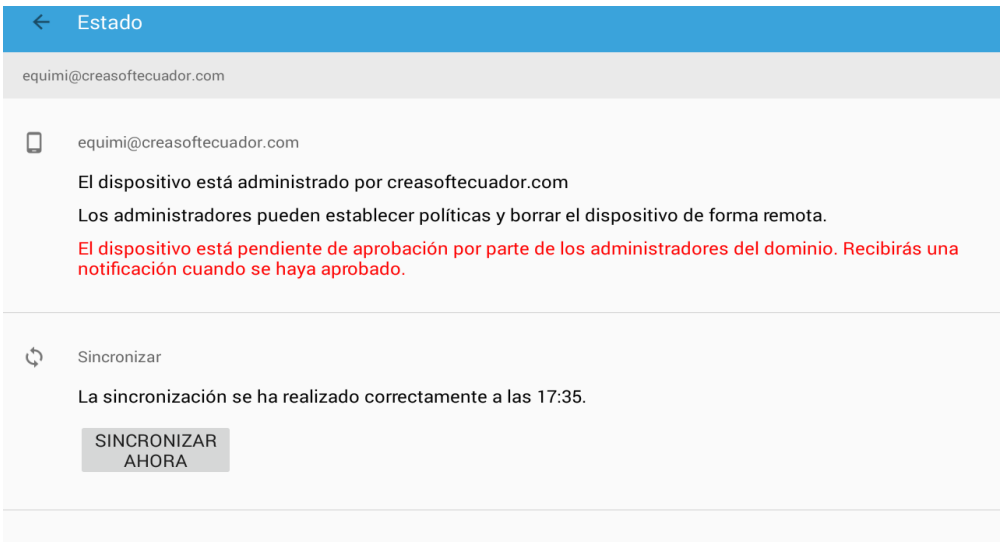

Figura 3.7: Mensaje de advertencia

Mediante el informe de inicio de sesión, se puede establecer qué usuarios han realizado un ingreso exitoso o han solicitado una verificación de cuentas, por lo tanto se considera que es una herramienta útil para detección de acceso no autorizado. En la siguiente figura se puede observar el registro de los inicios de sesión de varios usuarios.

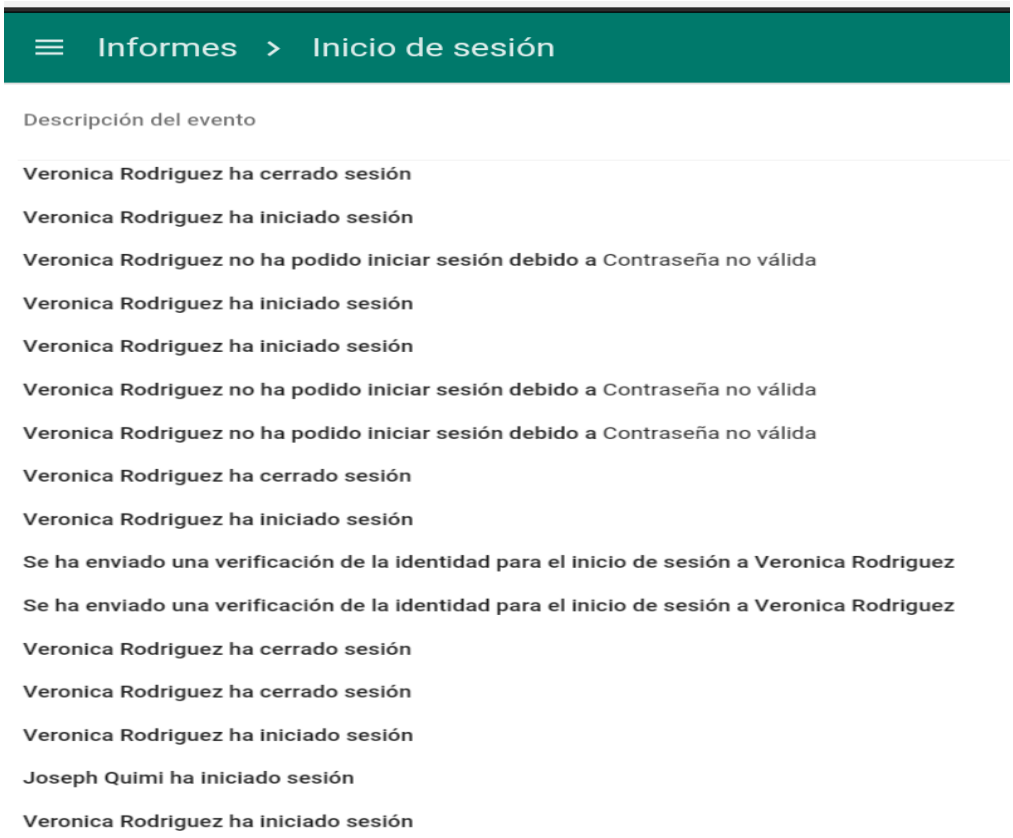

Figura 3.8: Registro de sesión de los usuarios

3.6. Prueba número seis, auditoría de informes.

Como medida de seguridad el administrador de CREASOFT ECUADOR, puede revisar qué usuarios han tenido acceso a los documentos y credenciales de acceso a servicios; ayudando a la detección de intrusos.

En la siguiente figura se obtiene una vista general de los documentos, que se encuentra en el dominio del usuario Joseph Quimí, divididos en varios tipos de documentos.

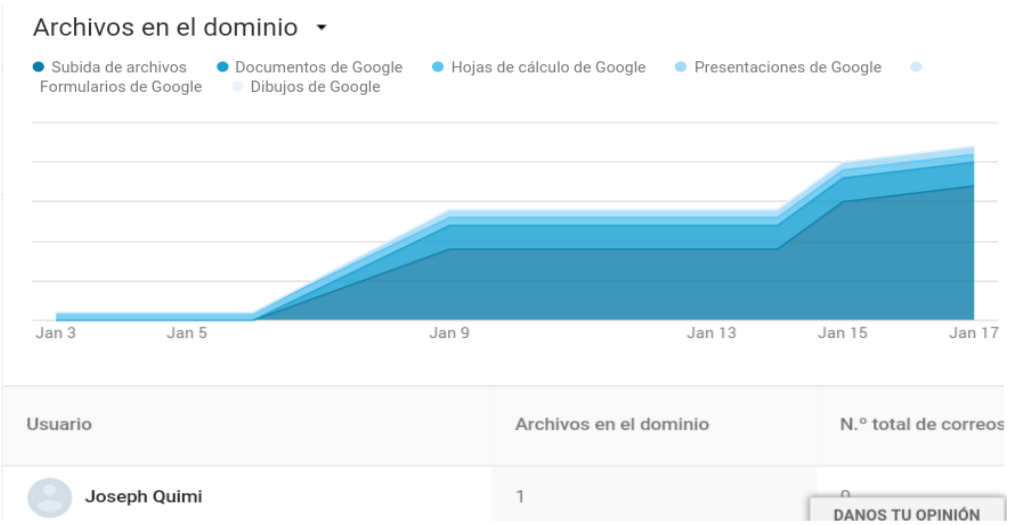

Figura 3.9: Archivos del usuario

Se observa, que no existen documentos que hayan sido revisados, por usuarios externos. En la siguiente figura se muestra los archivos visibles públicamente, compartidos fuera del dominio o visibles para los usuarios con un enlace.

Figura 3.10: Archivos visibles externamente

El usuario tiene acceso a 21 documentos que le pertenecen, ninguna persona no propietaria puede revisarlos y viceversa, al menos que compartan los archivos. En la siguiente figura se puede observar los archivos visibles internamente con usuarios del dominio, compartidos con otros usuarios a través de un enlace, además de los archivos que se mantienen privados.

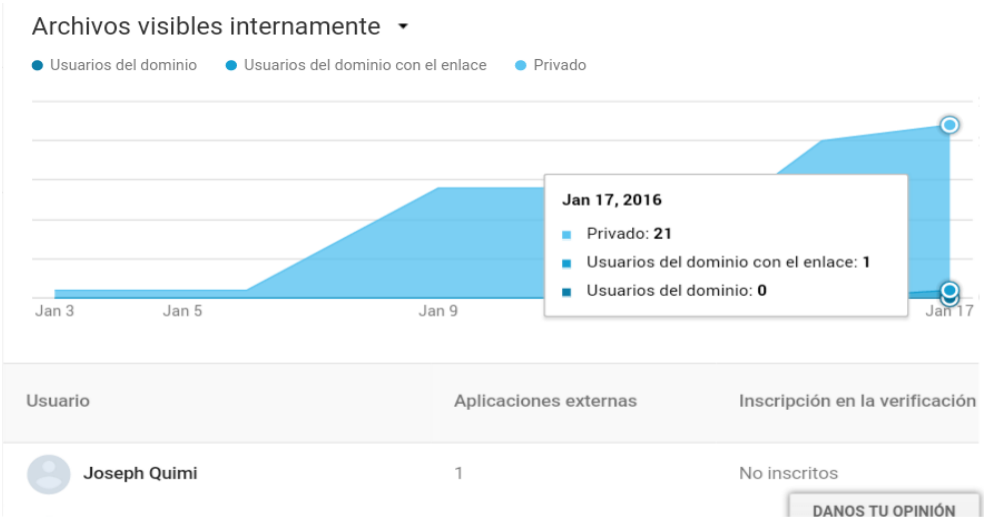

Figura 3.11: Archivos visibles internamente

3.7. Prueba número siete, protección contra la manipulación de la información transmitida:

Un atacante ha podido acceder a datos de la empresa a través de un dispositivo de un trabajador de CREASOFT ECUADOR, se tiene como objetivo cambiar políticas y servicios, tener acceso a documentos. Con la separación de funciones, el atacante exclusivamente tiene acceso a la cuenta del usuario, adicionalmente los perfiles de trabajo ayudan a la seguridad de accesos no autorizados, separando la información del usuario con los del trabajo. En la siguiente figura se puede observar los eventos, cambios de configuraciones y políticas aplicadas en los dispositivos.

Nombre del evento	Descripción del evento
Cambio en la configuración para móviles	La configuración DISABLE_UNKNOWN_SOURCES para los dispositivos móviles de creasoftecuador.com ha cambiado de false a true (Nombre de unidad organizativa: {creasoftecuador.com})
Cambio del estado de la alerta	El estado de la alerta para CHANGE_MOBILE_SETTING ha cambiado de off a on
Cambio del estado de la alerta	El estado de la alerta para TLS_FAILURE ha cambiado d off a on
Cambio del estado de la alerta	El estado de la alerta para CHANGE_DOCS_SETTING ha cambiado de off a on
Asignación de función	Se ha asignado la función _PLAY_FOR_WORK_ADMIN_ROLE al usuario verrodri@creasoftecuador.com
Aprobación de dispositivo móvil	Se ha aprobado el dispositivo móvil para verrodri@creasoftecuador.com (Tipo de dispositivo: {MOBILE_DEVICE_TYPE_ANDROID}, ID del dispositivo: {3fbc6890f1acf14e})
Autorización del acceso de cliente API	El acceso de cliente API a creasoftecuador.com desde cliente 1022526378366-llr2nj3275j65m2m9m9qft1vf4ebp1sf.apps.googleuserc (AppSheet) se ha autorizado para los ámbitos https://www.googleapis.com/auth/userinfo.email, https://www.googleapis.com/auth/userinfo.profile, https://www.googleapis.com/auth/documents, https://www.googleapis.com/auth/script.external_requ https://www.googleapis.com/auth/script.scriptapp, https://www.googleapis.com/auth/script.storage, https://www.googleapis.com/auth/spreadsheets
Añadir aplicación	La aplicación AppSheet con el ID - se ha añadido al dominio (ID de la aplicación: {1022526378366})
Autorización del acceso de cliente API	El acceso de cliente API a creasoftecuador.com desde cliente 540469545181-ogj554ch6adb2pfe9i7kef9etljavvul.apps.googleusercor (Google Apps Tips) se ha autorizado para los ámbitos https://www.googleapis.com/auth/userinfo.email, https://www.googleapis.com/auth/userinfo.profile
Añadir aplicación	La aplicación Google Apps Tips con el ID - se ha añadid al dominio (ID de la aplicación: {540469545181})
Autorización del acceso de cliente API	El acceso de cliente API a creasoftecuador.com desde cliente 629453589428-36immin380b5uf4uchds98kmc2l7t57l.apps.googleuser (Google Apps Script) se ha autorizado para los ámbitos

Figura 3.12: Registro de eventos

3.8. Prueba número ocho, inicio de sesión sospechoso

En algunos casos, cuando se detecta inicio de sesión sospechoso el administrador de CREASOFT ECUADOR, tiene la opción de proporcionar a los usuarios un código de seguridad para poder verificar sus credenciales. En la siguiente figura se puede observar el código de seguridad generado en un dispositivo con sistema operativo Android.

