



Aranda **Enterprise**
Mobility Management

Manual de Instalación y Uso
Versión 9

Tabla de contenido

1. Introducción	7
1.1. Qué es Aranda Enterprise Mobility Management	7
1.2. Requisitos de Sistema	8
2. Instalación	13
2.1. Configuración de Base de datos y Servicios Windows	17
2.2. Configuración de Licenciamiento	17
2.3. Configuración Inicial	22
3. Administración	22
3.1. Integración empresarial	22
3.1.1. Configuración de Correo	22
3.1.2. Configuración de Directorio Empresarial	24
3.1.3. Configuración conexión con CMDB	26
3.2. Usuarios	28
3.2.1. Listado de usuarios	28
3.2.2. Creación de usuario nuevo	30
3.2.3. General	31
3.2.4. Dispositivos	32
3.2.5. Grupos de usuarios	33
3.2.6. Roles	33
3.2.7. Seguridad y control de acceso usando roles	34
3.2.7.1. Descripción de los distintos tipos de Roles	34
3.2.7.2. Asignación de roles a un usuario	35
3.2.7.3. Asignación de roles a un grupo de usuarios	37
3.2.8. Importación de usuarios	40
3.2.9. Estado de usuarios	41
3.3. Grupos	43
3.3.1. Creación de grupos	43
3.3.2. Agregación de usuarios a un grupo	46
3.3.3. Agregación de dispositivos a un grupo	47
3.4. Grupos Dinámicos	48
3.5. Actividad de consola	51
3.6. Licenciamiento	52
3.7. Autenticación otros proveedores	53
3.7.1. Configuración	53
3.7.2. Ingreso por parte del usuario	55
4. Preferencias	56
4.1. Política de Grupo	56
4.2. Configuración calendarios	57
4.2.1. Horario laboral	58

4.2.2.	Días no laborales	59
4.2.3.	Dispositivos	61
4.3.	Móviles	62
4.3.1.	Vinculación	62
4.3.2.	Soporte Remoto	63
4.3.3.	Perfiles de Agente	64
4.3.3.1.	Creación de un perfil de agente	64
4.3.3.2.	Asociación de dispositivos	66
4.3.4.	iOS	66
4.3.4.1.	Pestaña "iOS"	66
4.3.4.2.	Certificado APNs	67
	Renovación de un certificado APN previamente creado	74
4.3.4.3.	Apple Business Manager (ABM)	75
4.3.4.4.	Volume Purchase Program (VPP)	81
4.3.5.	Android for work	86
4.3.5.1.	Pestaña "Android For Work"	86
4.3.5.2.	Grupos de Aplicaciones en Android For Work	89
	Gestión de páginas	90
4.3.6.	Configuración del Ping	92
4.3.7.	Aplicaciones del sistema Android	93
4.4.	Plantillas	95
4.5.	Scripts	96
4.5.1.	Creación de scripts	97
4.5.2.	Edición del Script	98
4.5.3.	Comandos disponibles para scripts	101
4.5.4.	Eliminación de scripts	102
4.6.	Zonas	103
5.	Vinculación de dispositivos	105
5.1.	Android	105
5.1.1.	Vinculación desde consola Web	106
5.1.2.	Vinculación desde el correo de invitación	107
5.1.3.	Vinculación usando link	108
5.1.4.	Vinculación ingresando la información de forma manual	109
5.2.	Android for Work	112
5.2.1.	Vinculación AFW Profile Owner	112
5.2.2.	Vinculación AFW Device Owner	114
5.3.	iOS	117
5.4.	Windows	125
5.4.1.	Vinculación Windows 10 Pro	125
5.4.1.1.	Vinculación al MDM Nativo de Microsoft Windows	125
5.4.1.2.	Vinculación del Agente Aranda AEMM para Windows	131
5.4.2.	Vinculación Windows 10 Mobile	134
5.5.	Desvinculación	140
5.5.1.	Desde la consola Web	140
5.5.2.	Desde el dispositivo	141

5.6.	Re-vinculación de dispositivos	143
5.7.	Problemas comunes de vinculación	144
6.	Dashboards	147
6.1.	Dashboard de Dispositivos	147
6.2.	Dashboard de Consumos	150
7.	Módulo Dispositivos	153
7.1.	Dispositivos	153
7.1.1.	General	153
7.1.2.	Actividad	154
7.1.3.	Aplicaciones	155
7.1.4.	Ubicación	155
7.1.5.	Consumo	156
7.2.	Proyectos de Gestión	160
7.3.	Gestión de Consumos	164
7.3.1.	Excepciones	165
8.	Aplicaciones	166
8.1.	Instalación de aplicaciones usando una URI externa	169
8.1.1.	Proceso De Carga Y Publicación De Archivo En Microsoft Azure	169
8.2.	Utilización De La Uri Creada En Microsoft Azure Como Url Externa De Aplicación En Aemm	181
8.3.	Costos	184
9.	Políticas	185
9.1.	Cumplimiento en dispositivos	185
	Listado y pre visualización	186
9.2.	Configuración de políticas	187
9.2.1.	Restricciones Android	187
9.2.2.	Restricciones en iOS	189
9.2.3.	Contraseña	190
9.2.3.1.	Android	190
9.2.3.2.	iOS	192
9.2.4.	Wifi	193
9.2.4.1.	Android	193
9.2.4.2.	iOS	194
9.2.5.	Web clips	194
9.2.5.1.	Android	194
9.2.5.2.	iOS	195
9.2.6.	Email	196
9.2.6.1.	Android	196
9.2.6.2.	iOS	197
9.2.7.	Exchange Active Sync	198
9.2.7.1.	Android	198

9.2.7.2.	iOS	200
9.2.8.	Aplicaciones	201
9.2.8.1.	Lista Blanca	201
9.2.8.2.	Lista Negra	201
9.2.8.3.	Aplicaciones requeridas	202
9.2.9.	Kiosco	203
9.2.9.1.	Android	203
9.2.9.2.	Android For Work	205
9.2.10.	Dispositivos asociados	206
9.2.11.	Aplicación de Políticas	207
9.3.	Versionamiento y re- distribución de políticas	208
10.	Reglas	212
10.1.	Configuración de conjuntos de reglas	213
10.2.	Listado y pre visualización de conjuntos de reglas	216
10.3.	Dispositivos asociados	217
10.3.1.	Visualizar dispositivos	217
10.3.2.	Agregar dispositivos	218
10.4.	Aplicación de conjuntos de reglas	219
11.	Documentos	220
11.1.	Administración de contenidos Creación de carpetas y Sub-carpetas	221
11.2.	Edición y eliminación de carpetas	222
11.3.	Agregar Archivos	223
11.4.	Editar, Descargar y Eliminar Archivos	225
11.5.	Administración de permisos	226
12.	Alertas	234
12.1.	Generación y manejo de alertas	235
13.	Content Management para android	236
13.1.	Ingreso a la aplicación	237
13.2.	Visualización general	239
13.3.	Menú de vistas	243
13.4.	Subir archivos	245
13.5.	Controles de la barra de opciones	248
13.6.	Filtros	249
14.	Content Management Para iOS	251
14.1.	Visualización general	253
14.2.	Menú de vistas	257

14.3.	Subir archivos _____	260
14.4.	Controles de la barra de opciones _____	264
14.5.	Filtros _____	265

Control de cambios	
Fecha de creación	Aranda Enterprise Mobile Management V9 Manual de Instalación y Uso
<i>2018. Septiembre 20</i>	<i>Versión 3</i>
<i>2019. Enero 21</i>	
<i>2020 Octubre 2</i>	Elaborado por
<i>2020 Diciembre 4</i>	<i>Aranda Software</i>
<i>2021 Enero 5</i>	

1. INTRODUCCIÓN

El uso de dispositivos móviles para mejorar la productividad en las empresas es cada vez más frecuente. Los empleados utilizan celulares y tabletas para acceder a información corporativa, comunicarse con otros empleados, realizar presentaciones, acceder al correo corporativo, ubicar servicios geográficamente, etc. En muchos casos los dispositivos son adquiridos y suministrados por la misma compañía. En otros casos los empleados utilizan su propio dispositivo como herramienta de trabajo, promoviendo así la tendencia conocida como BYOD (Bring your own device / Traiga su propio dispositivo). Todo lo anterior representa un reto de gestión importante para los administradores de IT, ya que en muchos casos deben responsabilizarse de la configuración de estos dispositivos móviles, bien sea para facilitar su ingreso al ambiente empresarial, para instalar las aplicaciones requeridas, para establecer restricciones de uso o para proteger la información corporativa en caso de pérdida o hurto del móvil, entre otras

1.1. Qué es Aranda Enterprise Mobility Management

Aranda EMM es una solución creada para enfrentar los retos de gestión de dispositivos móviles en empresas de cualquier tamaño, de una manera simple y eficiente, desde una consola única de administración. Aranda EMM permite realizar inventarios de software y hardware de los dispositivos móviles usados en la compañía, almacena datos de localización, información de red, históricos de eventos, información de estado (dispositivos rooteados, nivel de batería, espacio disponible, etc.). El administrador de IT podrá enviar a los móviles la configuración inicial requerida para que puedan ser usados apropiadamente: Acceso a redes Wifi, correo electrónico del empleado, aplicaciones necesarias para el trabajo, restricciones para asegurar un buen uso del dispositivo, listados de aplicaciones requeridas/prohibidas, políticas de contraseña, etc. Aranda EMM permite también aplicar reglas de comportamiento a los móviles, con las cuales se monitorean eventos relevantes como el ingreso o salida de zonas geográficas, estados del móvil, cumplimiento de políticas o desvinculación del sistema. De acuerdo a estas condiciones se ejecutan de forma automática acciones como el envío de correo o cambio de políticas. Se permite el envío de comandos manuales sobre los móviles, como bloqueo, cambio de contraseña, envío de notificaciones de texto y borrado completo. Los dispositivos ingresan al sistema mediante un proceso de vinculación muy sencillo, el cual puede ser monitoreado desde la consola web de administración

Con Aranda EMM las empresas podrán sacar más provecho de sus recursos de cómputo y podrán brindar a sus empleados un entorno confiable para usar sus dispositivos móviles en el trabajo. Soportando tabletas y teléfonos celulares de sistemas operativos Android y iOS.

1.2. Requisitos de Sistema

Los siguientes requerimientos se definen para la implementación de Aranda EMM en una instalación On Premise con hasta 200 equipos. Para un número mayor de dispositivos por favor comunicarse con Aranda Software.

Servidor de Aplicaciones – Consola AEMM	
Sistema Operativo	Windows Server® 2008/2012/2019 Standard Edition o superior, x64, con las últimas versiones de SP Instaladas
Memoria RAM	4 GB
Procesador	Intel Xeon > 3.16 GHz, 4MB Cache, Turbo, HT de 1 Core (o equivalente)
Discos Duros	DD 0 (RAID 10): Partición C: 100 GB (SO) DD 1 (RAID 10): Partición D: 30 GB (App y Web) <hr/> Notas: <ul style="list-style-type: none"> • Los discos duros pueden estar dentro del servidor o accesibles a él a través de una SAN (Storage Area Network). • Se recomienda que los Discos Duros sean SSD o SAS de 15.000 RPM.

<p>Requerimientos Adicionales</p>	<ul style="list-style-type: none"> • Internet Information Services 7.0/7.5/8.0/8.5/10/10.0 • Microsoft .NET Framework 4.7.2 con las últimas actualizaciones. • Certificado SSL emitido por una entidad certificadora reconocida. • Roles necesarios: <ul style="list-style-type: none"> ○ Web Server (IIS) <ul style="list-style-type: none"> ▪ Web Server <ul style="list-style-type: none"> • Common HTTP Features <ul style="list-style-type: none"> ○ Default Document ○ HTTP Errors ○ Static Content • Health and Diagnostics <ul style="list-style-type: none"> ○ HTTP Logging • Performance <ul style="list-style-type: none"> ○ Static Content Compression • Security <ul style="list-style-type: none"> ○ Request Filtering • Application Development <ul style="list-style-type: none"> ○ .NET Extensibility 3.5 ○ .NET Extensibility 4.6 ○ ASP ○ ASP .NET 3.5 ○ ASP .NET 4.6 ○ ISAPI Extensions ○ ISAPI Filters ○ WebSocket Protocol • Características necesarias: <ul style="list-style-type: none"> ○ .NET Framework 3.5 Features <ul style="list-style-type: none"> ▪ .NET Framework 3.5 (includes .NET 2.0 and 3.0) ○ .NET Framework 4.6 Features <ul style="list-style-type: none"> ▪ .NET Framework 4.6 ▪ ASP .NET 4.6
---------------------------------------	---

	<ul style="list-style-type: none"> ▪ WCF Services <ul style="list-style-type: none"> • HTTP Activation • Message Queuing • Named Pipe Activation • TCP Activation • TCP Port Sharing
Notas	<p>En caso de virtualizar este servidor, se recomienda reservar los recursos físicos en relación 1:1 con respecto a los recursos virtuales (Resource Allocation). Esta recomendación aplica para Memoria RAM, Procesador y Discos Duros.</p>

Servidor de Base de Datos	
Sistema Operativo	Windows Server®2008/2012/2019 Standard Edition o superior, x64, con las últimas versiones de SP Instaladas
Memoria RAM	6 GB Nota: se debe configurar SQL para que solo consuma 4GB y dejar el resto de la capacidad disponible para el sistema operativo.
Procesador	Intel Xeon > 3.0 GHz, > 6 MB Cache, Turbo, HT de 2 Core o superior.