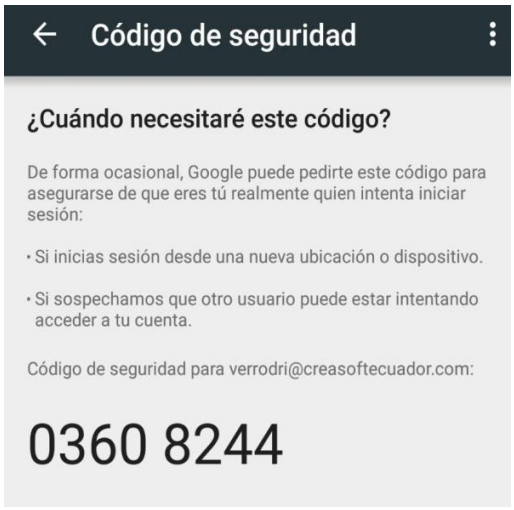

Figura 3.13: Código de seguridad en Android

Adicionalmente, el Administrador puede configurar la solución para que se envíe un correo electrónico, para confirmar que un usuario este iniciando sesión en un dispositivo nuevo. En la siguiente figura se puede observar un correo de reconocimiento, es decir la confirmación de inicio de sesión del usuario verrodri en un teléfono Sony Experia Z1.

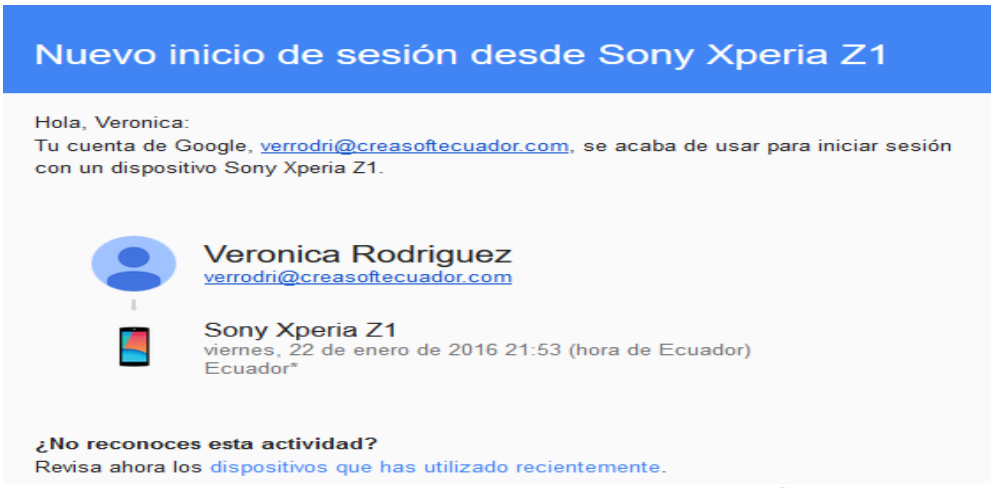

Figura 3.14: Mail de nuevo inicio de sesión

Y existe una opción para proteger la cuenta, si no reconoce el dispositivo, el usuario puede proteger su sesión en el dispositivo como se muestra en la siguiente figura.

Figura 3.15: Acceso en nuevo dispositivo

En caso de que se considere necesario el administrador de CREASOFT ECUADOR, comprueba los últimos eventos de seguridad de la cuenta como en la siguiente figura que se muestra el cambio de PIN o el de correo electrónico.

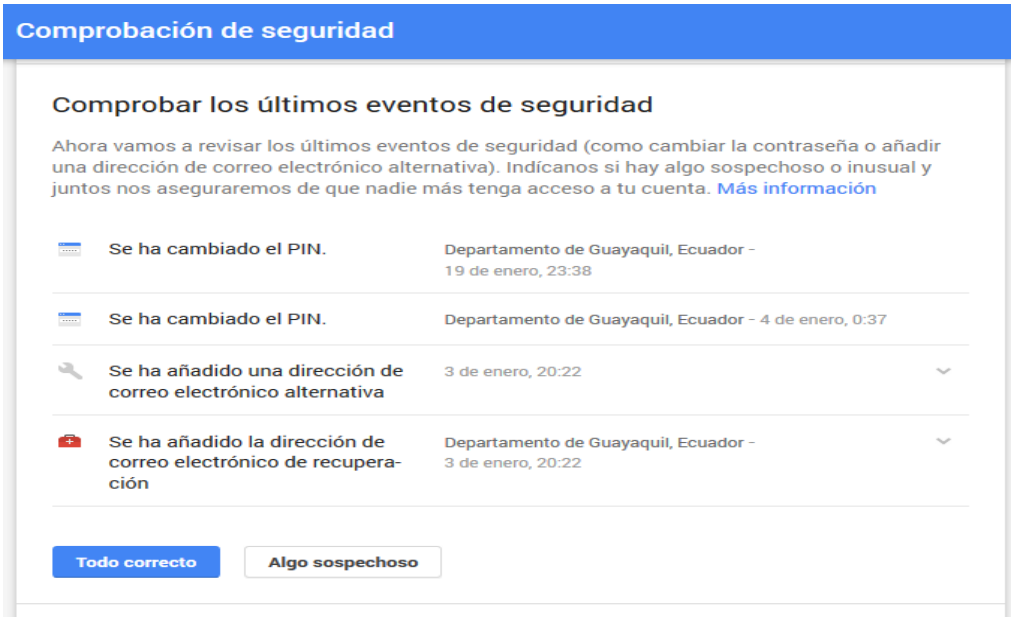

Figura 3.16: Comprobación de seguridad inicial del dispositivo

El administrador, comprueba la lista de los dispositivos conectados, con la cuenta de usuario propietaria como se observa en la siguiente figura.

Figura 3.17: Dispositivos Gestionados

Comprobar los permisos de las aplicaciones, los sitios web, las aplicaciones y los dispositivos para proteger la cuenta propietaria como se muestra en la siguiente figura.

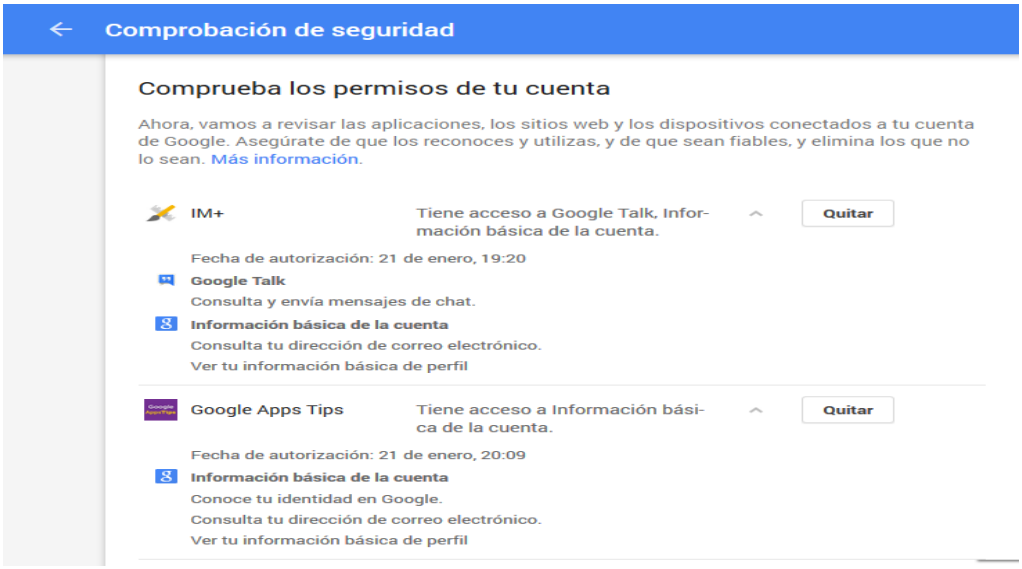

Figura 3.18 Comprobación de seguridad de aplicaciones en el dispositivo

3.9. Prueba número nueve, transferencia de datos de un usuario a una nueva cuenta

El administrador crea una solicitud de Verónica Rodríguez (verrodri@creasoftecuador.com) para eliminar al usuario Wendy Merejildo (wendym@creasoftecuador.com) por que la empresa renovó el personal y decide delegar la responsabilidad, entonces procede a transferir sus datos a otro usuario delegado en esta ocasión es Joseph Quimí (equimi@creasoftecuador.com). En la siguiente figura se muestra la información de la solicitud que se enviara.

Figura 3.19: Transferencia de cuenta

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

1. En la organización se produjo un cambio cultural, aumentando el compromiso y la productividad de los empleados. Ahora son capaces de acceder a los archivos sin utilizar un servicio de VPN o utilizarlo de una forma más eficiente, adjuntar archivos a los mensajes de correo electrónico de forma remota y unirse a reuniones sin estar físicamente presente, esencialmente trabajar sin fronteras.
2. En CREASOFT ECUADOR**,** se presenció un cambio de política con la que se solicitó a los administradores y personal del área de sistemas entrenar y evaluar a los empleados, a través del uso de la videoconferencia en lugar de la reunión presencial. Lo que permitió reducir los viajes de gestión y logística. La organización tenía designada a 2 personas, que realizaban 2 viajes al mes a 2 lugares diferentes; como parte del trabajo, se estima una disminución de 6 viajes al mes. Un viaje promedio cuesta $ 60, la organización ahorró $ 360 dólares por mes.
3. Se obtuvo una ventaja para CREASOFT ECUADOR: la colaboración en tiempo real, el control de versiones y la capacidad de ahorro de tiempo. Con Google Apps, los procesos que antes requerían de una semana de duración al empleado, por utilizar con el correo electrónico para enviar sus diapositivas a un contacto, ahora sólo necesitan minutos para lograrlo, debido a que la consolidación en tiempo real puede tener lugar. Google Hangouts y Docs, en reunión sesiones de colaboración se han vuelto más comunes dentro de la organización.
4. La comunicación y la colaboración basada en la nube, ha permitido a la organización desmantelar sus servidores del correo electrónico y el almacenamiento, por el ahorro en mantenimiento y soporte. Además, el medio basado en la nube permite a los empleados acceder a la perfección: documentos, correos electrónicos y otros archivos en los teléfonos inteligentes, tabletas o computadoras portátiles.

5. Los servicios que brinda Google Apps For Work, desde la implementación están activos y se usan para acceder a las funciones EMM (Enterprise Mobile Managment, gestión de movilidad empresarial) de la consola de administración, haciendo más eficiente la comunicación entre los empleados de la empresa.
6. El aumento de la colaboración y la eficiencia: El colaborar en tiempo real a través de la ofimática de Google, así como poder desarrollar espacios de colaboración de proyectos en Google Sites, permite a los empleados agilizar los procesos en los negocios y colaborar de manera más efectiva. Esto se traduce en un ahorro medio de tiempo de 15 minutos a 2 horas por semana, por empleado.
7. Tras la implementación de Google Apps para el Trabajo, se da referencia de la existencia de 32,5 horas por semana de eficiencia por parte de los empleados de CREASOFT ECUADOR. La tasa de adopción, o la velocidad a la que los empleados incorporan el uso de Google Apps en su forma de trabajar, fue de 60% en el mes 1, con un crecimiento del 100% en el mes 3. Como resultado, se obtuvo que la organización se ahorró en 3 meses 390 horas.

Recomendaciones.

1. Utilizar la opción de prueba gratuita de Google Apps es de 30 días, con la que se debe aprovechar la facilidad de crear más de 10 usuarios.
2. Configurar el firewall para acceder a los sitios, de lo contrario los usuarios serán bloqueados.
3. Registrar los datos para la facturación y así evitar el corte del servicio.
4. En los dispositivos con sistemas operativos Windows Phone, se debe evitar utilizar POP e IMAP en la configuración del correo electrónico, porque no es compatible. Se debe recurrir a Google Sync que admite enviar correo, es una característica que aprueba la utilización de una dirección de correo empresarial.

5. En el uso de Microsoft Office, se detectaron algunos problemas al trabajar con los formatos de archivo, en los documentos básicos, hojas de cálculo y presentaciones, sin embargo, no existen problemas que aporten excesivos inconvenientes.
6. Recordar que sólo hay soporte para dispositivos Android 5.0 en la utilización de Google Apps For Work.
7. Con teléfonos sin conexión móvil o sin tarjeta SIM, es imposible sincronizar.
8. En lo posible se debe limitar el uso de tamaño de documentos adjunto en el correo electrónico, dado que si se sobrepasa se bloqueará la cuenta.
9. Algunas políticas en los teléfonos son desplegadas en un lapso de 24 horas, se recomienda que estas se realicen los fines de semana.
10. Versión de Windows Server 2008 en adelante (AD DS), Windows Server Core no son compatibles.
11. GAPS debe estar instalado en todos los controladores de dominio.
12. Los controladores de dominio requieren de una conexión a Internet para acceder a los sitios web.

BIBLIOGRAFÍA

[1] J. Curtis. (2012, Noviembre 23). Bring Your Own Device (BYOD) [Online]. Disponible en: https://www.jisc.ac.uk/blog/bring-your-own-device-byod-23-nov-2012

[2] V. M. Rodríguez, J. E. Quimí, "Sistemas operativos usados", Creasoft Ecuador., Guayaquil, Ecuador, Rep., Dic. 2015.

[3] B. Shimmin. (2015, Febrero 26). Google's New "Android for Work" Program Actually Puts BYOD to Work [Online]. Disponible en: http://itcblogs.currentanalysis.com/2015/02/26/googles-new-android-for-work-program-actually-puts-byod-to-work/

[4] Google (2016, Enero 1). Acerca de la aplicación Política de dispositivos para Android [Online]. Disponible en: https://support.google.com/a/users/answer/

[5] Google (2016, Enero 1). Configurar dispositivos a través de Android for Work en dispositivos con Android 5.0 y versiones superiores [Online]. Disponible en: https://support.google.com/a/users/answer/6178111?hl=es&ref_topic=2365092

[6] CSDN (2015, Agosto 25), Google Message para Android (GCM nube push) [Online]. Disponible en: http://www.xuebuyuan.com/2230997.html

[7] Google (2016, Enero 1). Administrar dispositivos iOS. [Online]. Disponible en: https://support.google.com/a/answer/6080045?hl=es&ref_topic=1734198

[8] Exchange (2015, marzo 9) Directivas de buzones de correo para dispositivos móviles compatibles con teléfonos y dispositivos de Windows [Online]. Disponible en: https://technet.microsoft.com/es-es/library/jj983805(v=exchg.150).aspx

[9] Office (2016, enero 31). Configurar correo en Windows Phone. Cuentas de correo electrónico profesionales o educativas que usan Office 365 u otras cuentas de correo electrónico basado en Exchange [Online]. Disponible en:

https://support.office.com/es-es/article/Configurar-el-correo-en-Windows-Phone-181a112a-be92-49ca-ade5-399264b3d417?ui=es-ES&rs=es-ES&ad=ES#BKMK_O365Exchange

[10] Google (2015, enero 25) Comparar los planes de facturación de Google Apps for Work [Online]. Disponible en: https://support.google.com/a/answer/1247360?hl=es&ref_topic=6142432

[11] Ayuda de Administrador de Google Apps (2015, enero 25) Cómo ponerse en contacto con el equipo de asistencia de Google Apps [Online]. Disponible en: https://support.google.com/a/answer/1047213?hl=es

[12] Ayuda de Administrador de Google Apps (2014, enero 1) Como añadir tu logotipo [Online]. Disponible en: https://support.google.com/a/answer/96474?hl=es

[13] Google (2015, diciembre 9). Registro de auditoria de la Consola de administración [Online]. Disponible en: https://support.google.com/a/answer/4579579?hl=es

[14] Cómo conceder privilegios de administrador (2015, diciembre 14) Definiciones de los privilegios de administrador [Online]. Disponible en: https://support.google.com/a/answer/1219251?hl=es

[15] Sincronizar los datos de los usuarios con Google Apps Directory Sync (2015, diciembre 1) Preparar los datos y el servidor de directorios LDAP [Online]. Disponible en: https://support.google.com/a/answer/6124427?hl=es&ref_topic=6121003

[16] Google (2015, Agosto 19) Politicas de privacidad [Online]. Disponible en: https://privacy.google.com/?hl=es

[17] Ayuda de Administrador de Google Apps (2015, diciembre 23) Registros e informes de la consola de Administración [Online]. Disponible en: https://support.google.com/a/answer/4589321

[18] Administradores de Google (2015, diciembre 23) Google Apps for Work en dispositivos Android [Online]. Disponible en: https://support.google.com/a/answer/1228371?hl=es

[19] J. Areitio (2011, noviembre). Analisis de los riesgos y contramedidas en seguridad-privacidad de la tecnología NFC en móviles [Online]. Disponible en: http://www.redeweb.com/_txt/684/42.pdf

[20] T. Berger “Conferencia análisis de las tecnologías actuales de VPN” en La disponibilidad, fiabilidad y seguridad” Austria (2006 abril 20-22)

[21] VYPRVPN (2016, enero 14) Comparación de protocolos de VPN [Online]. Disponible en: https://www.goldenfrog.com/ES/vyprvpn/features/vpn-protocols

[22] Google (2016, enero 20). Límites de ancho de banda [Online]. Disponible en: https://support.google.com/a/answer/1071518?hl=es

[23] Google (2015, diciembre 11). Cómo funciona GADS [Online]. Disponible en: https://support.google.com/a/answer/6118539?hl=es&ref_topic=4497998

[24] Google (2015, diciembre 9). ¿Qué es Google Sync? [Online]. Disponible en: https://support.google.com/a/answer/135937?hl=es

[25] Google (2015, diciembre 1). Plan flexible. Cómo se calculan los pagos. [Online]. Disponible en: https://support.google.com/a/answer/1247362?hl=es&ref_topic=6142432

[26] Google (2015, diciembre 1). Plan anual. Cómo se calculan los pagos [Online]. Disponible en: https://support.google.com/a/answer/1247364

[27] Google (2015, diciembre 17). ¿Qué servicio quieres activar o desactivar para los usuarios? [Online]. Disponible en: https://support.google.com/a/answer/182442?hl=es

[28] Google (2015, diciembre 11). Implementar la Política de dispositivos de Google Apps en tu organización [Online]. Disponible en: https://support.google.com/a/answer/1056433?hl=es&ref_topic=1734198

[29] Google (2015, diciembre 11). Configurar y usar la aplicación Política de dispositivos para iOS [Online]. Disponible en: https://support.google.com/a/answer/3521320?hl=es&ref_topic=6079327

[30] Google (2015, Diciembre 9). Como configurar registros MX. (Pasos específicos del host) [Online]. Disponible en: https://support.google.com/a/answer/54717?hl=es-419&ref_topic=4445219

ANEXOS

ANEXO A. MANUAL DE USUARIO

Configuración inicial de Google Apps For Work

Paso 1. Configure la cuenta para la empresa CREASOFT ECUADOR, digite la dirección web https://apps.google.es/ y dé a clic en el botón empieza aquí

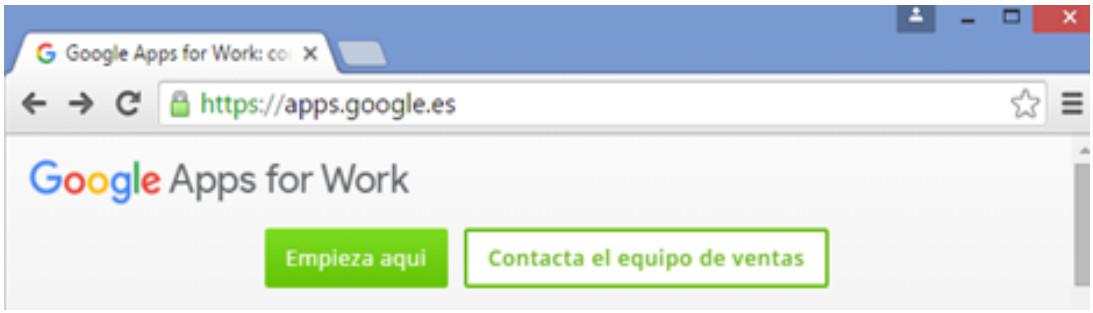

Figura A.1: Página de acceso principal a la solución.

Paso 2. Ingrese los datos personales, del administrador de la solución.

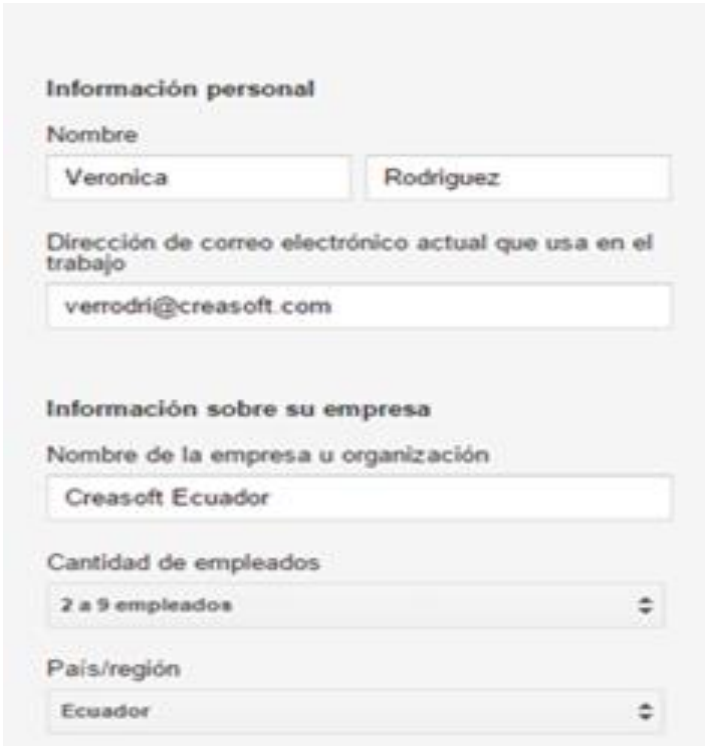

Figura A.2: Formulario Información personal.

Paso 3. Ingrese los datos del dominio creasoftecuador.com

Figura A.3: Información de dominio de la empresa.

Paso 4. Establezca los datos de la cuenta, crea una contraseña para el ingreso a la consola de administración, dé clic en el botón aceptar y regístrese.

Figura A.4: Formulario de creación de cuenta administrador.

Paso 5. En los pasos anteriores ya se configuró una cuenta para CREASOFT ECUADOR, la segunda opción es Añadir personas a la cuenta de google de click en el botón empezar.

Figura A.5: Configuración de la solución.

Paso 6. Añada otra cuenta que va a utilizar un administrador secundario, dé (a) clic en Añadir para agregar la cuenta.

Figura A.6: Formulario para añadir usuarios.

Paso 7. Verifique el dominio creasoftecuador.com,es propietario del usuario verrodri, por seguridad e integridad de la información empresarial, dé clic en el botón Verificar.

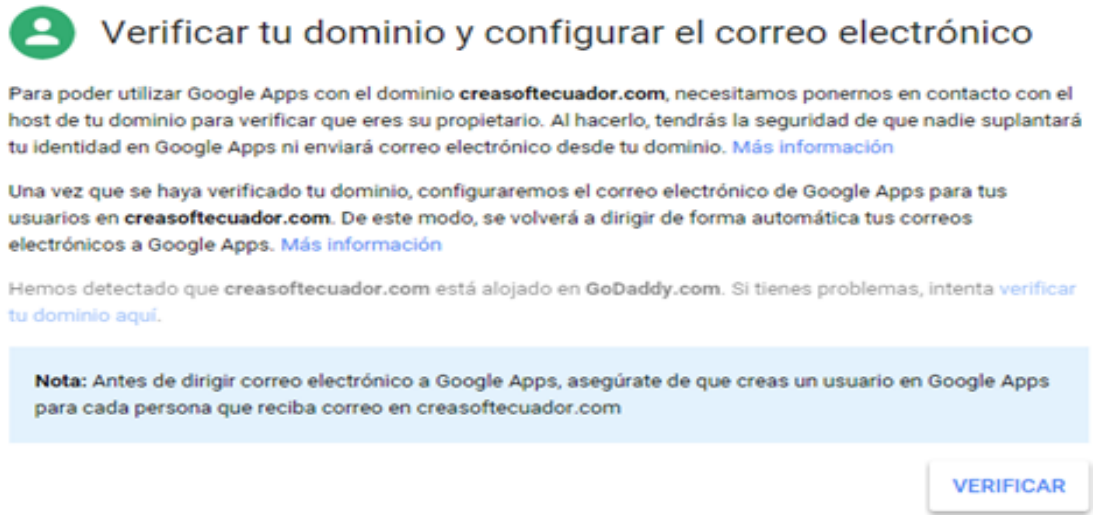

Figura A.7: Verificar el dominio.

Paso 8. Si el dominio pertenece a un partner de google inicié la pestaña automáticamente, ingrese los datos de usuario, contraseña, da clic en Inicio de sesión seguro. Caso contrario verifique a través de credenciales, en la pestaña Setup para iniciar la verificación en Welcome –Verify domain membership y dé clic en siguiente.

Figura A.8: Verificación de dominio entre Google y GoDaddy.

Paso 9. Confirme el acceso del DNS Servidor de nombre de dominio creasoftecuador.com, a la solución. Dé clic en aceptar.

Figura A.9: Solicitud de permiso de acceso al DNS en GoDaddy.

Paso 10. Verificar el dominio creasoftecuador.com da clic en el botón Empezar.

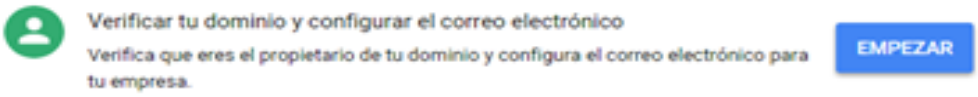

Figura A.10: Verificación de dominio para Configuración correo.

Paso 11. Espere un minuto para la verificación entre ellos, dominio y correo electrónico.

Figura A.11: Verificación de la dirección de correo.

Paso 12. Concluya con éxito la verificación, dé clic en siguiente y finalice.

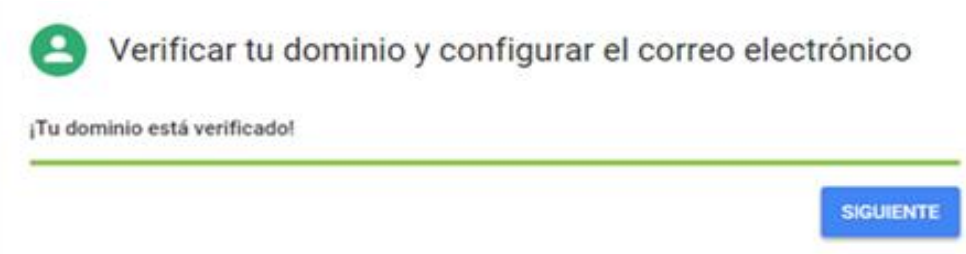

Figura A.12. Verificación de correo final.

MANUAL DE USUARIO: Administración de Google Apps For Work desde la Consola de administración.

La consola de administración cuenta con opciones necesarias para ingreso de cuentas, análisis y pruebas que brinda la solución, a continuación, se despliega cada opción.