Discos Duros	<p>DD 0 (RAID 1): Partición C: 100 GB (SO, Transaction Log LDF) DD 1 (RAID 10): Partición D: 10 GB (Data Files MDF)</p> <hr/> <p>Notas:</p> <ul style="list-style-type: none"> - Siendo un poco más costosa la opción 1 es la más recomendada, ya que su funcionamiento es mucho más rápido para las operaciones de lecturas y escrituras aleatorias en los MDF y para las lecturas y escrituras secuenciales en los LDF. - Los discos duros pueden estar dentro del servidor o accesibles a él a través de una SAN (Storage Area Network). - Para propuestas de Cluster deben contar con un almacenamiento compartido. - Se recomienda que los Discos Duros sean SSD o SAS de 15.000 RPM. - El espacio en GB es el requerido y puede ser aumentado en cualquiera de las 3 opciones.
SQL Server	<p>Microsoft SQL Server 2012/2014/2016/2017/2019 Standar o Enterprise. Instalación con: Full Text Search y Autenticación Mixta. Compatibilidad con Azure SQL.</p>
Requerimientos Adicionales	<ul style="list-style-type: none"> • Garantizar conectividad desde el servidor de aplicaciones hacia el servidor de base de datos.

Notas	<p>En caso de virtualizar este servidor, se recomienda reservar los recursos físicos en relación 1:1 con respecto a los recursos virtuales (Resource Allocation). Esta recomendación aplica para Memoria RAM, Procesador y Discos Duros En caso de virtualizar este servidor, no se recomienda crear los discos virtuales usando aprovisionamiento Liviano (Thin Provisioning)</p>
--------------	--

Dispositivos móviles

Sistema Operativo	Versiones	
Android	Vinculación Genérica	4.2+
	Vinculación con Android For Work	5.0+
Android en Dispositivos Samsung (Knox)	Android 4.2+ Knox 6+	
iOS	iPhone 5 o Superior con iOS 8+ iPad 2 o superior con iOS 8+	
Windows	Windows 10 Pro 1709+	

Navegadores de Internet para consola WEB
Internet Explorer 10+
Mozilla Firefox 28+
Google Chrome 33+

Requerimientos de Red		
Entorno	Requerimiento	Justificación
Servidor de Aplicaciones	Puerto 443 TCP (Entrada)	Conexión de usuarios de consola y dispositivos móviles
	Puertos 389.636 (Salida)	Acceso al servidor LDAP en la Intranet, en el caso de usar la funcionalidad de sincronización con el directorio activo de la empresa
	Puertos 25, 587 (Salida)	Acceso al servidores de envío de correo electrónico

	Puerto 443 (Salida) hacia el dominio arandapush1.arandasoft.com	Envío de notificaciones push hacia dispositivos móviles
Todos los Dispositivos	Puerto 443 hacia Servidor de aplicaciones	Conexión a consola de administración
Dispositivos Windows	Salida a los dominios *.notify.windows.com, *.wns.windows.com, *.notify.live.net	Conexión al servicio de notificaciones push para windows
Dispositivos iOS	Puerto 5223 (Salida) hacia direcciones en el formato 17.*.*.*	Conexión al servicio de notificaciones push para iOS
Dispositivos Android	Puertos 5228, 5229, 5230 hacia dominios android.googleapis.com, gcm- http.googleapis.com, fcm- http.googleapis.com	Conexión al servicio de notificaciones push para android, tienda de google play y plataforma de Android for Work
Estación de trabajo de usuario de Consola AEMM	Puerto 443 (Salida) hacia el servidor de aplicaciones	Conexión a la consola de administración
	Puerto 443 (Salida) hacia el dominio c.tile.openstreetmap.org	Presentación de mapas en Open Street Maps

2. INSTALACIÓN

El instalador comienza a extraer los archivos necesarios y a preparar el proceso



De clic en **siguiente** para continuar con la instalación.



Ingrese el nombre de usuario y la organización. De clic en **siguiente**:

Aranda Mobile Device Management - InstallShield Wizard

Información del cliente

Por favor, introduzca la información.

Nombre de usuario:
User

Organización:
User Enterprise

InstallShield

< Atrás Siguiente > Cancelar

Seleccione el tipo de instalación completa.

Aranda Mobile Device Management - InstallShield Wizard

Tipo de instalación

Elija el tipo de instalación que se adapte mejor a sus necesidades.

Seleccione un tipo de instalación.

Completa
Se instalarán todos los componentes del programa. (Necesita más espacio en disco).

Personalizada
Elija los componentes del programa que desee instalar y la ubicación en que se instalarán. Recomendada para usuarios avanzados.

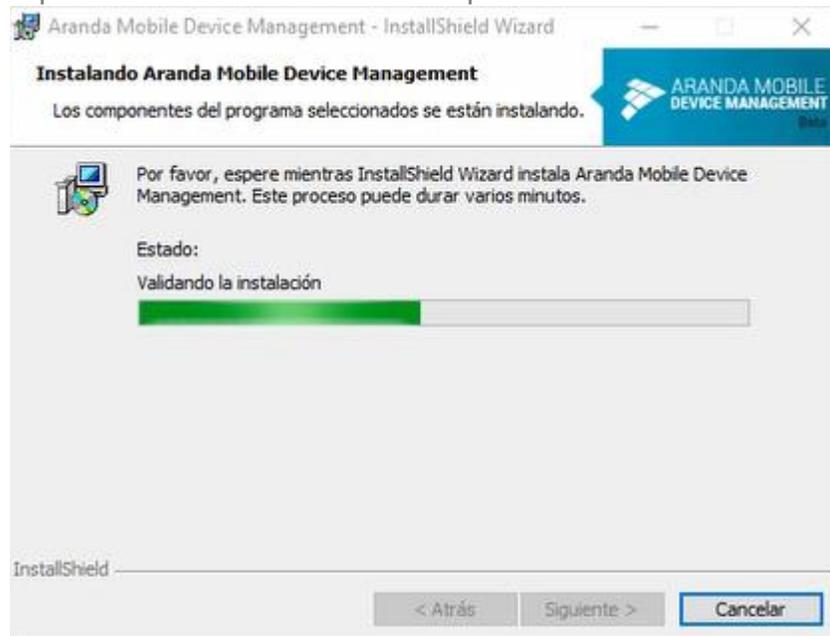
InstallShield

< Atrás Siguiente > Cancelar

De clic en **Instalar**



Espera a que el proceso de instalación se complete



Seleccione finalizar para terminar el proceso de instalación



2.1. Configuración de Base de datos y Servicios Windows

Para la creación o actualización de la base de datos y las respectivas conexiones desde las aplicaciones, así como la gestión de los servicios Windows es necesario utilizar la herramienta **Aranda Database Tools** suministrada por Aranda Software.

Para más información sobre **Aranda Database Tools** referirse a la siguiente dirección de internet:

<http://corp.arandasoft.com:5554/kb2/KnowledgebaseArticle10224.aspx>

2.2. Configuración de Licenciamiento

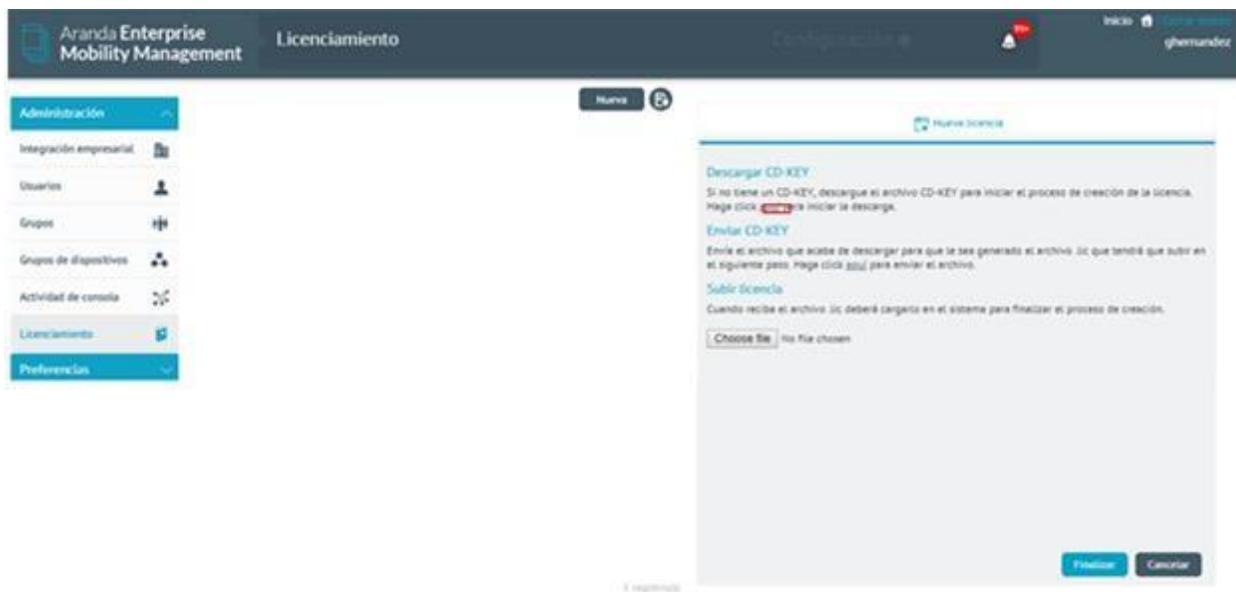
Todos los productos de Aranda Software necesitan de una licencia para su funcionamiento, razón por la cual, la primera vez que ingrese a Aranda EMM se le solicitará una licencia.

A continuación:

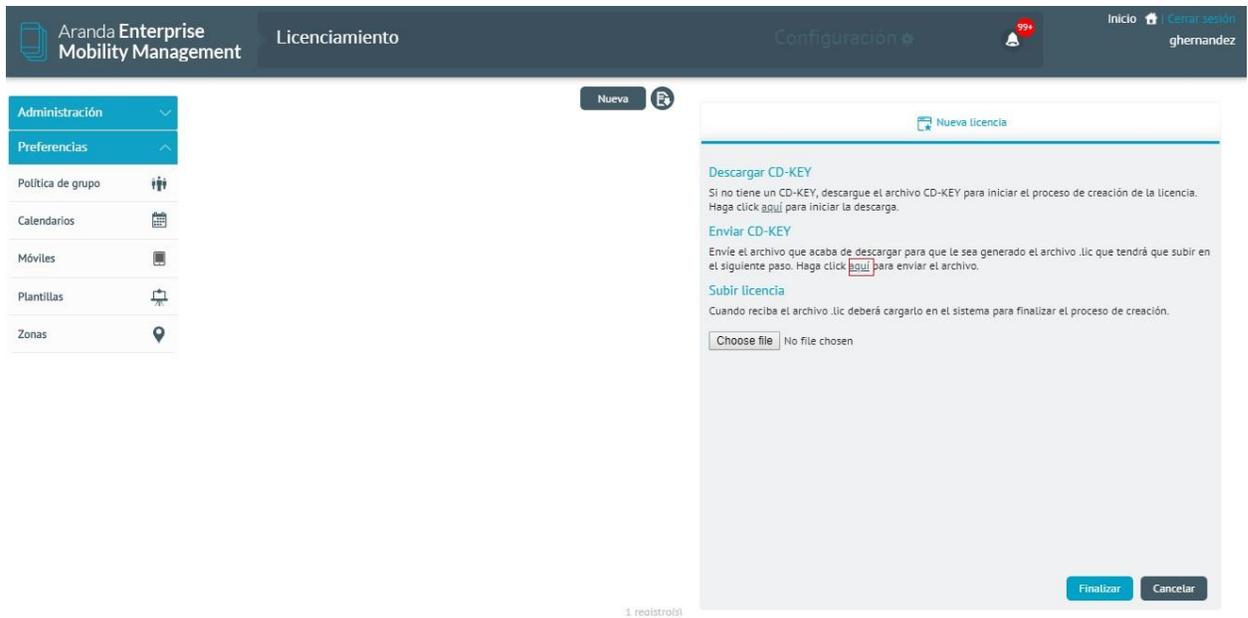
De clic en la opción **Nueva**



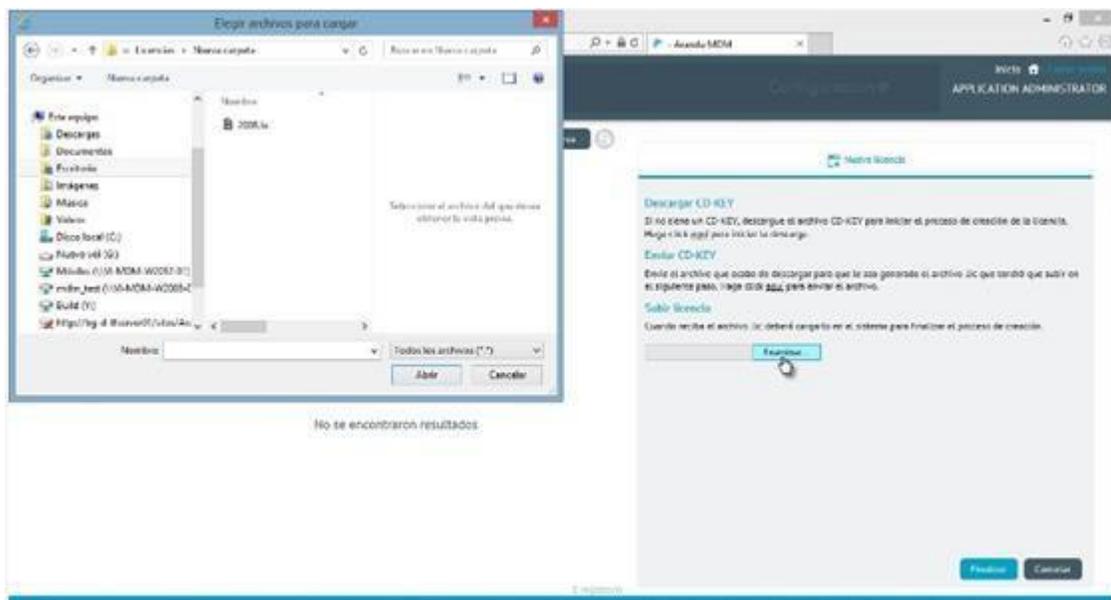
Descargar el Machine – KEY



Envíe vía correo electrónico el Machine -KEY a su representante en Aranda Software



Seleccione la licencia que recibió a través del correo electrónico



Y de clic en la opción **finalizar**.