Paso 1. Ingrese con las credenciales de administrador en la dirección https://admin.google.com/AdminHome?hl=es&pli=1&fral=1, en la parte superior derecha despliegue las opciones y dé clic en Administración

Figura A.13: Consola de administración principal.

Paso 2. En la consola de administración dé clic en el Perfil empresa, personalice el nombre de la empresa a CREASOFT ECUADOR, personalice el logo, personalice la dirección web de acceso, para mayor comodidad de los usuarios administradores, ingrese la dirección de correo que administra la cuenta principal de la empresa, dirección de correo alternativa que sirve para restablecer la contraseña.

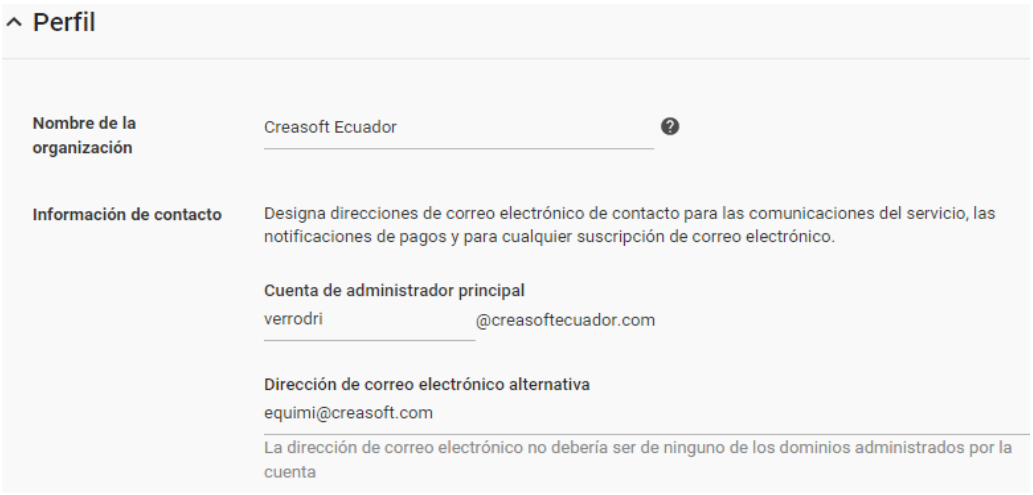

Figura A.14: Formulario de perfil de la organización.

Paso 3. En la parte superior izquierda despliegue las distintas opciones como se muestra en la figura.

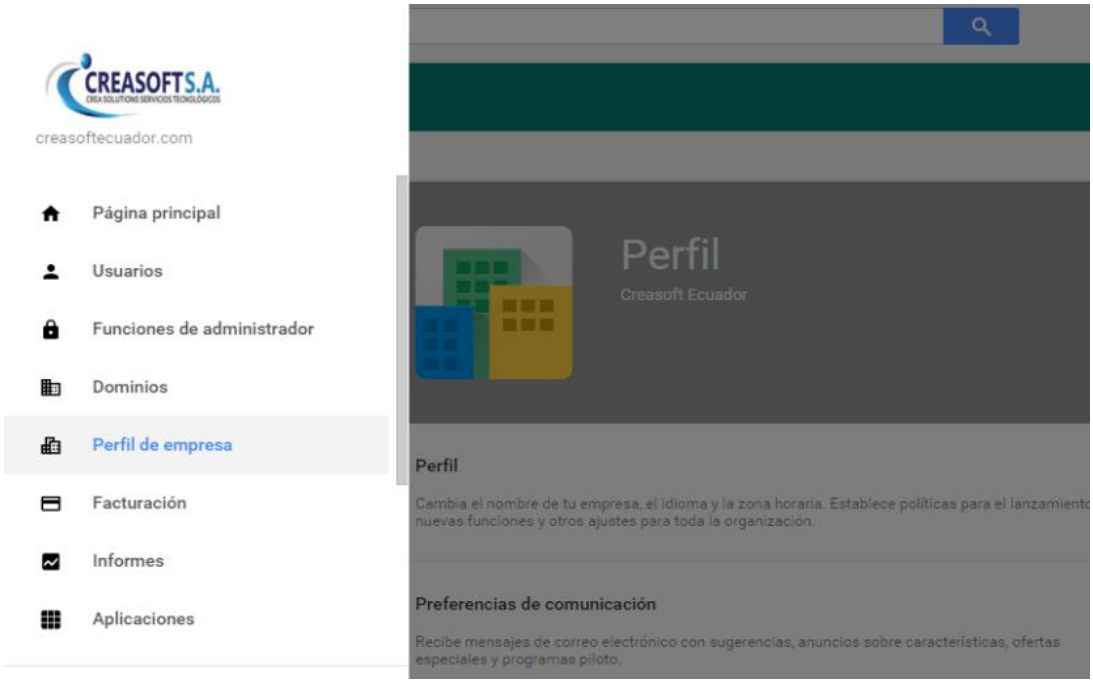

Figura A.15: Menú de acceso directo a la consola.

Paso 4. Usuarios. Ingrese usuarios de manera individual o colectiva, invite a usuarios, a unirse a la plataforma, muestre los usuarios registrados. Cuenta con:

filtro por tipo de usuarios por organización, usuarios activos, usuarios invitados, usuarios suspendidos y usuario con transferencia de datos.

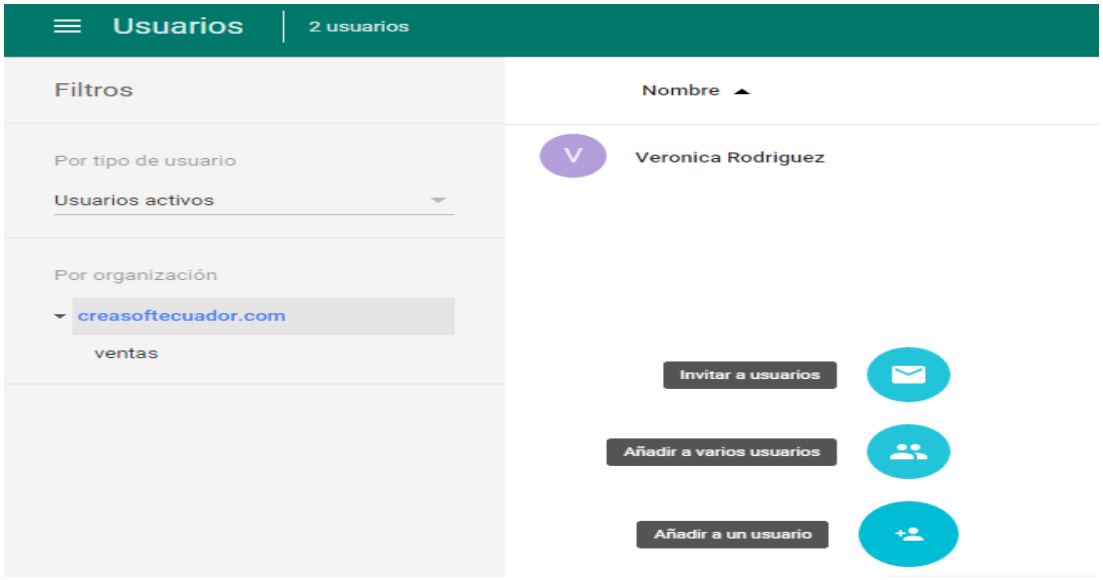

Figura A.16: Opciones de usuario.

Paso 5. Funciones de administrador. El superadministrador asigna funciones y privilegios a los administradores, adicionalmente permite crear nuevas funciones con privilegios personalizados, se ubicarán en la sección Funciones creadas por usuarios.

Figura A.17: Funciones de administrador.

Paso 6 Aplicaciones. Contiene el paquete Google Apps, son 9 aplicaciones por defecto, servicios Móvil Sync para la sincronización de los dispositivos móviles, además de Sitios Web para crear y compartir, servicios adicionales para almacenar fotos, videos, administra aplicaciones de terceros, aplicaciones SAML para que los usuarios con las credenciales de Google Apps inicien sesión en aplicaciones empresariales almacenadas en la nube.

Figura A.18: Aplicaciones y servicios adicionales de google.

Paso 7. En el botón superior izquierdo escoge Informes, permite analizar las actividades de toda la organización y visualizar e importar informes. Se encarga de auditar las actividades en la solución, mantiene el registro guardado de los cambios que se ejecutan, descripción del evento, usuario, dirección IP y fecha.

Figura A.19: Informes disponibles.

Paso 8. Administración de dispositivos, concede permisos de acceso mediante la red, administra dispositivos móviles y los dispositivos que utilizan Chrome.

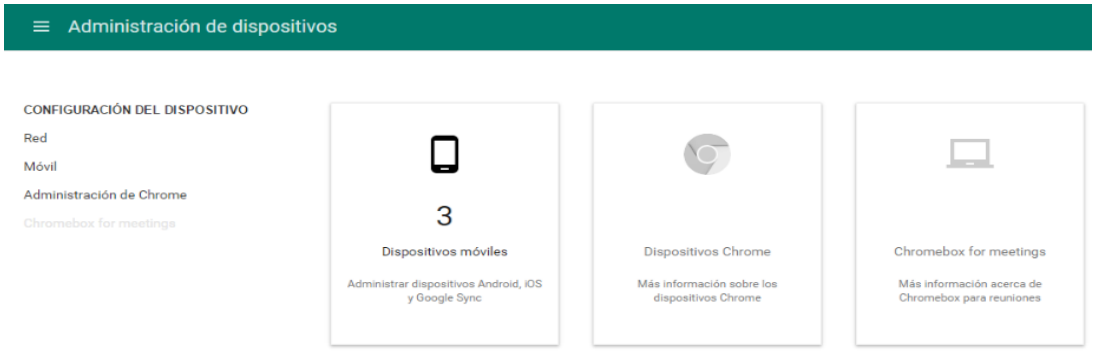

Figura A.20: Administración de dispositivos.

Paso 9. Seguridad, proporciona medidas que rigen a los usuarios móviles, Puede escoger la verificación en dos pasos, ingresa un código de verificación e ingresa usuario y contraseña.

Figura A.21: Seguridad de la solución.

Control de las contraseñas de un usuario, puedes asignar políticas de longitud de contraseña.

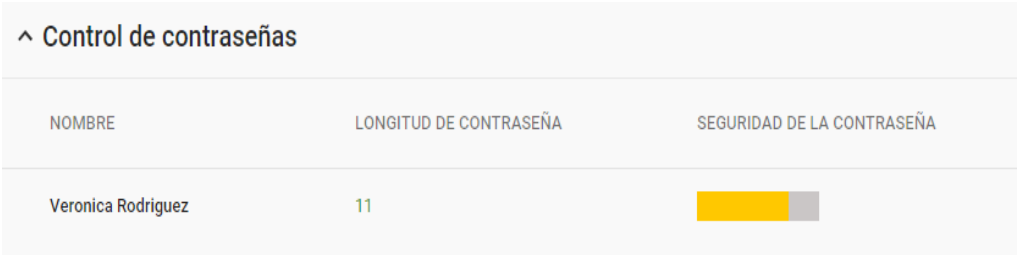

Figura A.22: Seguridad del usuario en la contraseña.

Nota. Detalle de cláusulas del contrato, políticas de privacidad, los accesos a los centros de datos físicos que son 24 horas del día los 7 días a la semana, sitios de controles, seguridad personal, de red y de datos.

MANUAL DE USUARIO: Configuración de Funciones del administrador

Paso 1. Escoger funciones del sistema, el superadministrador de CREASOFT ECUADOR permite gestionar los dispositivos en forma global incluyendo todos los niveles.

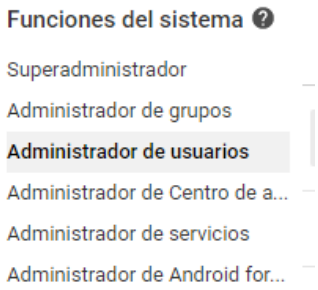

Figura A.23: Funciones del administrador del sistema.

Paso 2. Agregar nuevo administrador presionando el botón asignar administradores

Figura A.24: Configuración de administrador.

Paso 3. Agregar privilegios para administradores, crear unidades organizativas, usuarios.

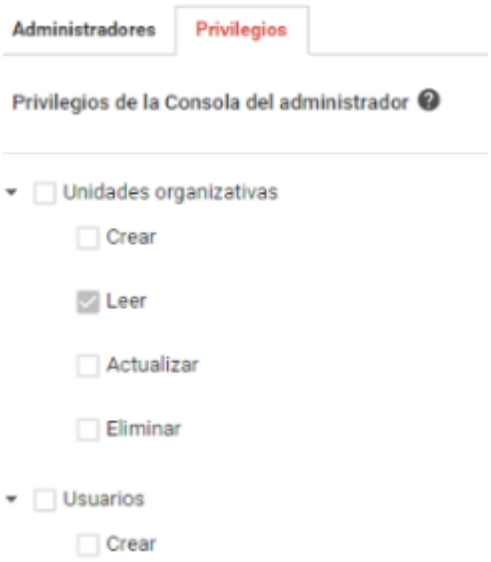

Figura A.25: Privilegios disponibles de la solución.

Paso 4. Funciones creadas por usuarios, permite crear nuevas funciones personalizadas como se muestra en la siguiente figura.