Aranda Enterprise Mobility Management Licenciamiento Configuración Inicio Cerrar sesión ghernandez

Nueva

Nueva Licencia

Descargar CD-KEY
Si no tiene un CD-KEY, descargue el archivo CD-KEY para iniciar el proceso de creación de la licencia. Haga click [aquí](#) para iniciar la descarga.

Enviar CD-KEY
Envíe el archivo que acaba de descargar para que le sea generado el archivo .lic que tendrá que subir en el siguiente paso. Haga click [aquí](#) para enviar el archivo.

Subir licencia
Cuando reciba el archivo .lic deberá cargarlo en el sistema para finalizar el proceso de creación.

Choose file No file chosen

Finalizar Cancelar

De este modo, la licencia se carga exitosamente

Aranda Enterprise Mobility Management Licenciamiento Configuración Inicio Cerrar sesión ghernandez

Nueva

Aranda MOBILE DEVICE MANAGEMENT

Tipo: Demo
Fecha de expiración: 07/12/2019

General Usuarios nombrados

Compañía	Aranda Software	Producto	Aranda MOBILE DEVICE MANAGEMENT
Tipo	Demo	Fecha de expiración	07/12/2019
Usuarios nombrados	10	Usuarios nombrados disponibles	10
Usuarios concurrentes	10	Número de dispositivos	50

1 registro(s)

En la licencia se visualizarán la fecha de expiración, usuarios nombrados, usuarios concurrentes y el número de dispositivos permitidos

Aranda Enterprise Mobility Management Licenciamiento Configuración Inicio Cerrar sesión ghernandez

Administración Preferencias Política de grupo Calendarios Móviles Plantillas Zonas

Aranda MOBILE DEVICE MANAGEMENT Tipo: Demo Fecha de expiración: 07/12/2019

General Usuarios nombrados

Compañía	Aranda Software	Producto	Aranda MOBILE DEVICE MANAGEMENT
Tipo	Demo	Fecha de expiración	07/12/2019
Usuarios nombrados	10	Usuarios nombrados disponibles	10
Usuarios concurrentes	10	Número de dispositivos	50

1 registros

Los Usuarios nombrados son las licencias que siempre tendrán acceso a la consola. Para agregar este tipo de usuarios se debe ingrese a la pestaña **usuarios nombrados** y adiciónelos.

Aranda Enterprise Mobility Management Licenciamiento Configuración Inicio Cerrar sesión ghernandez

Administración Preferencias Política de grupo Calendarios Móviles Plantillas Zonas

Aranda MOBILE DEVICE MANAGEMENT Tipo: Demo Fecha de expiración: 07/12/2019

General Usuarios nombrados

Buscar usuarios

No hay usuarios nombrados asociados a esta licencia.

Guardar Cancelar

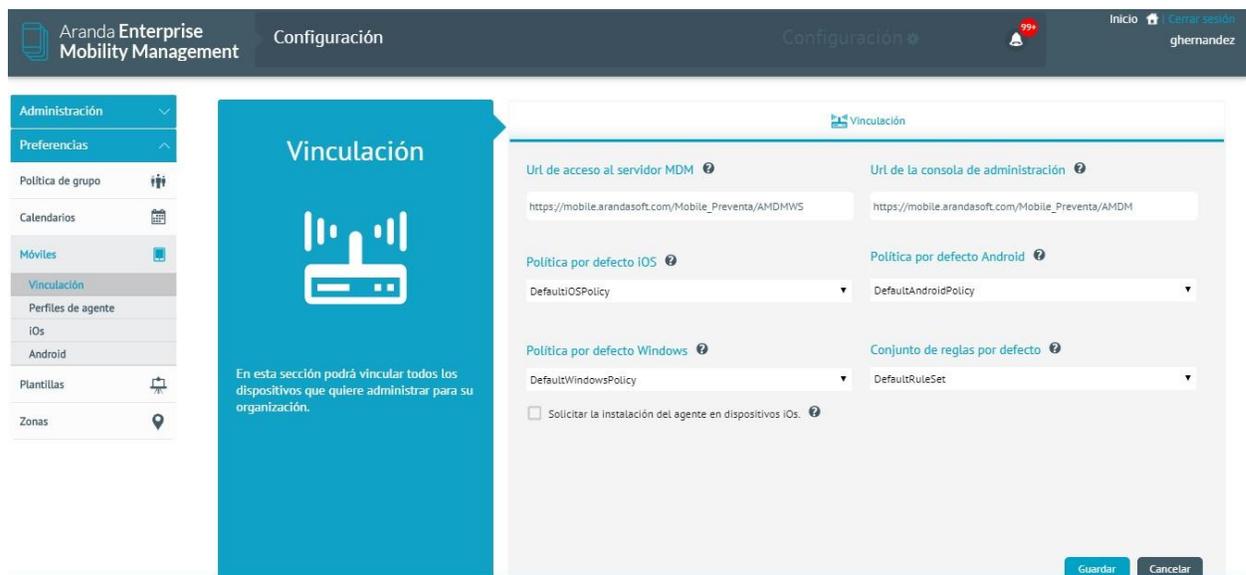
1 registros

2.3. Configuración Inicial

Para configurar Aranda EMM es necesario tener en cuenta lo siguiente:

Configuración de las URLS para acceso a la consola y el servidor.

- URL de acceso al servidor MDM: Se utiliza para la comunicación con los dispositivos móviles.
- URL de la consola de administración: Permite que el usuario acceda al proceso de vinculación desde el dispositivo y pueda gestionar su vinculación. (Para más información. Ver [3.2 Vinculación](#))



The screenshot shows the 'Vinculación' configuration page in the Aranda Enterprise Mobility Management console. The page includes a sidebar with navigation options like 'Administración', 'Preferencias', 'Política de grupo', 'Calendarios', 'Móviles', 'Vinculación', 'Perfiles de agente', 'iOS', 'Android', 'Plantillas', and 'Zonas'. The main content area is titled 'Vinculación' and contains the following configuration fields:

- Url de acceso al servidor MDM:** `https://mobile.arandasoft.com/Mobile_Preventa/AMDMWS`
- Url de la consola de administración:** `https://mobile.arandasoft.com/Mobile_Preventa/AMDM`
- Política por defecto iOS:** DefaultiOSPolicy
- Política por defecto Android:** DefaultAndroidPolicy
- Política por defecto Windows:** DefaultWindowsPolicy
- Conjunto de reglas por defecto:** DefaultRuleSet
- Solicitar la instalación del agente en dispositivos iOS.

Buttons for 'Guardar' (Save) and 'Cancelar' (Cancel) are located at the bottom right of the configuration area.

3. ADMINISTRACIÓN

3.1. Integración empresarial

3.1.1. Configuración de Correo

Requerimiento para el envío de correos. El usuario debe ingresar:

- SMTP: Nombre del servidor que permite el transporte del email en la Internet.
- Usuario: Nombre de usuario utilizado para para conectar con el SMTP.
- Contraseña: Contraseña para conectar al SMTP.
- Habilitar SSL: Activar/Desactivar la opción del certificado SSL.
- Remitente: Dirección de correo electrónico para enviar las notificaciones
- Nombre del remitente: Nombre que aparecerá en las notificaciones de correo.
- Puerto: Número de puerto por el que se conectara al SMTP.

Aranda Enterprise Mobility Management Integración empresarial Configuración Inicio | Cerrar sesión ricardo.chicangana

Administración Integración empresarial Usuarios Grupos Grupos dinámicos Actividad de consola Licenciamiento Preferencias

Correo Directorio empresarial Conexión con CMDB

Esta sección le permitirá configurar una cuenta de email que será usada para enviar los correos de vinculación a los usuarios

SMTP ?	Usuario ?
outlook.office365.com	mdm@arandasoft.com
Contraseña ?	Habilitar SSL ?
.....	<input checked="" type="checkbox"/> Habilitar
Remitente ?	Nombre del remitente ?
mdm@arandasoft.com	Aranda EMM
Puerto ?	
587	

Probar configuración Guardar Cancelar

Luego de hecha la anterior configuración, ésta se puede probar enviando un correo de prueba haciendo clic en el botón “Probar Configuración”. Una vez pulsado el botón se solicitará una dirección de correo destinatario donde se recibirá un correo de prueba enviando desde el servidor AEMM.

Aranda Enterprise Mobility Management Integración empresarial Configuración Inicio | Cerrar sesión ricardo.chicangana

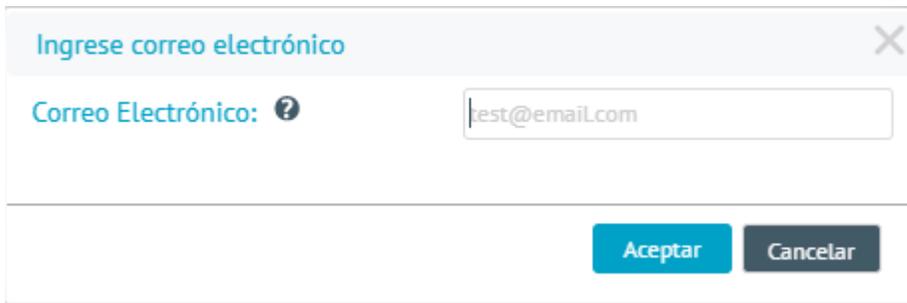
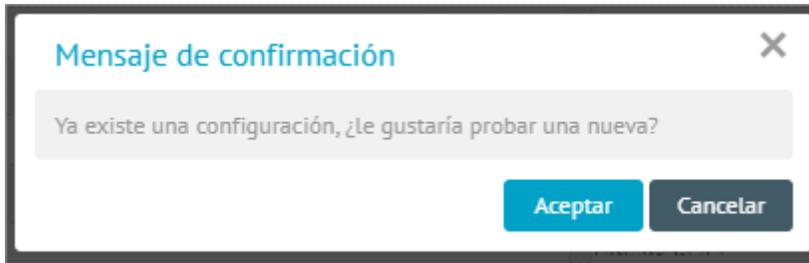
Administración Integración empresarial Usuarios Grupos Grupos dinámicos Actividad de consola Licenciamiento Preferencias

Correo Directorio empresarial Conexión con CMDB

Esta sección le permitirá configurar una cuenta de email que será usada para enviar los correos de vinculación a los usuarios

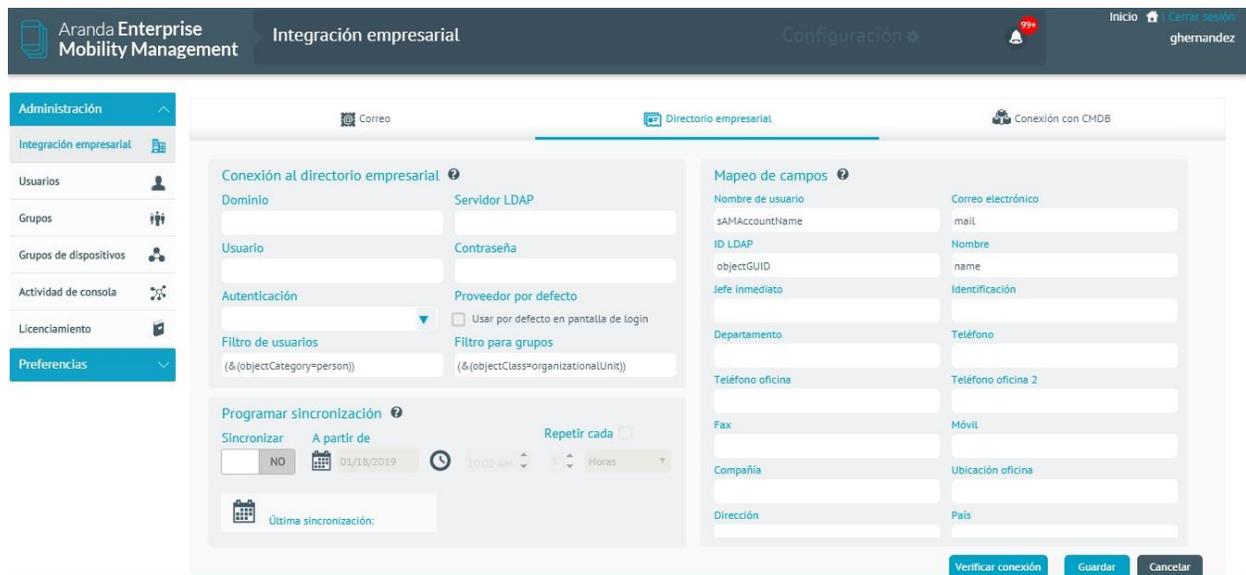
SMTP ?	Usuario ?
outlook.office365.com	mdm@arandasoft.com
Contraseña ?	Habilitar SSL ?
....	<input checked="" type="checkbox"/> Habilitar
Remitente ?	Nombre del remitente ?
mdm@arandasoft.com	Aranda EMM
Puerto ?	
587	

Probar configuración Guardar Cancelar



3.1.2. Configuración de Directorio Empresarial

Ingrese los datos para conectar con su directorio empresarial.

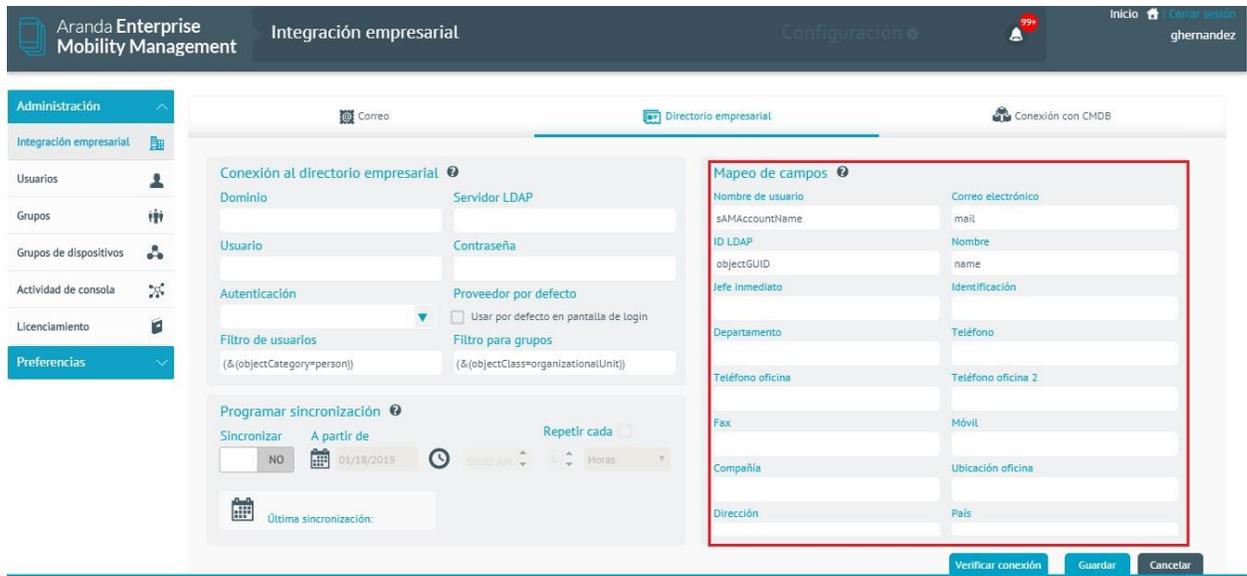


Para acceder a la información de usuarios y grupos del directorio activo de su compañía, es necesario ingresar los siguientes datos.

- Conexión al directorio empresarial: Información para conectar con el directorio activo.

- Programar sincronización: La programación para la sincronización de usuarios o grupos desde el directorio empresarial.

- Mapeo de campos: Asignación de correspondencia de campos para mapear información de los usuarios desde el directorio empresarial.

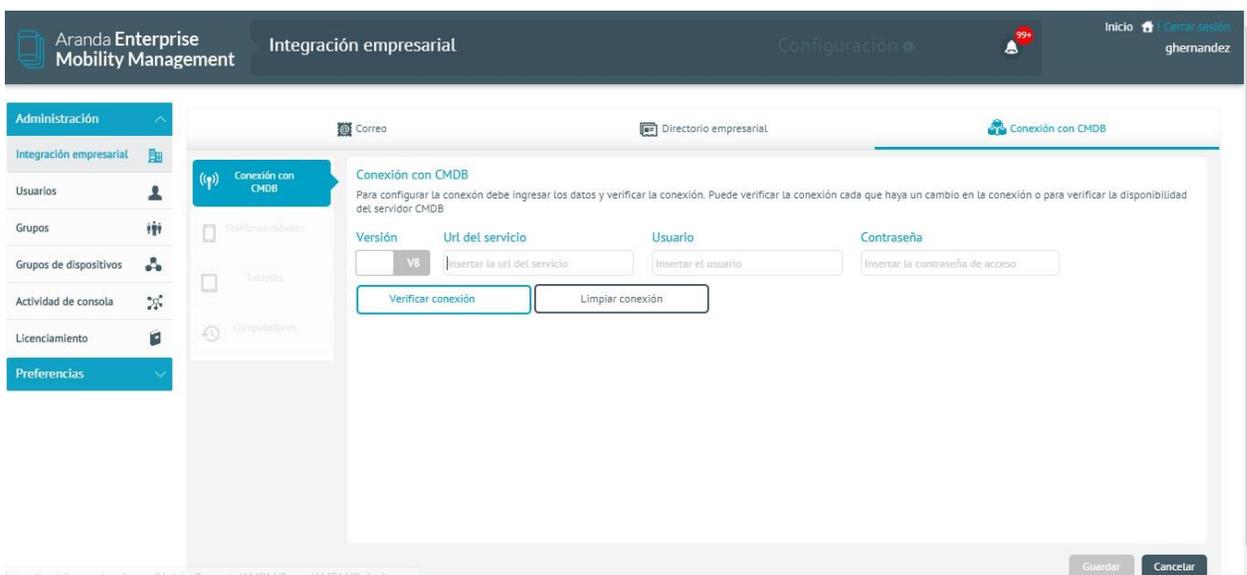


La consola de administración de AEMM brinda la posibilidad de importar usuarios o grupos, con el fin de evitar sincronizar todo el directorio activo cuando se desea incluir un número limitado de usuarios o grupos.

3.1.3. Configuración conexión con CMDB

Ingrese los datos para conectar con la CMDB deseada y de clic en la opción "**Verificar Conexión**". Url del servicio: Debe ingresar la dirección URL de la API CMDB.

- Usuario: El usuario de ingreso a la CMDB.
- Contraseña: El password asociado al usuario de CMDB.



Ahora de clic en la opción **Guardar**.

Aranda Enterprise Mobility Management Integración empresarial Configuración Inicio Cerrar sesión gherandez

Administración Integración empresarial Usuarios Grupos Grupos de dispositivos Actividad de consola Licenciamiento Preferencias

Correo Directorio empresarial **Conexión con CMDB**

Conexión con CMDB
 Para configurar la conexión debe ingresar los datos y verificar la conexión. Puede verificar la conexión cada que haya un cambio en la conexión o para verificar la disponibilidad del servidor CMDB

Versión: VB Url del servicio: http://preventaco.arandasoft.com/CMD Usuario: gherandez Contraseña: *****

Verificar conexión Limpiar conexión

Guardar Cancelar

Seleccione los campos de los activos (CIs) que desea mapear y realice el mapeo de los campos adicionales de la CMDB con los de Aranda EMM.

Aranda Enterprise Mobility Management Integración empresarial Configuración Inicio Cerrar sesión gherandez

Administración Integración empresarial Usuarios Grupos Grupos de dispositivos Actividad de consola Licenciamiento Preferencias

Correo Directorio empresarial **Conexión con CMDB**

Conexión con CMDB
 Para configurar la conexión debe ingresar los datos y verificar la conexión. Puede verificar la conexión cada que haya un cambio en la conexión o para verificar la disponibilidad del servidor CMDB

Versión: VB Url del servicio: Insertar la url del servicio Usuario: Insertar el usuario Contraseña: Insertar la contraseña de acceso

Verificar conexión Limpiar conexión

Guardar Cancelar

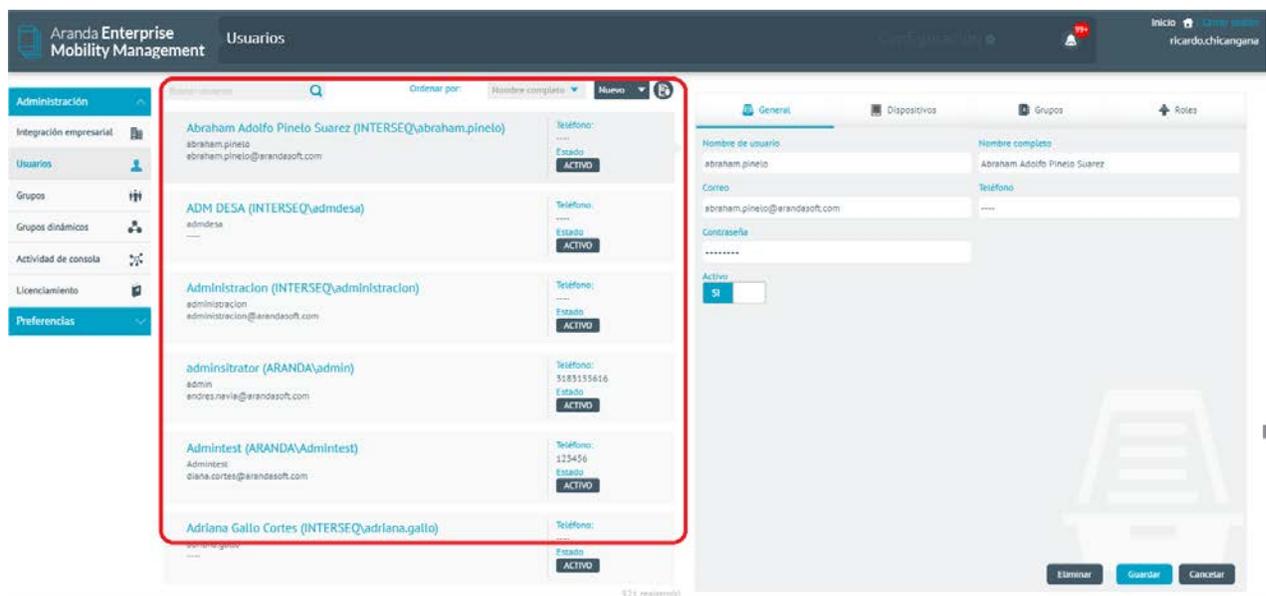
3.2. Usuarios

Usuarios Aranda EMM (Consola, Móvil)

Se conocen dos tipos de usuarios en AEMM; los de consola y los usuarios móviles. Los usuarios de consola son aquellos que pueden intervenir y monitorear los dispositivos móviles que se registren en la consola y los usuarios móviles son los que se vinculan en la consola con su dispositivo móvil pero nunca tienen una administración directa en la consola.

3.2.1. Listado de usuarios

Al acceder a la sección de usuarios se presenta un listado paginado con scroll infinito de los usuarios existentes en el sistema.



En la parte superior del listado se presentan los siguientes controles:

Búsqueda: Permite la búsqueda básica de usuarios, por su nombre de usuario o su nombre completo.

Ordenación: Permite ordenar el listado por los campos; nombre completo, nombre de usuario y correo; de manera ascendente y descendente.

Nuevo: Permite la creación e importación de nuevos usuarios.

Exportación: Permite la exportación del listado a archivo Excel descargable.

The screenshot displays the 'Usuarios' (Users) management interface. On the left, there is a sidebar with navigation options: Administración, Integración empresarial, Usuarios, Grupos, Grupos dinámicos, Actividad de consola, Licenciamiento, and Preferencias. The main area shows a list of users with columns for 'Nombre completo', 'Nombre de usuario', 'Correo', 'Teléfono', and 'Estado'. A red box highlights the search bar and the 'Nuevo' button. On the right, a detailed view of a user is shown, including fields for 'Nombre de usuario', 'Nombre completo', 'Correo', 'Teléfono', and 'Contraseña', along with an 'Activado' checkbox.

Por cada usuario se presenta un registro en el listado que contiene la siguiente información:

- **Nombre completo:** Nombre completo del usuario
- **Nombre de usuario:** Nombre de usuario usado para autenticarse ante el sistema
- **Correo:** Correo electrónico del usuario, usado para el envío de notificaciones del sistema
- **Teléfono:** Número telefónico del usuario
- **Estado:** Estado el usuario ante el sistema, puede ser Activo o Inactivo

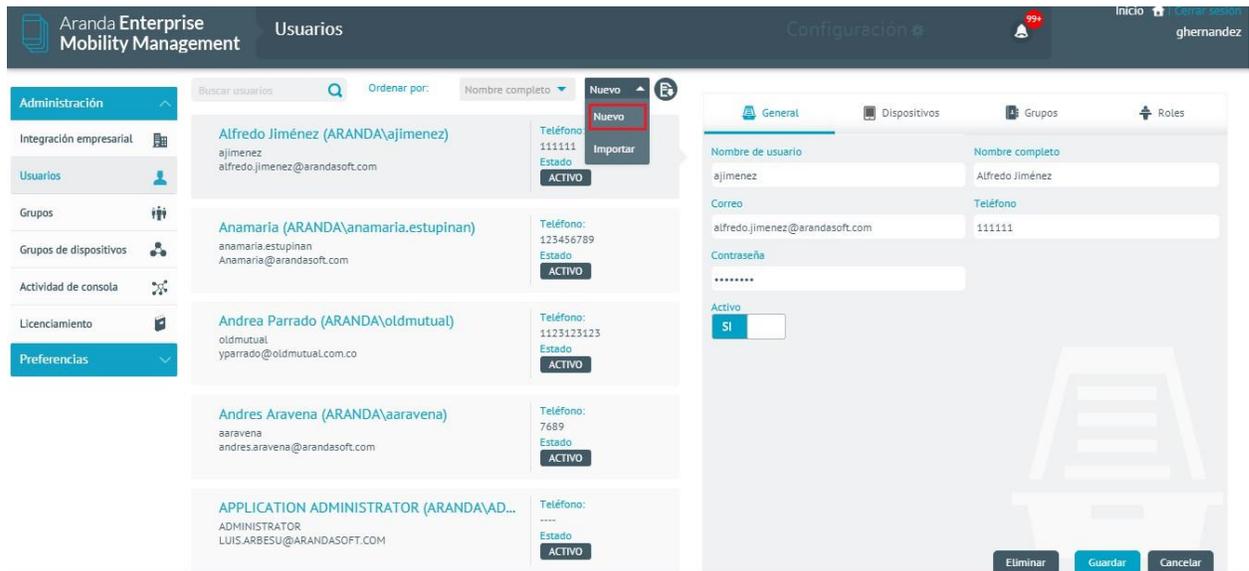
The detailed view shows the following information for the user 'User Test (ARANDA\usertest)':

- Nombre completo:** User Test (ARANDA\usertest)
- Nombre de usuario:** usertest
- Correo:** ricardo.chicangana@arandasoft.com
- Teléfono:** 310
- Estado:** ACTIVO