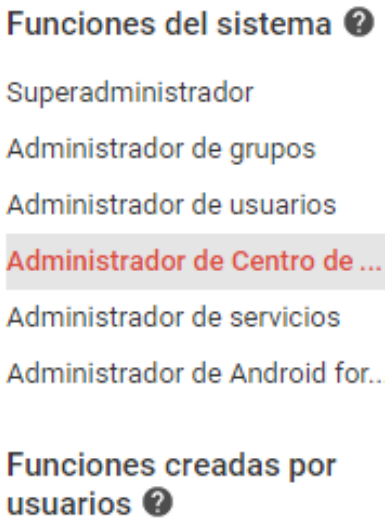

Figura A.26: Funciones para administradores en general.

MANUAL DE USUARIO: Configuración de informes de Google Apps For Work.

Paso 1. En la pestaña informe selecciona el tipo de informe que se desee, acepte y proceda a visualizar los informes.

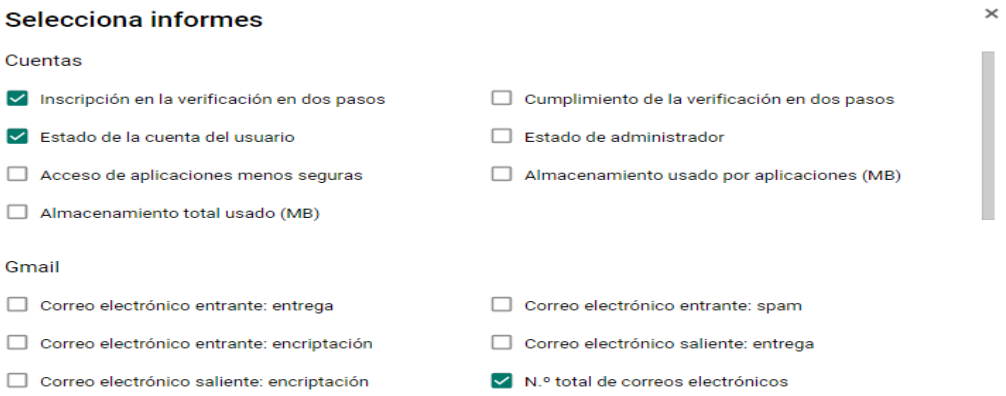

Figura A.27: Selección de informes.

Paso 2. Informe de verificación en dos pasos de los dispositivos móviles conectados.

Figura A.28: Informe de cuentas de usuarios.

Paso 3. Informe del estado de la cuenta del usuario, visualiza la actividad de la cuenta, dispositivos bloqueados, en suspensión y activos

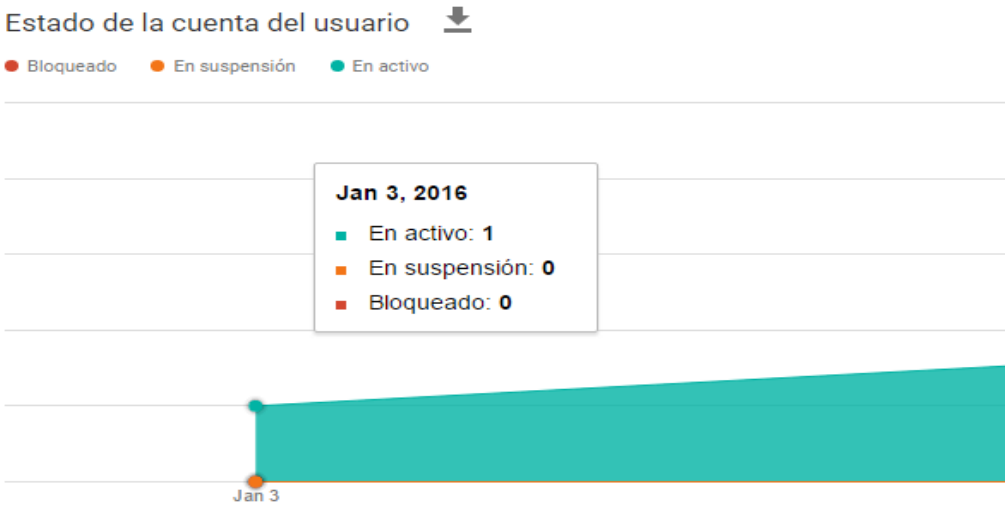

Figura A.29: Informe de estado de las cuentas de usuarios.

Paso 4. Informe de archivos visibles, compartidos con los usuarios del dominio.

Figura A.30: Informe de archivos visibles externamente.

Paso 5. Informes de archivos almacenados en Google Drive, puede aplicar políticas de usuarios y de dispositivos, activación o desactivación de servicios para un grupo de usuarios.

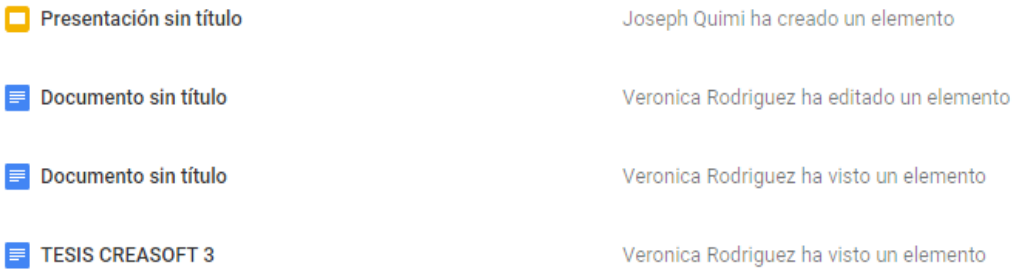

Figura A.31: Informe de documentos almacenados en Google Drive.

MANUAL DE USUARIO: Configuración de Administración de dispositivos en redes

El administrador de CREASOFT ECUADOR, tiene la ventana de redes para configuración de conexiones en los dispositivos móviles, Wi-Fi, Ethernet, VPN, Certificados.

Figura A.32: Administrador de redes.

Configuración del dispositivo en redes Wi-Fi

Paso 1. Analizar y agregar los SSID de las redes inalámbricas de la empresa.

Paso 2. En Administración de dispositivos seleccionar Redes Wi-Fi para Configuración.

Paso 3. Ingresar los identificadores de la red Wi-Fi, habilitar conexión automática y tipo de seguridad de la red.

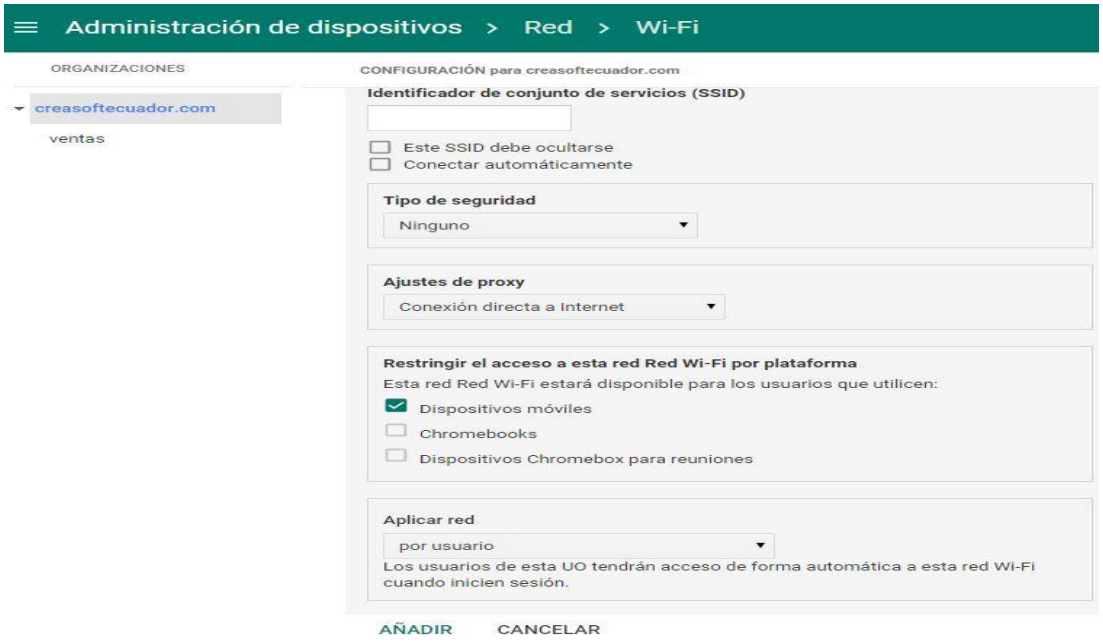

Figura A.33: Formulario para ingresar redes Wi-Fi.

Configuración del dispositivo en redes Ethernet

La Configuración para Ethernet es un subconjunto de las redes Wi-Fi, que utilizan los dispositivos móviles y se hereda de la Configuración Wi-Fi

Paso 1. En Administración de dispositivos seleccionar redes Ethernet.

Paso 2. Ingresar los identificadores de la red Ethernet, el tipo de autenticación inalámbrica 802.1x, protocolo de autenticación, usuario y contraseña precompartida.

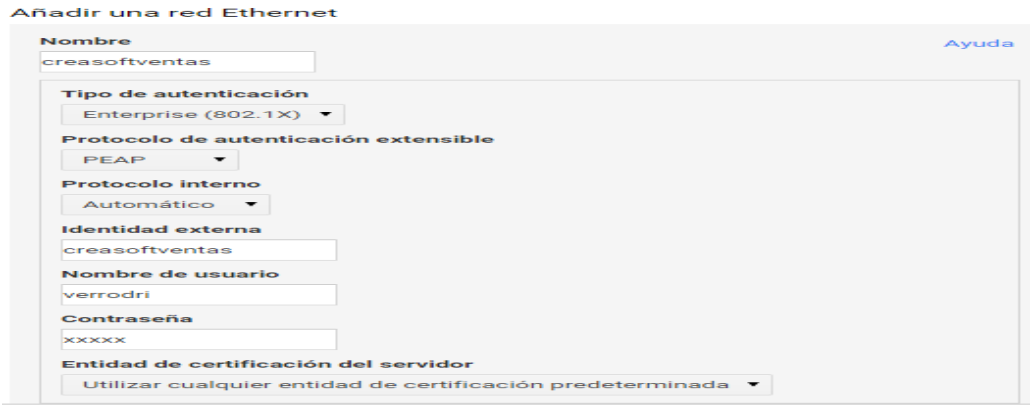

Figura A.34: Formulario de redes Ethernet inalámbricas.

Configuración del dispositivo de Redes Privadas Virtuales

El usuario, al estar aislado de una zona de internet que no está administrado por la empresa puede Configuración la red virtual.

Paso 1. En Administración de dispositivos seleccionar redes VPN, la VPN puede ser L2tp que trabaja con IPSec u Open VPN.

Paso 2. Ingresa los campos, clave precompartida, nombre usuario, contraseña, host remoto se refiere a la dirección ip del host o nombre servidor que facilita el acceso a la VPN.

Figura A.35: Formulario de redes privadas virtuales.

Paso 3. Configuración del dispositivo en redes con certificados, en la pestaña redes dar clic en certificados para agregarlos.

Los certificados tienen formato X.509 PEM (Privacy Enhanced Mail) públicos, para servidores PEAP, TLS, en redes Wifi una contraseña o si tiene conFigura A.do claves públicas SSL.

Manual de Usuario: Administración de dispositivos móviles, configuración de administración de dispositivos.

Entre las distintas opciones la solución, activa dispositivos, establece el número de veces que se ha introducido la contraseña antes de borrar los datos de la empresa que están almacenados además de otras opciones que se muestran en la figura.

Figura A.36: Administración de dispositivos móviles.

Paso 1. Configuración general, controla la sincronización de las cuentas, seguridad, contraseñas y otros ajustes.

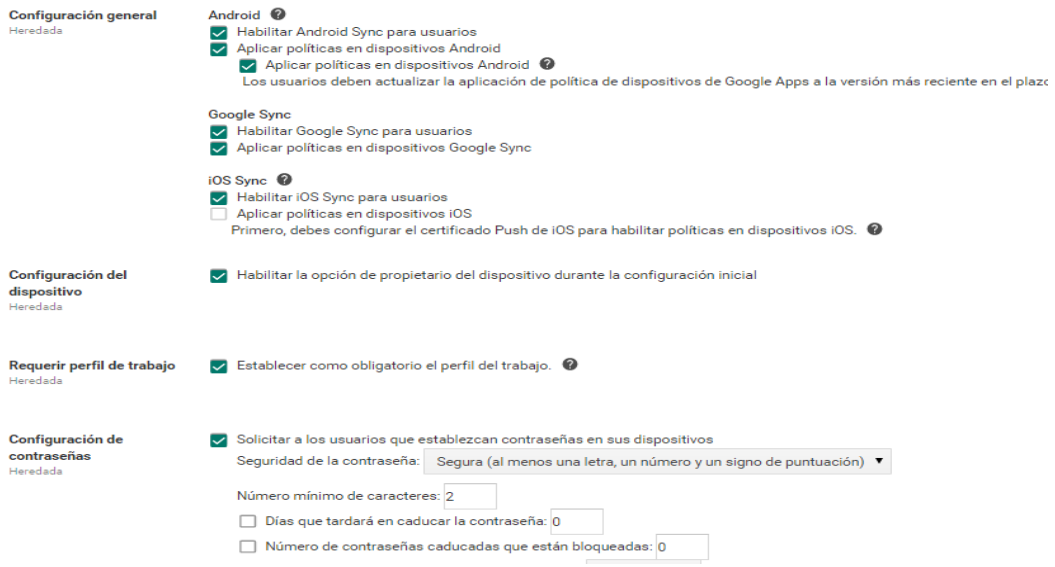

Figura A.37: Formulario de Configuración básica de dispositivos móviles.