3.2.2. Creación de usuario nuevo

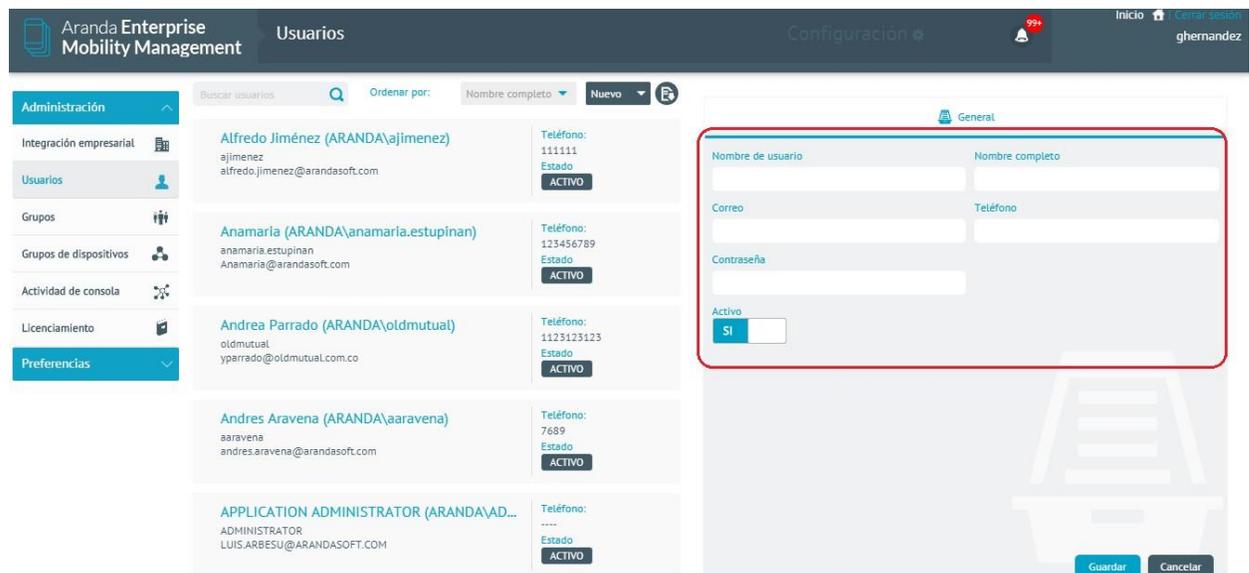
Los usuarios de consola son creados como usuarios locales y se hacen necesarios cuando estos no se obtienen del directorio activo, a este tipo de usuarios les es permitido realizar modificaciones a su información.

Para crear un usuario ingrese a **configuración** > luego a **usuarios** y de clic en **Nuevo**



The screenshot shows the 'Usuarios' management interface. On the left is a navigation menu with options like 'Administración', 'Usuarios', 'Grupos', etc. The main area displays a list of users. The 'Nuevo' button is highlighted with a red box. On the right, a 'General' configuration form is visible, containing fields for 'Nombre de usuario', 'Nombre completo', 'Correo', 'Teléfono', 'Contraseña', and an 'Activo' checkbox.

Ingrese la información requerida:



This screenshot shows the same 'Usuarios' page, but the 'General' configuration form on the right is highlighted with a red box. The form contains the following fields: 'Nombre de usuario', 'Nombre completo', 'Correo', 'Teléfono', 'Contraseña', and an 'Activo' checkbox with a 'SI' button next to it. At the bottom of the form are 'Guardar' and 'Cancelar' buttons.

De clic en **Guardar**

Aranda Enterprise Mobility Management Usuarios

Configuración Inicio Cerrar sesión ghernandez

Administración

Integración empresarial

Usuarios

Grupos

Grupos de dispositivos

Actividad de consola

Licenciamiento

Preferencias

Buscar usuarios

Ordenar por: Nombre completo

Nuevo

<p>Alfredo Jiménez (ARANDA\ajimenez)</p> <p>ajimenez alfredo.jimenez@arandasoft.com</p> <p>Teléfono: 1111111 Estado: ACTIVO</p>	<p>Anamaria (ARANDA\anamaria.estupinan)</p> <p>anamaria.estupinan Anamaria@arandasoft.com</p> <p>Teléfono: 123456789 Estado: ACTIVO</p>
<p>Andrea Parrado (ARANDA\oldmutual)</p> <p>oldmutual yparrado@oldmutual.com.co</p> <p>Teléfono: 1123123123 Estado: ACTIVO</p>	<p>Andres Aravena (ARANDA\aaravena)</p> <p>aaravena andres.aravena@arandasoft.com</p> <p>Teléfono: 7689 Estado: ACTIVO</p>
<p>APPLICATION ADMINISTRATOR (ARANDA\AD...)</p> <p>ADMINISTRATOR LUIS.ARBESU@ARANDASOFT.COM</p> <p>Teléfono: ---- Estado: ACTIVO</p>	

General

Nombre de usuario

Nombre completo

Correo

Teléfono

Contraseña

Activo

SI

Guardar Cancelar

Los usuarios se pueden almacenar como activos e inactivos. (Si el usuario se encuentra inactivo no tiene interacción con ningún proceso)

Aranda Enterprise Mobility Management Usuarios

Configuración Inicio Cerrar sesión ghernandez

Administración

Integración empresarial

Usuarios

Grupos

Grupos de dispositivos

Actividad de consola

Licenciamiento

Preferencias

Buscar usuarios

Ordenar por: Nombre completo

Nuevo

<p>Alfredo Jiménez (ARANDA\ajimenez)</p> <p>ajimenez alfredo.jimenez@arandasoft.com</p> <p>Teléfono: 1111111 Estado: ACTIVO</p>	<p>Anamaria (ARANDA\anamaria.estupinan)</p> <p>anamaria.estupinan Anamaria@arandasoft.com</p> <p>Teléfono: 123456789 Estado: ACTIVO</p>
<p>Andrea Parrado (ARANDA\oldmutual)</p> <p>oldmutual yparrado@oldmutual.com.co</p> <p>Teléfono: 1123123123 Estado: ACTIVO</p>	<p>Andres Aravena (ARANDA\aaravena)</p> <p>aaravena andres.aravena@arandasoft.com</p> <p>Teléfono: 7689 Estado: ACTIVO</p>
<p>APPLICATION ADMINISTRATOR (ARANDA\AD...)</p> <p>ADMINISTRATOR LUIS.ARBESU@ARANDASOFT.COM</p> <p>Teléfono: ---- Estado: ACTIVO</p>	

General

Nombre de usuario

Nombre completo

Correo

Teléfono

Contraseña

Activo

SI

Guardar Cancelar

En el detalle de cada usuario se pueden encontrar las secciones de General, Dispositivos, Grupos y Roles que se describen a continuación.

3.2.3. General

Se gestiona información como nombre de usuario, nombre completo, correo, teléfono, y contraseña. El usuario solo se puede eliminar si este no se encuentra asociado a grupos.

The screenshot shows the 'Usuarios' (Users) management interface. On the left is a navigation menu with options like 'Administración', 'Integración empresarial', 'Usuarios', 'Grupos', 'Grupos de dispositivos', 'Actividad de consola', 'Licenciamiento', and 'Preferencias'. The main area displays a list of users with details for 'Alfredo Jiménez (ARANDA\ajimenez)', including phone number (111111), email (ajimenez@arandasoft.com), and status (ACTIVO). On the right, a 'General' tab is active, showing fields for 'Nombre de usuario' (ajimenez), 'Nombre completo' (Alfredo Jiménez), 'Correo' (alfredo.jimenez@arandasoft.com), 'Teléfono' (111111), and 'Contraseña'. There is also an 'Activo' checkbox checked 'SI'. At the bottom right are buttons for 'Eliminar', 'Guardar', and 'Cancelar'.

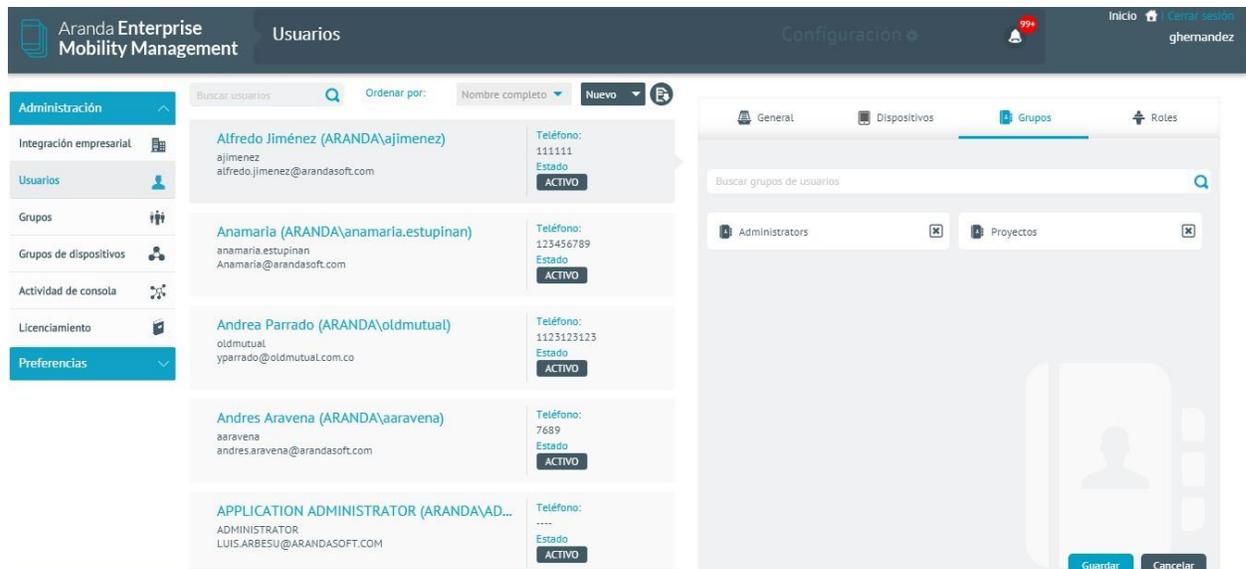
3.2.4. Dispositivos

Se visualizan los dispositivos que el usuario tiene vinculados.

This screenshot shows the same user list as the previous image, but the 'Dispositivos' (Devices) tab is selected for the user 'Alfredo Jiménez'. The device list shows one entry: 'Androidajimenez81' with a 'VER' (View) button next to it. The background of the device list area features a faint image of a smartphone.

3.2.5. Grupos de usuarios

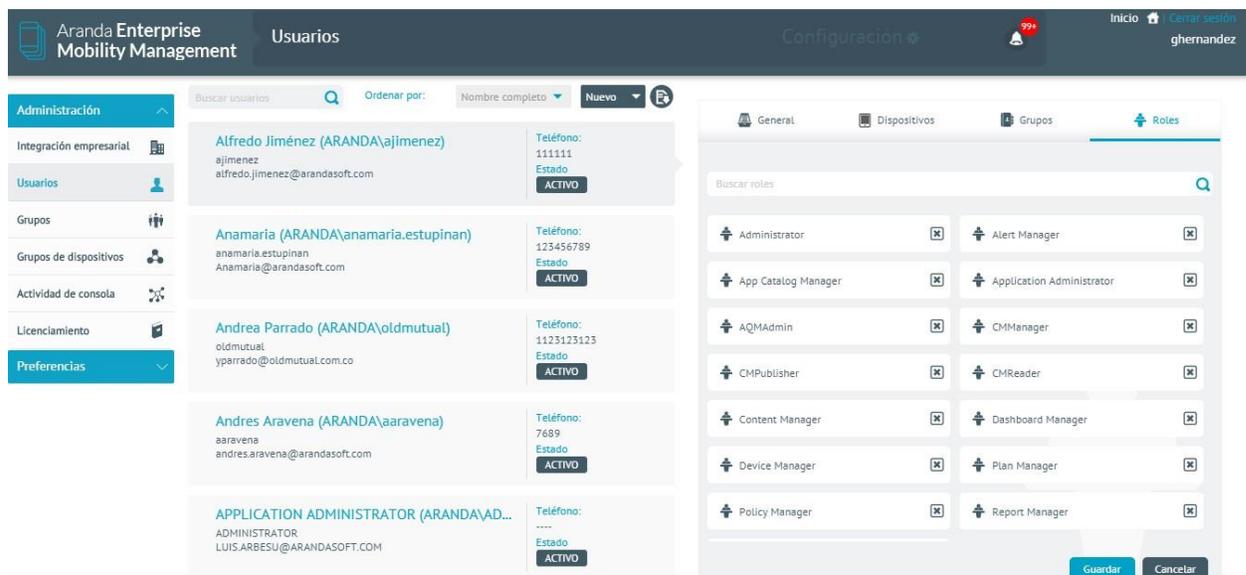
Contiene los grupos a los cuales se encuentra asociado el usuario.



The screenshot shows the 'Usuarios' management page in Aranda Enterprise Mobility Management. The left sidebar contains navigation options like 'Administración', 'Integración empresarial', 'Usuarios', 'Grupos', 'Grupos de dispositivos', 'Actividad de consola', 'Licenciamiento', and 'Preferencias'. The main content area displays a list of users with details such as name, email, phone number, and status (ACTIVE). The right-hand panel is titled 'Grupos' and shows a search bar for user groups, with 'Administrators' and 'Proyectos' listed as selected groups. Buttons for 'Guardar' and 'Cancelar' are visible at the bottom right of the panel.

3.2.6. Roles

Indica los roles o permisos que tiene el usuario para el acceso a la consola. Existen 11 tipos de roles.



This screenshot shows the 'Roles' configuration page for the same user. The left sidebar is identical. The main content area shows a list of roles that can be assigned to the user. The roles listed are: Administrator, Alert Manager, App Catalog Manager, Application Administrator, AQMAAdmin, CMManager, CMPublisher, CMReader, Content Manager, Dashboard Manager, Device Manager, Plan Manager, Policy Manager, and Report Manager. Each role has a plus icon and a checkbox to indicate it is selected. The 'Roles' tab is highlighted in the top navigation bar of the right panel.

Los usuarios también se pueden clasificar como usuarios locales y de directorio activo (Para más información diríjase al apartado [3.1.2 Configuración del directorio empresarial](#)).

3.2.7. Seguridad y control de acceso usando roles

3.2.7.1. Descripción de los distintos tipos de Roles

Para el uso y administración de la consola web se han establecido un conjunto de roles por defecto que permiten segmentar las diferentes funcionalidades disponibles dentro de la consola, creando la posibilidad de permitir o restringir el acceso a cada una de ellas. Existen 11 tipos de roles:

- **Device Manager:** Gestor de dispositivos, tiene permisos para ver, editar y enviar comandos a dispositivos.
- **Device Reader:** Visualizador de dispositivos, tiene permisos para ver información sobre dispositivos.
- **Policy Manager:** Gestor de Políticas, tiene permisos para crear, ver, editar, eliminar y aplicar políticas.
- **Policy Editor:** Editor de políticas, tiene permisos para ver y editar políticas.
- **Policy Reader:** Visualizador de Políticas, tiene permisos para ver información de políticas.
- **Ruleset Manager:** Gestor de conjuntos de reglas, tiene permisos para crear, ver, editar y eliminar conjuntos de reglas.
- **AppCatalog Manager:** Gestor de catálogo de aplicaciones, tiene permisos para importar, ver y eliminar aplicaciones del catálogo.
- **Content Manager:** Gestor de contenidos, tiene permisos para crear, ver, editar y eliminar contenidos.
- **Plan Manager:** Gestor de planes de consumo, tiene permisos para crear, ver, editar, eliminar y aplicar planes de consumo.
- **Settings Manager:** Gestor de configuraciones, tiene permisos para editar y aplicar configuraciones del sistema.
- **Administrator:** Administrador general de la aplicación, tiene todos los permisos de los roles anteriores.

Cada rol tiene asignado un conjunto de permisos que restringen o permiten el acceso a cada funcionalidad, la forma de asociar estos comportamientos a los usuarios de la plataforma es a través de la relación que se puede establecer entre los usuarios y los roles, o entre los roles y los grupos de usuarios (los cuales a su vez están integrados por usuarios que heredan los roles del grupo o grupos al que pertenecen).

Aranda Enterprise Mobility Management Usuarios

Configuración

Inicio [Cerrar sesión](#) ricardo.chicangana

ricardo

Ordenar por: Nombre completo Nuevo

Administración

- Integración empresarial
- Usuarios
- Grupos
- Grupos dinámicos
- Actividad de consola
- Licenciamiento
- Preferencias

Daniel Ricardo Rodriguez Rodriguez (INTERSEQ\danielrodrigu...
 daniel.rodriguez
 daniel.rodriguez@arandasoft.com
 Teléfono: ---
 Estado: ACTIVO

David Ricardo Sanchez Pabon (INTERSEQ\david.sanchez)
 david.sanchez
 david.sanchez@arandasoft.com
 Teléfono: ---
 Estado: ACTIVO

Kevin Ricardo Cordoba Ortiz (INTERSEQ\Kevin.Cordoba)
 Kevin.Cordoba

 Teléfono: ---
 Estado: ACTIVO

Nicolas Ricardo Robles Vargas (INTERSEQ\nicolas.robles)
 nicolas.robles
 nicolas.robles@arandasoft.com
 Teléfono: ---
 Estado: ACTIVO

Ricardo Chicangana Solano (INTERSEQ\ricardo.chicangana)
 ricardo.chicangana
 ricardo.chicangana@arandasoft.com
 Teléfono: ---
 Estado: ACTIVO

William Ricardo Ariza Velez (INTERSEQ\williamariza)
 william.ariza
 william.ariza@arandasoft.com
 Teléfono: ---
 Estado: ACTIVO

General Dispositivos Grupos Roles

Buscar roles

Administrador	AppCatalog Manager
AppCatalogManager	AQAdmin
CHManager	Content Manager
Device Manager	Device Reader
DeviceManager	DistributionManager
PatchManager	Plan Manager
Policy Editor	Policy Manager
Policy Reader	PolicyManager
RulesetManager	Ruleset Manager

Guardar Cancelar

Para la asignación o modificación de los roles que un usuario tiene existen 2 formas:

Asígnelos al usuario directamente o asígnelos a un grupo de usuarios y haga que el usuario pertenezca al grupo.

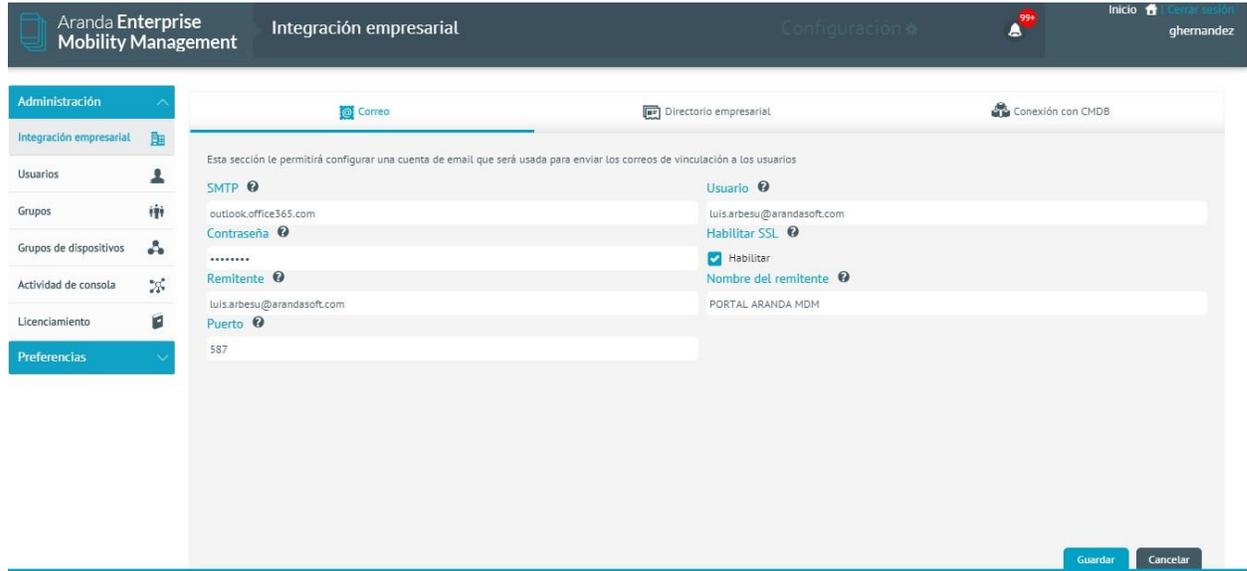
3.2.7.2. Asignación de roles a un usuario

Ingresa a la sección de **configuración** en la parte superior derecha de la consola.

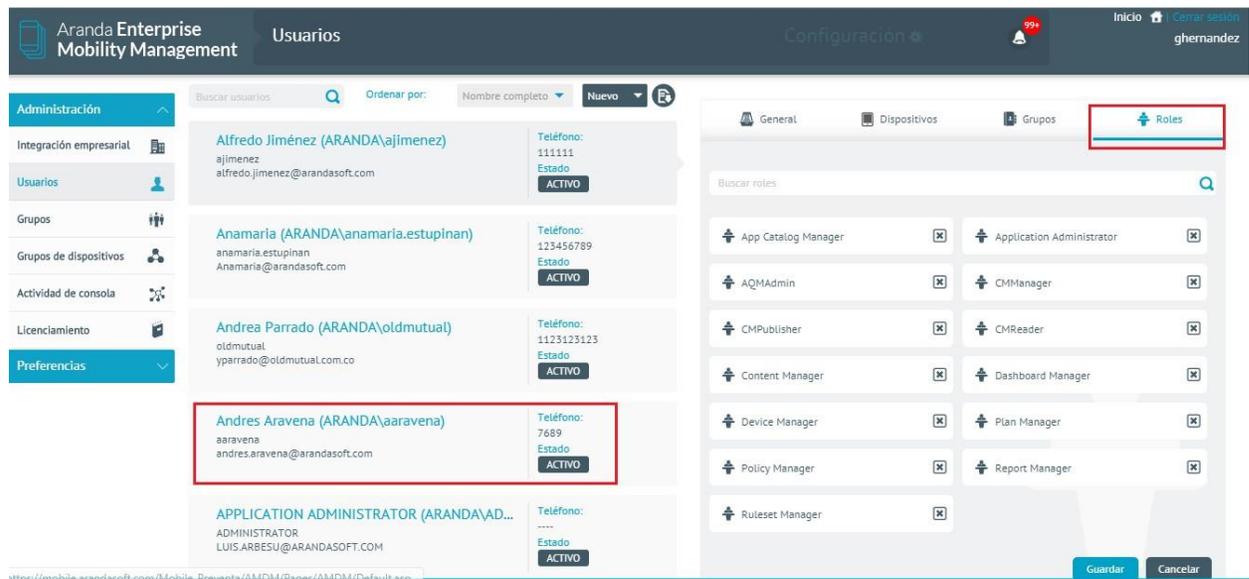
Dashboard Dispositivos Aplicaciones Políticas Reglas Reportes Documentos

Configuración Cerrar sesión ADMINISTRATOR

Luego ingrese a la sección **General** desde el menú Izquierdo y posteriormente a **usuarios**.



Seleccione el usuario dando clic en el listado de usuarios, si es necesario se puede buscar u ordenar el listado de usuarios para facilitar la ubicación del usuario al que se le quiere asignar los roles, luego de clic en la pestaña **roles** del panel derecho.



En la caja de búsqueda se puede ingresar el texto de búsqueda para obtener el rol que se va a asignar al usuario, repita este procedimiento por cada rol y luego de clic en el botón **Guardar**.

The screenshot shows the 'Usuarios' configuration page in Aranda Enterprise Mobility Management. On the left, there is a sidebar with navigation options: Administración, Integración empresarial, Usuarios, Grupos, Grupos de dispositivos, Actividad de consola, Licenciamiento, and Preferencias. The main area displays a list of users with their details (name, phone, email, and status). On the right, there is a 'Roles' assignment panel with a search bar and a grid of roles. The roles listed are: Administrator, Alert Manager, App Catalog Manager, Application Administrator, AQMAdmin, CMManager, CMPublisher, CMReader, Content Manager, Dashboard Manager, Device Manager, Plan Manager, and Policy Manager. Each role has a plus icon to assign it and a minus icon to remove it. The 'Guardar' button at the bottom right of the roles panel is highlighted with a red box.

Para quitar un rol a un usuario, este se puede eliminar dando clic en el icono derecho de cada rol asociado al usuario y luego dando clic en el botón **Guardar** del panel derecho.

This screenshot is identical to the previous one, but with red boxes highlighting the minus icons for the 'Administrator', 'Alert Manager', 'App Catalog Manager', and 'CMReader' roles in the 'Roles' panel, indicating they are being removed from the user.

3.2.7.3. Asignación de roles a un grupo de usuarios

La asignación de roles a un grupo de usuarios se realiza desde la sección de grupos de usuarios de la interfaz de configuración. Los usuarios que pertenecen a un grupo de usuarios heredan sus roles (incluso se visualizan para el usuario en la pestaña **roles** de forma aditiva con los roles que se han asociado directamente al usuario) sin embargo los roles de un grupo no son heredados por los sub-grupos contenidos en él.

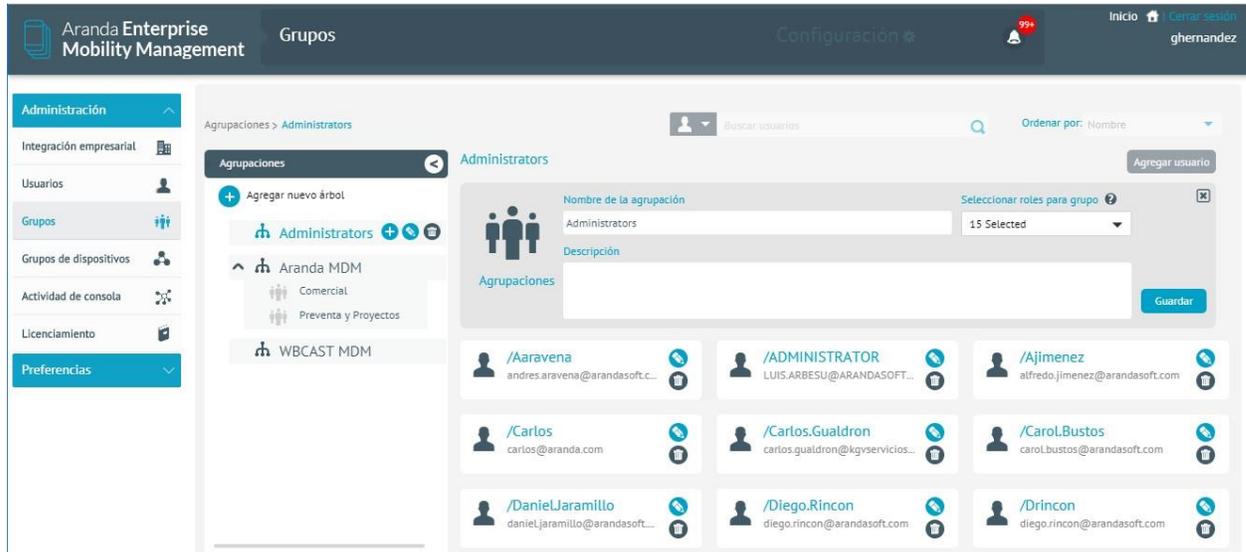
Seleccione el grupo al cual se le van a agregar los roles y de clic en **Editar**.

The screenshot shows the 'Grupos' (Groups) section of the Aranda Enterprise Mobility Management interface. On the left sidebar, the 'Administración' menu is expanded, and 'Grupos' is selected. The main content area shows a list of groups under 'Administraciones > Administrators'. The 'Administrators' group is highlighted, and its edit icon (a pencil) is circled in red. The main area also displays a grid of users with their names and email addresses, each with an edit icon.

Seleccione los roles que se van a agregar y de clic en **Guardar**.