Cuando se detecta que la seguridad de un dispositivo está comprometida, puede enviar notificaciones, desactivar el uso compartido personal y empresarial, bloquear el dispositivo.

Android	Google Sync	IOS Sync
Habilitar Android Sync para usuarios	Habilitar Google Sync para usuarios	Habilitar IOS Sync para usuarios
Aplicar políticas en dispositivos Android	Aplicar políticas en dispositivos Google Sync	Habilitar políticas en los dispositivos IOS
Eliminación de los datos de la cuenta de Android si		CalDAV (calendario y contactos) iCloud cifrado copia de seguridad

el dispositivo no se sincroniza. 20 días		

Tabla 7. Configuración de los dispositivos [28], [29].

Paso 2. Activación de dispositivos, la lista de dispositivos es analizada por el administrador, inmediatamente bloquea, elimina la cuenta, activa primero los dispositivos antes de brindarle acceso a los datos, se visualiza detalles de id, nombre de persona al que pertenece, correo, modelo, tipo, ultima sincronización, estado, opciones de eliminación remota, aprobar los dispositivo pendientes.

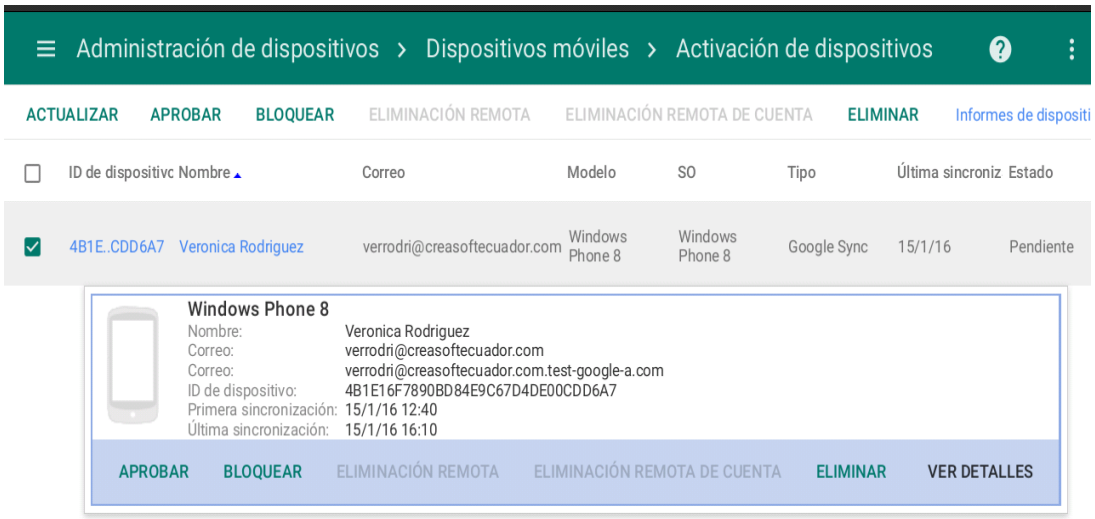

Figura A.38: Formulario para aprobación de dispositivos móviles.

Paso 3. Dispositivo administrado, contiene el listado de los dispositivos que se hayan vinculado a la cuenta y sus detalles, modelo, sistema operativo, tipo de sincronización.

Figura A.39: Lista de dispositivos móviles vinculados a la solución.

Paso 4. Configuración certificado push de los dispositivos con sistema operativo IOS de Apple.

Figura A.40: Configuración de certificado de dispositivos Apple.

Paso 5. Administrar aplicaciones para dispositivos iOS, configuración de certificados para utilizar las aplicaciones.

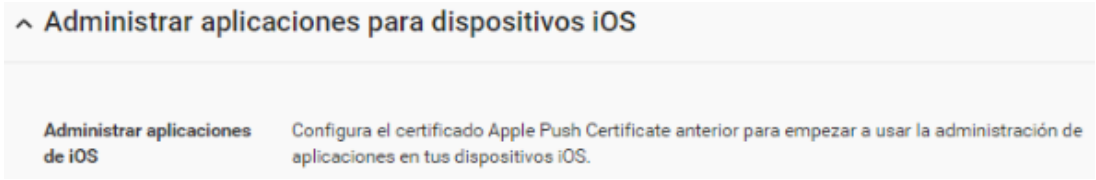

Figura A.41: Administrar aplicaciones para dispositivos iOS.

Paso 6. Administrar las aplicaciones instaladas en los dispositivos con el sistema operativo Android por medio de la consola de administración.

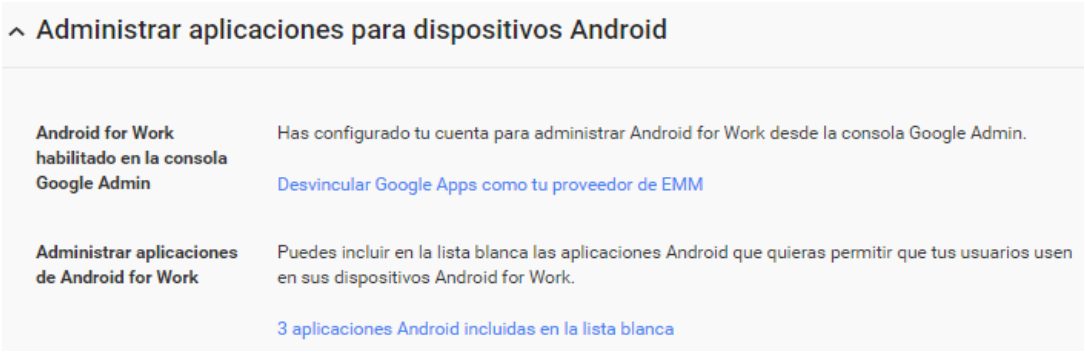

Figura A.42: Administrar aplicaciones para dispositivos Android.

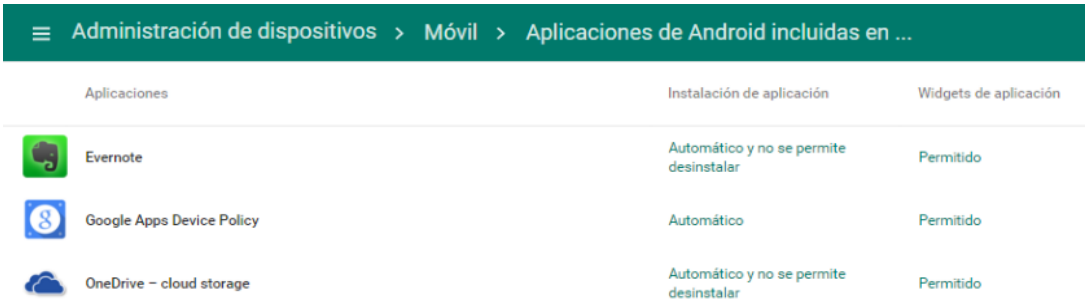

Figura A.43: Administración de aplicaciones de Android.

MANUAL DE USUARIO: para la migración y configuración de la dirección de correo electrónico.

Paso 1. Inicie sesión con la cuenta de perfil de administrador y acceda al panel de control cPanel, para activar el correo primero se procede a cambiar los registros Mx del dominio creasoftecuador.com, elija la opción para migrar el correo [30].

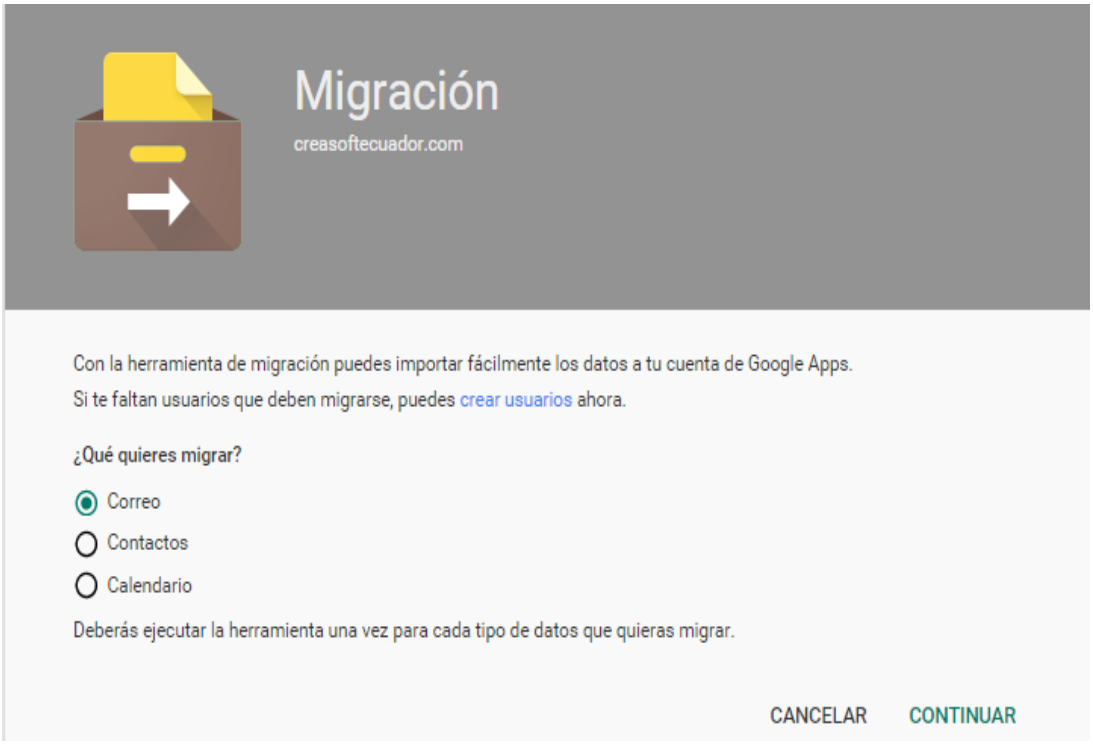

Figura A.44: Herramienta de migración.

Paso 2. Ingrese el nombre de la empresa a la que contrató el dominio, ingrese las credenciales de la cuenta para poder migrar.

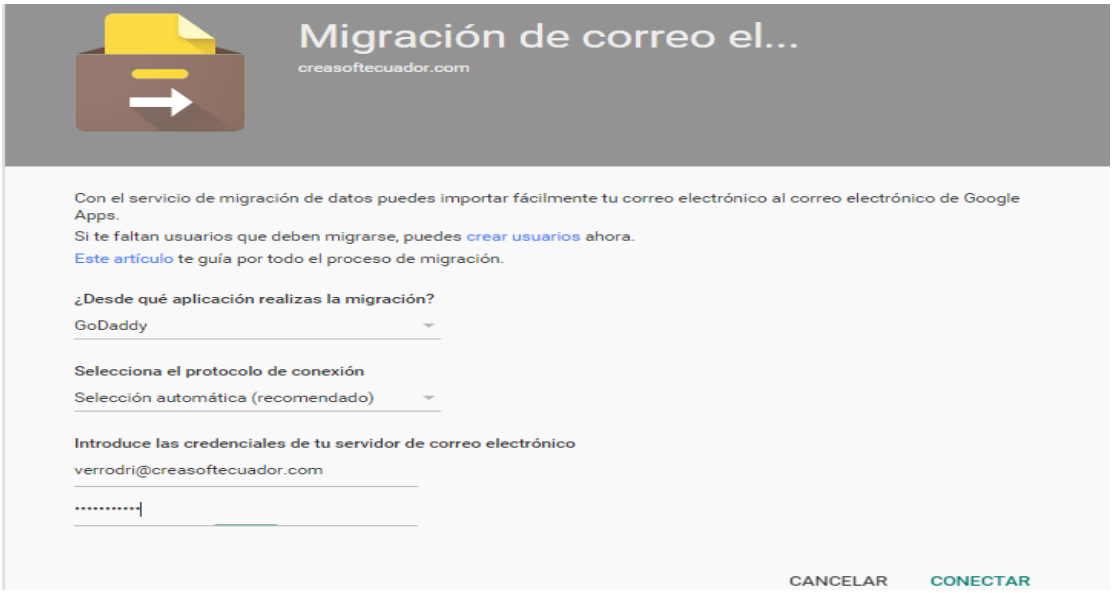

Figura A.45: Datos de migración.

Paso 3. Escoja el tiempo para migrar el correo electrónico, 6 meses y a continuación la conexión se establece, dé clic en seleccionar a usuarios.

Figura A.46: Detalles de migración de correo.

Paso 4. Selecciona los usuarios y finaliza la configuración de los registros en la solución, el flujo de correo a los servidores de Google tiene una duración 48 horas.

Figura A.47: Lista de usuario migrado.

Manual de usuario. Configuración un dispositivo móvil IOS con Google Sync

Paso 1. En la pestaña ajustes añada la cuenta y presione el botón otras (correo empresarial propietario) con Microsoft Exchange

Figura A.48: Configuración de correo a dispositivo iOS.

Paso 2. Añada el correo, el dominio empresarial, nombre de usuario y contraseña.

Figura A.49: Formulario datos Exchage en iOS.