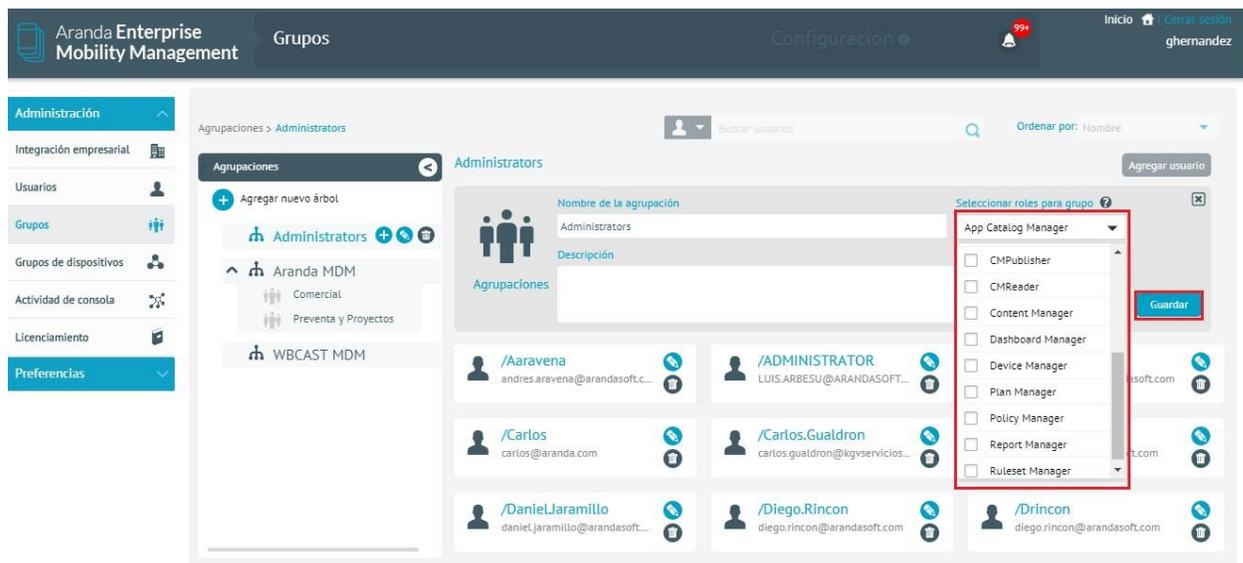
The screenshot shows the 'Grupos' section of the Aranda Enterprise Mobility Management interface. The 'Administrators' group is selected in the left sidebar. The main area displays a form for editing the group. A dropdown menu titled 'Seleccionar roles para grupo' is open, showing a list of roles with checkboxes. The roles listed are: Administrator, Alert Manager, App Catalog Manager, Application Administr..., AQMAdmin, AQMSpecialist, AQMUser, CMManager, and CMPublisher. The 'Guardar' button is visible at the bottom right of the form.

Para retirarle un rol a un grupo debe dar clic en **Editar**.



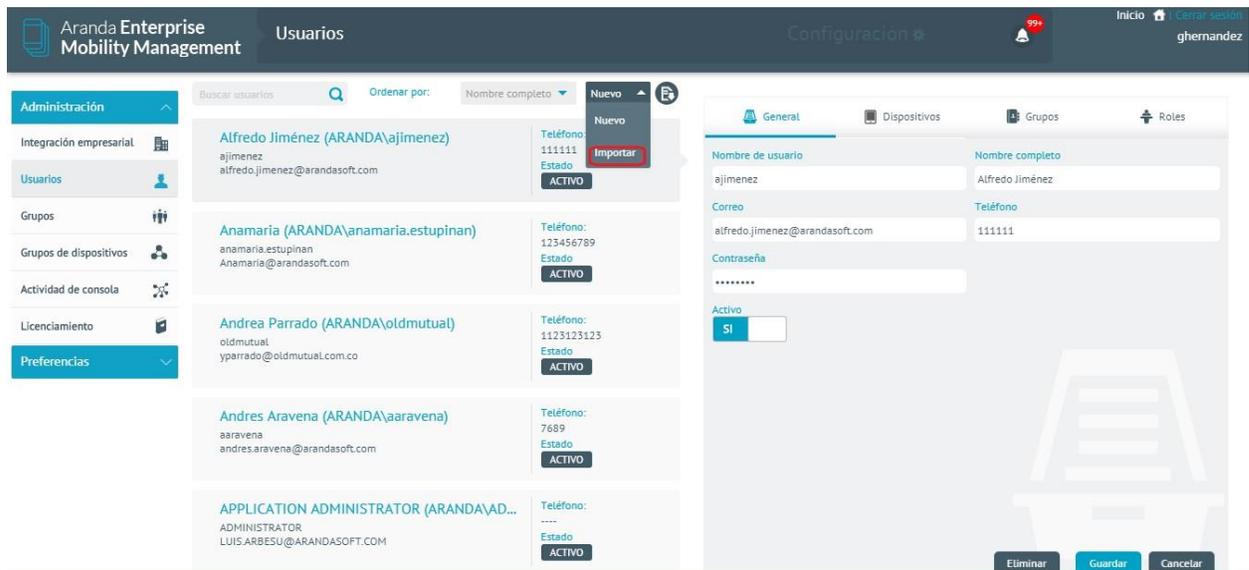
Quite el Check de selección de la casilla del rol que desea retirar y luego de clic en **Guardar**.

La acción de asignación de roles a un grupo solamente se puede hacer en grupos creados en la consola AEMM, los grupos importados en la sincronización con directorio activo no se les puede gestionar roles.

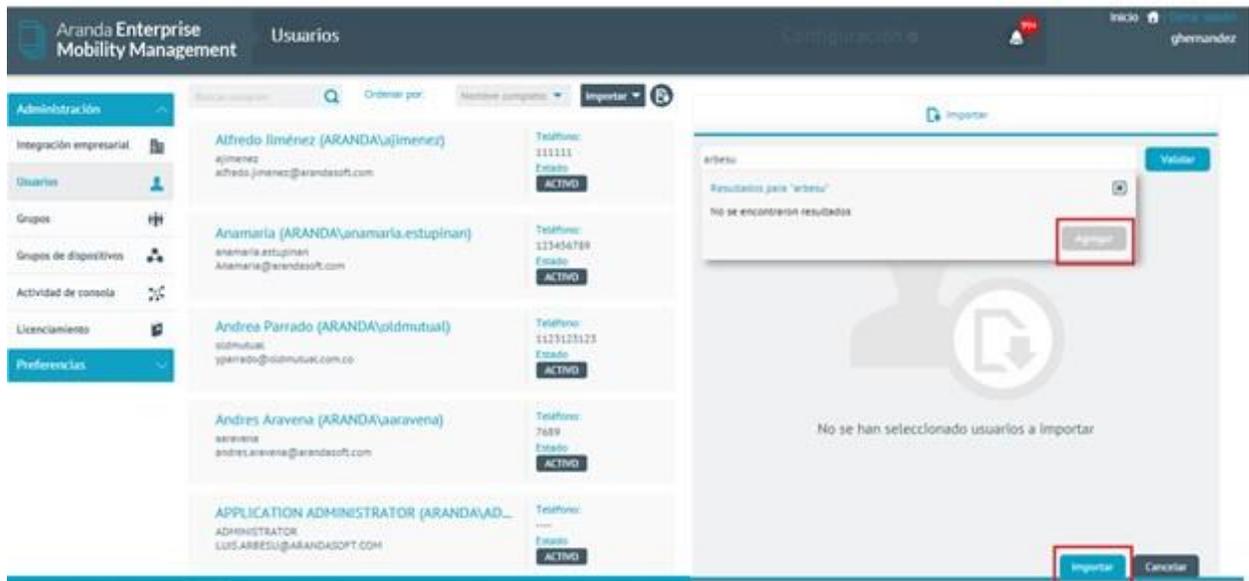


3.2.8. Importación de usuarios

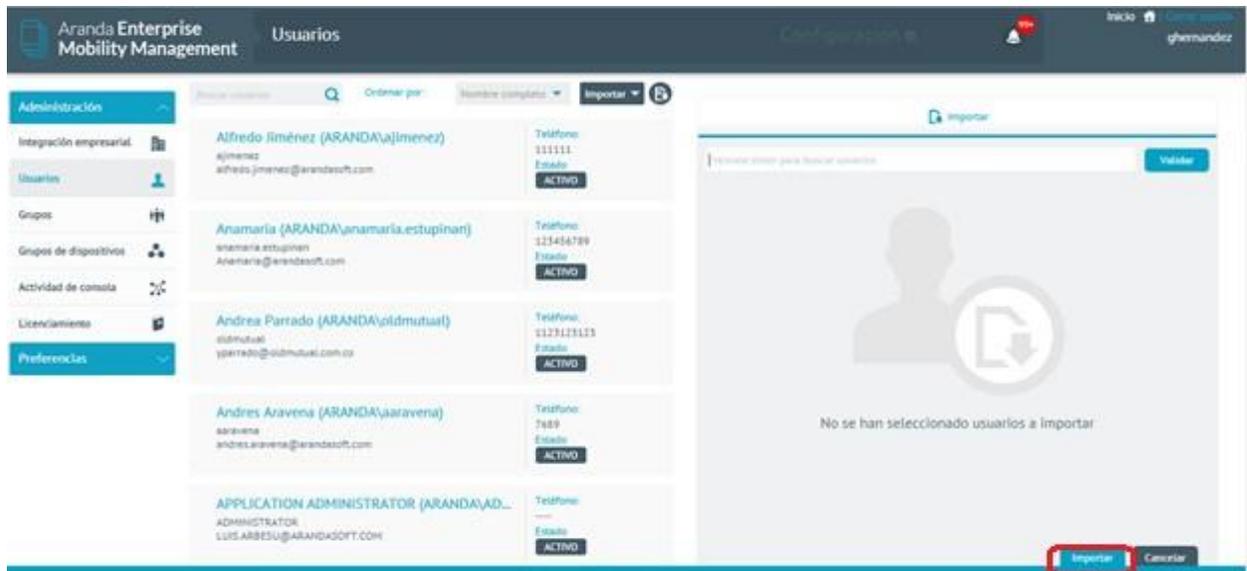
Ingrese a **Usuarios** y seleccione **Importar**



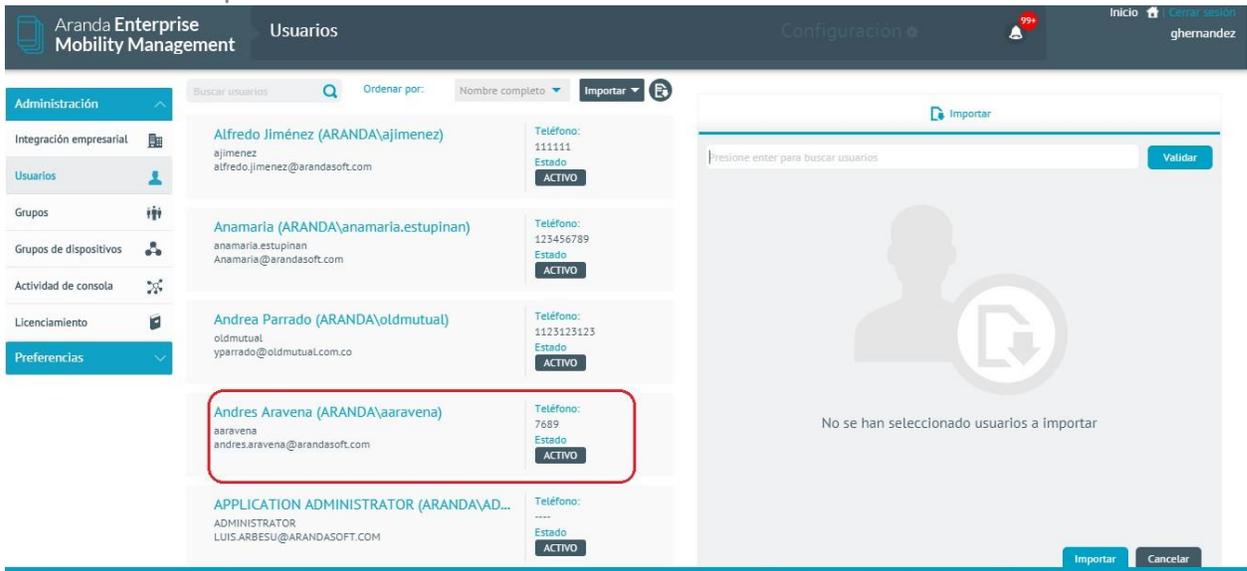
Digite el nombre de usuario y selecciónelo (los usuarios que ya se encuentran importados están acompañados de un recuadro en la imagen).



De clic en la opción **Importar**.



El usuario se importa exitosamente.



3.2.9. Estado de usuarios

Un usuario o grupo puede tener dos estados (Activo e inactivo), si el usuario o grupo se encuentra inactivo no tiene interacción con ningún proceso en AEMM.

Usuario inactivo: Si el usuario pertenece al Directorio Activo no es posible realizar cambios en el estado.

The screenshot shows the 'Usuarios' (Users) management interface. On the left, a sidebar contains navigation options: Administración, Integración empresarial, Usuarios, Grupos, Grupos de dispositivos, Actividad de consola, Licenciamiento, and Preferencias. The main area displays a list of users with their details, including name, email, phone number, and status (ACTIVO). A red box highlights the 'Activo' checkbox, which is currently checked. On the right, a form for editing user details is visible, with fields for 'Nombre de usuario', 'Nombre completo', 'Correo', 'Teléfono', and 'Contraseña'. The 'Activo' checkbox is also highlighted in the form.

Nombre de usuario	Nombre completo
aaravena	Andres Aravena
andres.aravena@arandasoft.com	7689

Por el contrario, si el usuario se obtiene como usuario local, tiene la posibilidad de cambiar su estado.