Paso 3. Acepte los avisos de seguridad y dé clic en aceptar, sincronice los correos, los eventos programados en el calendario, cuentas, aplicaciones y otros. Nota: también puede descargar Gmail.

MANUAL DE USUARIO. Configuración de un dispositivo móvil con Windows Phone 8.1

Paso 1. Ingrese a la Configuración en Setting / Email + account /Add an account/ Advance setup

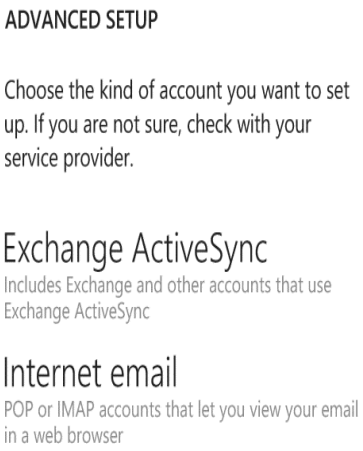

Figura A.50: Configuración correo en dispositivo Windows Phone.

Paso 2. Ingrese los datos del usuario, contraseña y dominio, si desea descargar los correos anteriores, aquí se puede configuración esta opción, escoja 3 días.

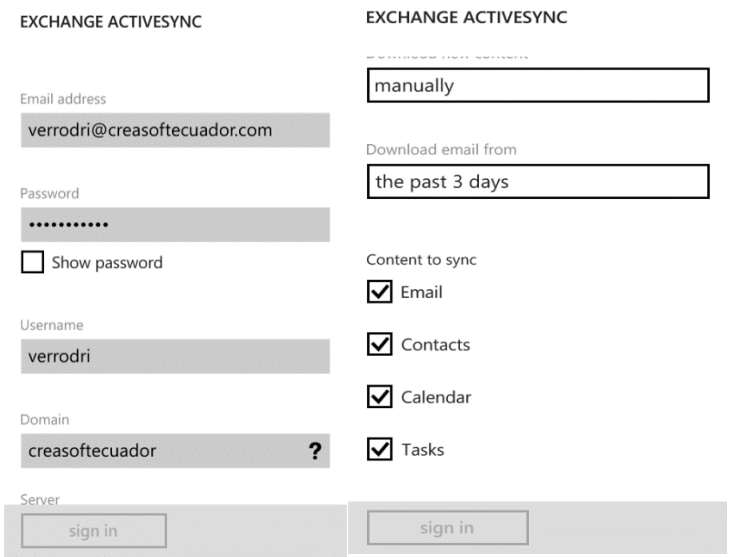

Figura A.51: Formulario datos Exchange en Windows Phone.

Manual de usuario: Instalación de la solución en el dispositivo Android.

Paso 1. Luego de agregue la cuenta, instale las políticas de privacidad en el dispositivo.

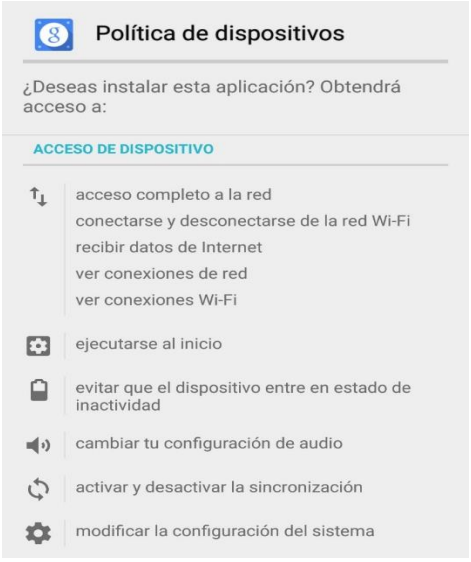

Figura A.52: Instalación de políticas de privacidad en el dispositivo.

Paso 2. Se aplican las políticas por defecto en el dispositivo móvil y requiere realizar el cambio de contraseña como política predeterminada.

Figura A.53: Políticas de privacidad aplicadas en el dispositivo.

Paso 3. Cifrar el teléfono por motivos de seguridad, los datos se envían cifrados al momento de transmitir información entre el dispositivo y Google.

Figura A.54: Cifrado del dispositivo.

Paso 4. Crear perfil de trabajo, en el sistema operativo Android necesita previamente la instalación de la APP política de dispositivos.

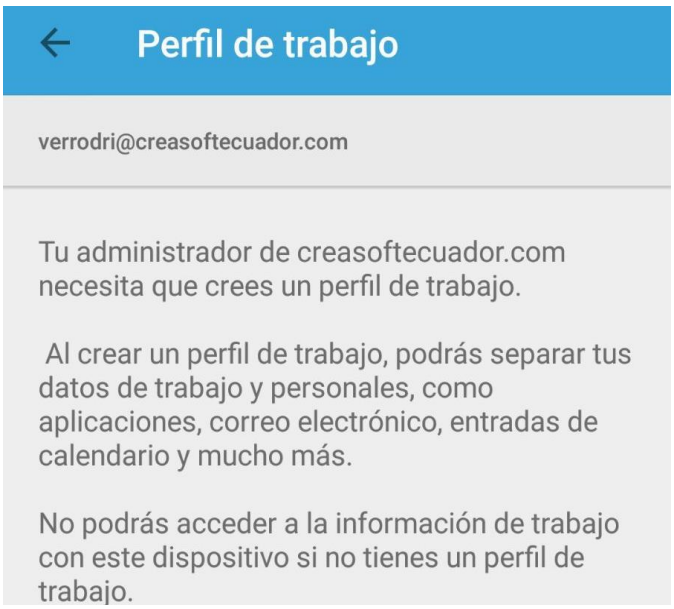

Figura A.55: Creación de perfil de trabajo en el dispositivo.

Paso 5. Configuración del perfil de trabajo en el dispositivo móvil, configuración de las capacidades del administrador de la solución.

Figura A.56: Configuración del perfil de trabajo en el dispositivo.

Paso 6. Instalación automática de aplicaciones autorizadas por el administrador.

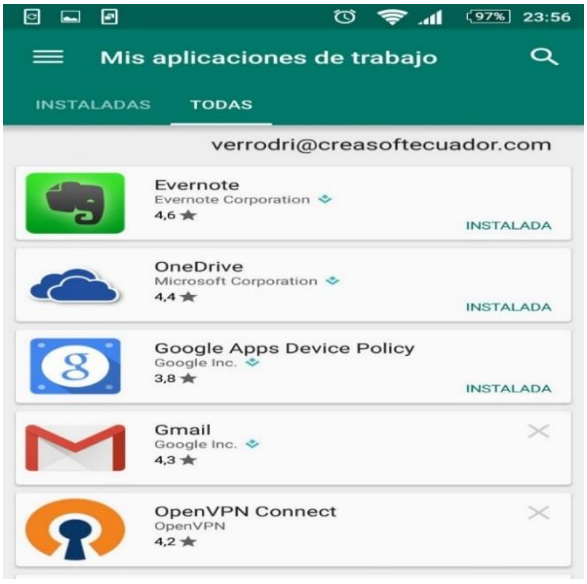

Figura A.57: Aplicaciones instaladas automáticamente en el dispositivo.

Paso 7. Acceso a la tienda de aplicaciones Play Store y visualización de las aplicaciones de trabajo permitidas en el dispositivo, en el segmento empresarial.

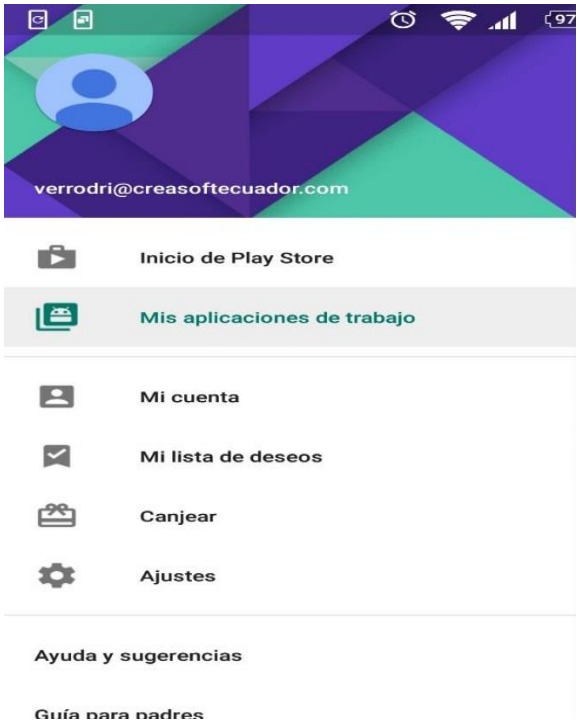

Figura A.58: Tienda de aplicaciones Play Store de Google Apps For Work.

ANEXO B.

DATASEET DE ROUTER CISCO VPN RV320.

La conectividad de red es el centro de cada pequeña empresa y el acceso seguro, la protección de firewall y el alto rendimiento son los pilares de cada router Cisco® Small Business de la serie R. El router Cisco VPN con WAN Gigabit dual RV320 no es la excepción. Con una interfaz de usuario intuitiva, el router Cisco RV320 está listo para funcionar en minutos. El router Cisco RV320 ofrece acceso confiable y altamente seguro para usted y sus empleados, tan transparente que no sabrá que está allí.

Figura B.59: Router Cisco VPN con WAN Gigabit dual RV320

Funciones y ventajas

- Los puertos WAN Gigabit Ethernet dobles facilitan el equilibrio de carga y la continuidad comercial.
- Los puertos Gigabit Ethernet asequibles y de alto rendimiento permiten la transferencia rápida de archivos grandes y admiten varios usuarios.
- Los puertos USB dobles admiten un módem 3G/4G o una unidad flash. La red WAN también tiene conmutación por falla con el módem 3G/4G conectado a un puerto USB.
- Las plataformas VPN con SSL y VPN de sitio a sitio permiten una conectividad altamente segura, por lo que el router Cisco RV320 es perfecto para empleados remotos y diversas oficinas.

- El firewall con inspección activa de estado de paquetes (SPI) y el cifrado de hardware ofrecen una sólida seguridad.
- Las herramientas de configuración fáciles de utilizar, de acuerdo con asistentes, pueden utilizarse para establecer la conectividad de red y administrar la seguridad. En un entorno comercial en constante cambio, su pequeña red empresarial debe ser potente, flexible, accesible y altamente confiable, en especial cuando el crecimiento es la mayor prioridad. Su red debe poder adaptarse de manera rentable a este crecimiento.

El router Cisco VPN con WAN Gigabit dual RV320 es la elección de todas las redes para las que el rendimiento, la seguridad, la confiabilidad y la adaptabilidad encabezan la lista de requisitos. El router Cisco RV320 ofrece dos conexiones a un proveedor de servicios mediante el equilibrio de carga para obtener un alto rendimiento o a dos proveedores diferentes para garantizar la continuidad comercial. Las redes privadas virtuales (VPN) de alta capacidad conectan diversas oficinas y permiten a una gran cantidad de empleados acceder a la información que necesitan desde cualquier lugar con la misma seguridad que desde la oficina principal.

Especificaciones del producto

En la tabla 10, se enumeran las principales especificaciones del producto Cisco RV320.

Descripción	Especificación
WAN dual	● Puertos Gigabit Ethernet duales ● Falla ● Equilibrio de carga
Estándares	● 802.3, 802.3u ● IPv4 (RFC 791) ● IPv6 (RFC 2460)
Conectividad WAN	● Servidor de protocolo de configuración dinámica de host (DHCP), cliente DHCP, agente de retransmisión DHCP ● IP estática ● Protocolo punto a punto sobre Ethernet (PPPoE) ● Protocolo de túnel punto a punto (PPTP) ● Puente transparente ● Relé de DNS, DNS dinámico (DynDNS.org, 3322.org), base de datos local de DNS ● IPv6
Protocolos de routing	● Protocolo de información de routing (RIP) v1, v2 y RIP para IPv6 (RIPng) ● Routing entre VLAN ● Routing estático ● VLAN admitidas: 7

Traducción de direcciones de red (NAT)	● Traducción de direcciones de puertos (PAT) ● NAT uno a uno ● NAT transversal
Vinculación de protocolos	Los protocolos se pueden vincular a un puerto WAN específico para equilibrar la carga.
Perímetro de la red (DMZ)	● Puerto DMZ ● Host DMZ
Dos puertos USB 2.0	Almacenamiento y soporte de módem 3G/4G
Seguridad	
Firewall	● Firewall SPI ● Prevención de denegación de servicio (DoS): ping de la muerte, inundación SYN, falsificación de IP, WinNuke
Reglas de acceso	● Reglas de acceso según cronogramas ● Hasta 50 entradas
Reenvío de puerto	Hasta 30 entradas
Activación de puerto	Hasta 40 entradas
Bloqueo	Java, cookies, ActiveX, proxy HTTP
Filtrado de contenido	Bloqueo estático de dirección URL o bloqueo de palabras clave
Administración segura	● Acceso web HTTPS al administrador de dispositivos ● Aplicación de complejidad de nombre de

	usuario/contraseña
VLAN	802.1Q (VLAN) 7 VLAN admitidas
VPN	
Seguridad IP (IPsec)	● 25 túneles IPsec de sitio a sitio para conectividad de sucursales ● 25 túneles VPN IPsec a través del cliente VPN de Cisco y clientes de terceros como “The GreenBow”para la conectividad VPN de acceso remoto
VPN con SSL	10 túneles VPN con SSL para acceso remoto de clientes
PPTP	10 túneles PPTP para acceso remoto
Cifrado	● Estándar de cifrado de datos (DES) ● Estándar de triple cifrado de datos (3DES) ● Cifrado con norma de cifrado avanzado (AES): AES-128, AES-192, AES-256
Autenticación	MD5/SHA1
IPsec NAT transversal	Compatible con túneles gateway a gateway y túneles cliente a Gateway
Transferencia de VPN PPTP	Protocolo de túnel de capa 2 (L2TP), IPsec
VPN avanzada	Detección de punto muerto (DPD) ● DNS dividido ● Respaldo de VPN ● Intercambio de claves por Internet (IKE) con certificado

Calidad de servicio (QoS)	
QoS basada en el servicio	Prioridad o control de velocidad
Control de tráfico	Ancho de banda de carga y descarga por servicio
Tipos de priorización	Prioridad basada en la aplicación en el puerto WAN
Prioridad	Servicios asignados a uno o dos niveles de prioridad
Rendimiento	
Rendimiento de NAT	900 Mbps
Rendimiento de VPN con IPsec	100 Mbps
Rendimiento de VPN con SS	20 Mbps
Conexiones simultaneas	20000
Configuración	
Interfaz de usuario web	Administrador de dispositivos de acuerdo con el navegador (HTTP/HTTPS)
Administración	
Protocolos de administración	● Navegador web (HTTP/HTTPS) ● Protocolo simple de administración de redes (SNMP) v1, v2c y v3 ● Bonjour

Registro de eventos	● Registro local ● Syslog ● Alerta por correo electrónico ● Servicio de mensajes cortos (SMS)
Capacidad de actualización	● Firmware que se puede actualizar mediante el navegador web ● Importación o exportación de archivos de configuración de o a una unidad flash USB

Tabla 8: Especificaciones del producto

Especificaciones del sistema

En la tabla 11, se enumeran las especificaciones del sistema de Cisco RV320.

Descripción	Especificación
Dimensiones del producto (ancho x alto x profundidad)	206 x 132 x 44 mm (8,1 x 5,2 x 1,7 pulgadas)
Puertos	Cuatro puertos RJ-45 Gigabit Ethernet 10/100/1000 Un puerto RJ-45 Gigabit Ethernet (WAN) 10/100/1000 Un puerto RJ-45 Gigabit Ethernet 10/100/1000 DMZ/Internet (WAN)
Fuente de alimentación	12 V 1,5 A
Certificación	FCC clase B, CE clase B, UL, cUL, CB, CCC, BSMI, KC, Anatel
Temperatura de	De 0° a 40 °C (32° a 104 °F)

funcionamiento		
Temperatura almacenamiento	**de**	0° a 70 °C (32° a 158 °F)
Humedad funcionamiento	**de**	De 10 a 85%, sin condensación
Humedad almacenamiento	**de**	De 5 a 90%, sin condensación

Tabla 9: Especificaciones del sistema

Información sobre la garantía

Obtenga información sobre la garantía en la página Product Warranties (Garantías de productos) de Cisco.com.

Información para realizar pedidos

Ofrezca ayuda a los clientes para que comprendan cuáles son los componentes y las piezas que necesitan comprar para instalar y utilizar el producto. En la Tabla 3, se ofrece información para realizar pedidos de Cisco RV320. En esta sección, también se ofrece un vínculo directo a la herramienta de Cisco para realizar pedidos y enumera los números de piezas para la comodidad de los clientes.

Para hacer un pedido, visite la página principal de pedidos de Cisco. Para descargar software, visite el centro de software de Cisco.

Nombre del producto	Numero de pieza
Router VPN con WAN dual RV320	RV320-K9-NA
Router VPN con WAN dual RV320	RV320-K9-G5
Router VPN con WAN dual RV320	RV320-K9-AU
Router VPN con WAN dual RV320	RV320-K9-CN
Router VPN con WAN dual RV320	RV320-K9-AR

Tabla 10: Información para realizar pedidos

Garantía limitada de por vida de Cisco para productos Cisco Small Business

Este producto Cisco Small Business incluye una garantía de hardware limitada de por vida. Los términos de la garantía del producto y otra información aplicable a los productos de Cisco están disponibles en www.cisco.com/go/warranty.

Servicio de soporte técnico de Cisco Small Business

Este servicio opcional ofrece cobertura asequible de tres años para su tranquilidad. Este servicio por suscripción a nivel del dispositivo lo ayuda a proteger su inversión y a obtener el máximo valor de los productos Cisco Small Business. Proporcionado por Cisco y respaldado por su partner de confianza, este servicio integral ofrece acceso extendido a Cisco Small Business Support Center y reemplazo de hardware acelerado, de ser necesario.

Más información

Para obtener más información sobre el Router Cisco VPN con WAN Gigabit dual RV320, visite www.cisco.com/go/rv320.

Anexo C Diagrama de Gantt

ANEXO D

Correos de aviso de migración de correo, dirigido a los empleados.

Correo número uno.

Asunto del correo Línea: [CREASOFT] está moviendo a Google Apps!

A todos [CREASOFT] empleados:

Estamos muy contentos de anunciar que Creasoft pronto moverá su correo electrónico y calendario plataforma desde [Microsoft Outlook] para Gmail y Google Apps. Con Google Apps, vamos a obtener los beneficios de un robusto conjunto de características e innovador, la capacidad de acceder a los servicios de correo electrónico y calendario desde cualquier ordenador conectado a Internet, mucho más capacidad de almacenamiento y reducir los costos de infraestructura y de apoyo. Es más, Google Apps es fácil de usar, y creemos que usted encontrará que es una forma más eficaz de gestionar su correo electrónico y calendario!

En las próximas semanas / meses [], recibirá avisos adicionales al comenzar el cambio de los empleados [Outlook / Notas] cuentas de Gmail. Pero no se preocupe, usted no perderá datos importantes, y su dirección de correo electrónico no va a cambiar.

Atentamente,

CREASOFT ECUADOR

Correo número 2.

Asunto del correo Línea: IMPORTANTE: Su correo electrónico y calendario se va a migrar a Google Apps

CREASOFT ahora está empezando a cambiar nuestros sistemas de correo electrónico y calendario a partir de [Microsoft Outlook / Lotus Notes] para Google Apps. Con Google Apps, vamos a obtener los beneficios de 100% basado en la web las herramientas de colaboración y mensajería, así como menores costos de infraestructura y de apoyo. Usted ha sido elegido para ser [un usuario piloto] para Google Apps Mail y Calendar. Nos gustaría que usted utilice los servicios y nos proporciona retroalimentación antes de desplegar estos servicios a otros equipos. Con su ayuda, estamos seguros de que podemos rodar con éxito los servicios a todos los [nombre de la empresa] empleados.

Estamos migrando sus [/ Notas de Outlook] de datos de la siguiente manera:

Mensajes en el buzón de entrada [Outlook / Notes] (incluidas las subcarpetas) y carpeta Enviados ==> Gmail Los eventos programados en su [Outlook / Notas] Calendario ==> Google Calendar Los contactos personales en sus [contactos de Outlook / Notes Libreta de direcciones] ==> Mis contactos en Gmail

Lo que sucederá

En [Fecha / Hora], nos desviamos su cuenta [Outlook / Notes] y gire en su nueva cuenta de Google Apps.

En ese momento, habrá una [X hora / minuto] [Outlook / Notas] apagón ya que migrar los datos.

Por favor, no use [Outlook / Notas] después de [fecha / hora].

Atentamente,

CREASOFT ECUADOR

Correo número tres.

Asunto del correo Línea: AVISO FINAL: Su cuenta [Microsoft Outlook / Lotus Notes] está a punto de migrar a Google Apps

Este mensaje es el último aviso de que su cuenta [Microsoft Outlook / Lotus Notes] se desactivará en [Fecha / hora] mientras que establecimos con Google Apps. *** Por favor, cierre la sesión de [Microsoft Outlook / Lotus Notes] ahora. *** [PERSPECTIVAS / NOTAS] CORTE Mientras que migrar los datos, habrá una [X hora / minuto] interrupción de su cuenta [Outlook / Notes], de la siguiente manera: [agregar gama fecha / hora para la migración]

LO QUE DEBE HACER AHORA

Imprimir Apps Guía de inicio rápida de Google << agregar link o adjuntar archivos >> y dejarlo en su escritorio. Esta guía le muestra cómo acceder a su nueva cuenta de Google Apps y acceder a sus servicios de correo electrónico y calendario. Imprime tu [Outlook / Notas] Calendario antes de [fecha / hora], en caso de tener que referirse a ella antes de acceder a Google Calendar en [Fecha / hora]. ¿Preguntas?

Atentamente,

CREASOFT ECUADOR

GLOSARIO

BYOD siglas en inglés Bring your own device, en español Trae tu propio dispositivo. Hace referencia a que los empleados de una empresa pueden llevar su dispositivo (Tablet, celular o laptop) al lugar de trabajo.

APP es el término informático que hace referencia a las aplicaciones.

Wi-Fi 802.1x controla el acceso a la red corporativa en un punto de acceso (AP), utilizando protocolo de autenticación extensible (EAP), además permite ver una conexión punto a punto en una red local.

SSAE 16/ISAE 3402 tipo II Statement on Standards for Attestation Engagements / "International Standard on Assurance Engagements son auditorías externas encargadas de analizar y garantizar la seguridad lógica, seguridad física, gestión de cambios, organización, administración e integridad de los procesos de los clientes de las empresas.

EAP Protocolo de autenticación extensible, encapsula los datos con diferentes métodos actualmente más de 40 definidos oficialmente, mayormente utilizada en redes inalámbricas y conexiones punto a punto.

PEAP Conocido como EAP protegido, utiliza autenticación y cifrado, requiere una clave PKI del lado del servidor para crear un túnel seguro (TLS) para proteger la autenticación de usuarios y la información viaja cifrada.

LEAP protocolo de autenticación ligero desarrollado por CISCO, utilizado en la red LAN inalámbrica con claves WEP dinámicas y autenticación mutua frecuente.

TLS Seguridad en la capa de transporte, utiliza protocolos criptográficos en las comunicaciones por la red

X.509 Término utilizado por UIT-T para definir un formato estándar para infraestructuras de claves públicas cifradas en los inicios de sesión únicos.

Android. Sistema operativo implementado en la mayoría de celulares con pantalla táctil basado en Unix.

IOS. Sistema operativo para celular propietario de Apple Inc. utilizado los celulares Iphone.

Windows Phone. Sistema operativo diseñado para celular basado en el sistema operativo Windows.

Google apps for work. Solución en la nube con características similares a los servidores tradicionales internos.

Unidades organizativas. Es un contenedor de usuarios computadoras y grupos que permite su administración.

EMM Siglas en ingles Enterprise mobility management. En español Gestión de movilidad empresarial, proceso de utilizar teléfonos inteligentes como medio de trabajo.

DNS Base de datos jerárquica y distribuida que contiene asignaciones de nombres de dominio DNS para varios tipos de datos, como direcciones IP.

L2TP (Layer 2 Tunneling Protocol) es un protocolo para conectar redes privadas virtuales remotas de una empresa o del hogar, no posee características criptográficas, es económico

IPsec (Internet Protocol Security) es un protocolo de autenticación y/o cifrado que utiliza una clave precompartida, aplicado sobre el protocolo de internet IP.

GCM Google Cloud Messaging es un servicio, permite a los desarrolladores enviar los datos desde los servidores de google a las aplicaciones Android, aplicaciones Chrome y extensiones.

MDM (Mobile Device Management) es un de software, permite asegurar, monitorear y administrar dispositivos móviles sin importar el operador de telefonía o proveedor de servicios.

API La interfaz de programación de aplicaciones, abreviada como API (del inglés: Application Programming Interface), es el conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

CALDAV es un protocolo de sincronización, permite a un cliente acceder a información del calendario en un servidor remoto: extiende WebDAV (protocolo basado en HTTP para la manipulación de datos) y utiliza iCalendar como formato para los datos.

Microsoft Exchange ActiveSync es un protocolo usado para sincronizar correos, contactos y calendarios

DashBoard es una Interfaz gráfica de usuario, yace tanto en consolas de videojuegos como en algunos sistemas operativos. Es una interfaz donde el usuario puede administrar el equipo y/o software.

CA siglas en inglés Certification Authority, es una empresa comprometida a emitir o revocar certificados digitales, utilizados en la firma electrónica.

S/MIME Secure / Multipurpose Internet Mail Extensions, Extensiones de Correo de Internet de Propósitos Múltiples / Seguro es un estándar para criptografía de clave pública y firmado de correo electrónico

MAM Gestión de aplicaciones móviles (MAM) describe el software y los servicios responsables de aprovisionamiento y controlar el acceso a las aplicaciones móviles desarrolladas internamente y disponibles comercialmente utilizados en entornos de negocios en ambos y proporcionado empresa "traer sus propios" teléfonos inteligentes y computadoras tablet .

Apple Store es una cadena de tiendas, conocida también como Retail Store de propiedad de Apple.

Play Store es una plataforma de distribución digital de aplicaciones móviles, consumida por dispositivos con sistema operativo Android, es desarrollada por la empresa Google

Streaming es la distribución multimedia por una red de computadoras, el usuario accede a los recursos sin interrupción.

Mbps Megabits por segundo es la tasa de transferencia empleada como medida para las conexiones a internet.

MB Un Megabyte equivale a 1024 bytes de memoria.