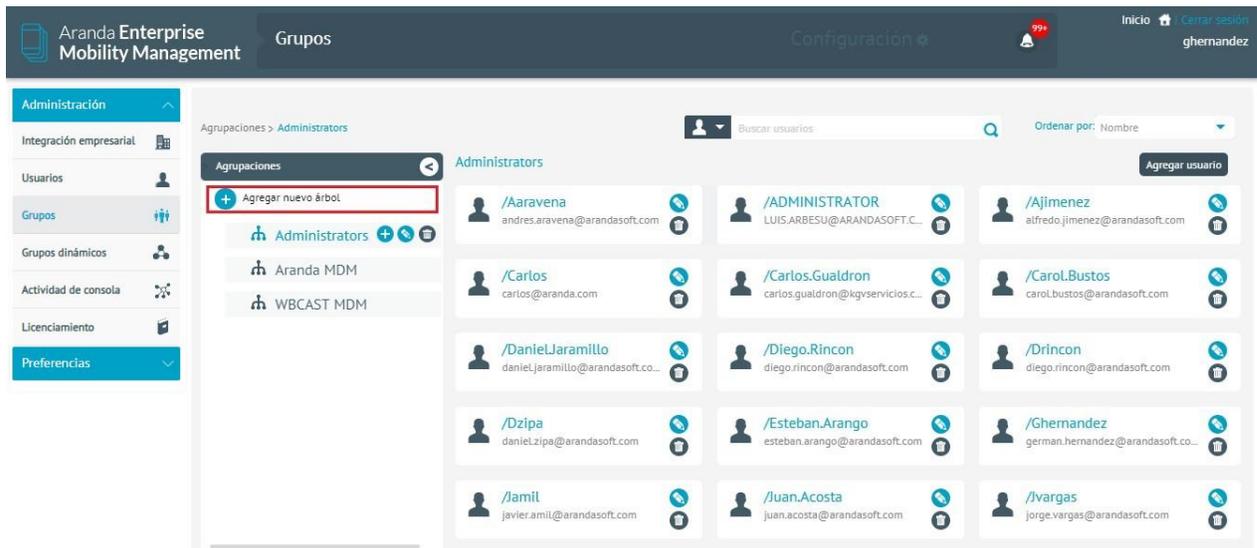
This is a duplicate of the screenshot above, showing the same 'Usuarios' management interface. The 'Activo' checkbox is highlighted with a red box, indicating that the user's status can be changed.

3.3. Grupos

3.3.1. Creación de grupos

Los grupos de consola se crean como grupos locales y se hacen necesarios cuando estos no se obtienen del Directorio Activo, a este tipo de grupos se les es permitido realizar modificaciones a su información, así como también crear sub-grupos (Nodos) dentro de ellos, ya sean un grupo principal (Árbol) o Nodos. Dentro de estos grupos se pueden asociar usuarios y/o dispositivos.

Para crear un grupo ingrese a **Configuración > General**, y luego a Grupos, luego de clic en **Agregar nuevo árbol**.



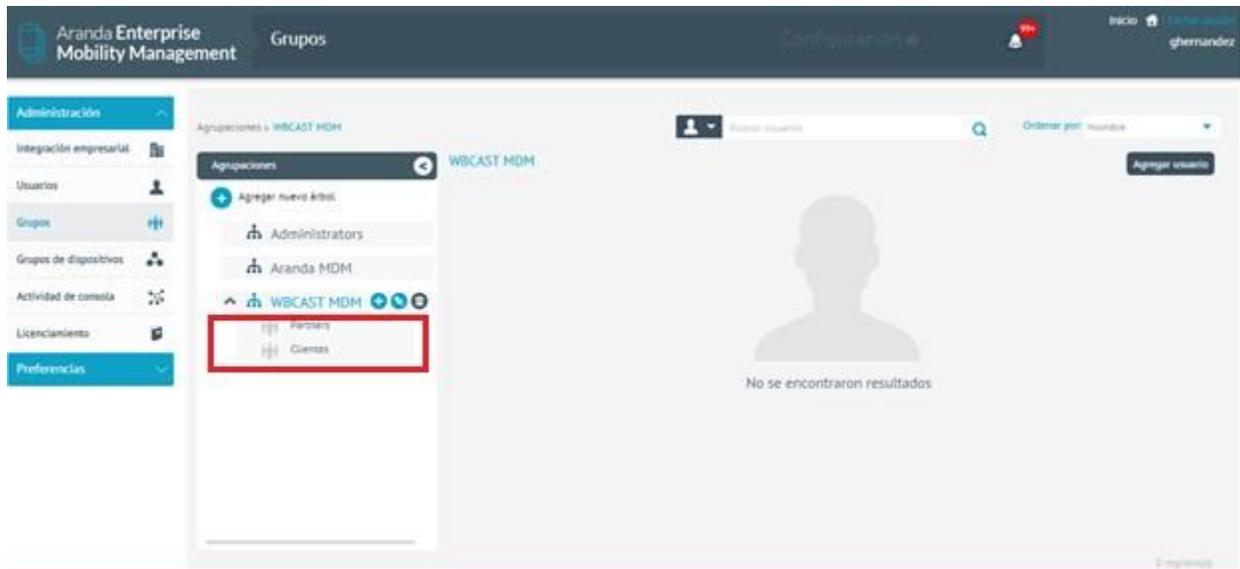
The screenshot displays the 'Administrators' group management interface. On the left, a sidebar contains navigation links. The main area shows a list of administrators with search and sort options. A red box highlights the 'Agregar nuevo árbol' button in the 'Agrupaciones' section.

Nombre	Correo electrónico	Acciones
/Aaravena	andres.aravena@arandasoft.com	[Iconos]
/ADMINISTRATOR	LUIS.ARBESU@ARANDASOFT.C...	[Iconos]
/Ajimenez	alfredo.jimenez@arandasoft.com	[Iconos]
/Carlos	carlos@aranda.com	[Iconos]
/Carlos.Gualdron	carlos.gualdron@kgyservicios.c...	[Iconos]
/Carol.Bustos	carol.bustos@arandasoft.com	[Iconos]
/DanieLJaramillo	daniel.jaramillo@arandasoft.co...	[Iconos]
/Diego.Rincon	diego.rincon@arandasoft.com	[Iconos]
/Drincon	diego.rincon@arandasoft.com	[Iconos]
/Dzipa	daniel.zipa@arandasoft.com	[Iconos]
/Esteban.Arango	esteban.arango@arandasoft.com	[Iconos]
/Ghernandez	german.hernandez@arandasoft.co...	[Iconos]
/Jamil	javier.amil@arandasoft.com	[Iconos]
/Juan.Acosta	juan.acosta@arandasoft.com	[Iconos]
/Jvargas	jorge.vargas@arandasoft.com	[Iconos]

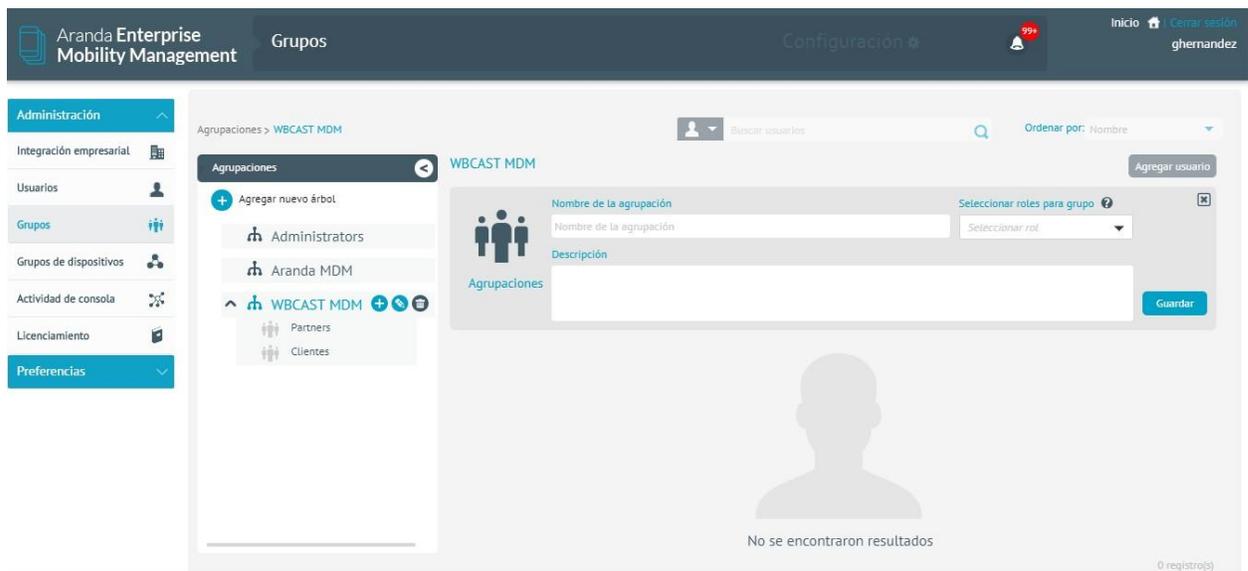
Ingrese la información requerida, si desea puede asociarles roles a los grupos o si no, lo puede hacer posteriormente.

Seleccione **Guardar**.

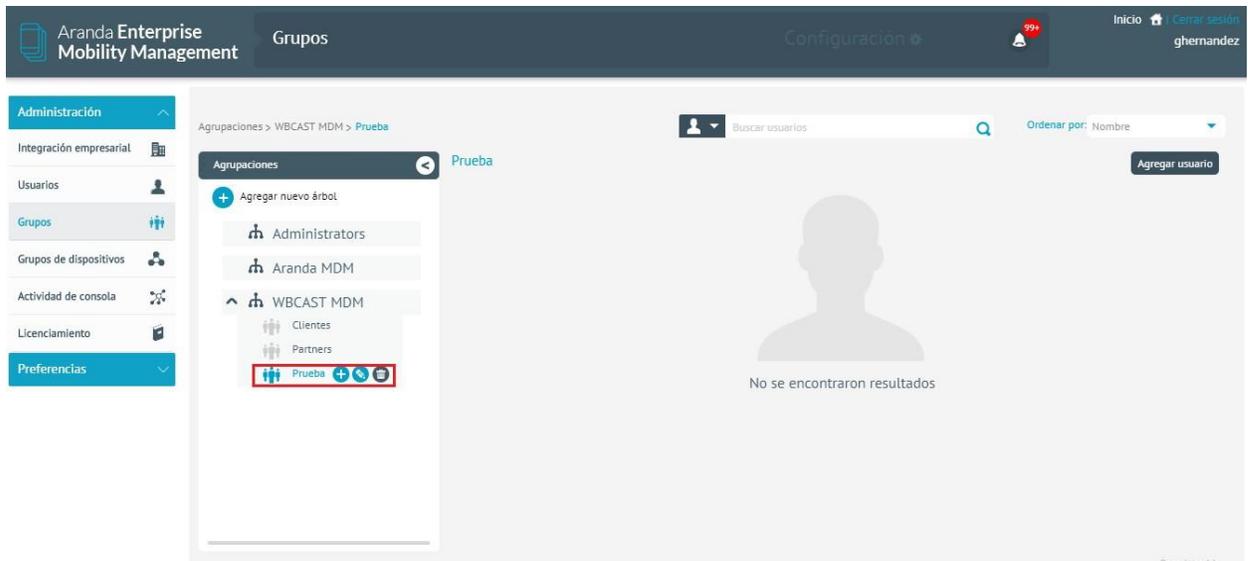
Para la creación de un sub-grupo (Nodo) debe ubicarse en el grupo que lo va a contener y dar clic en **Agregar agrupación**.



Ingrese la información requerida.

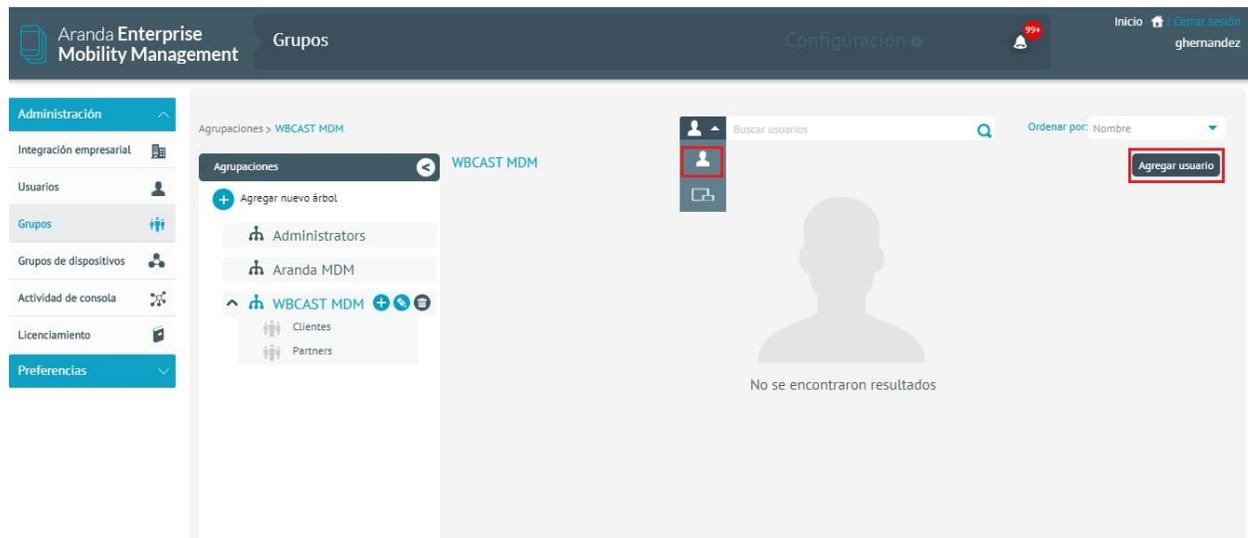


Ahora de clic en **guardar**.

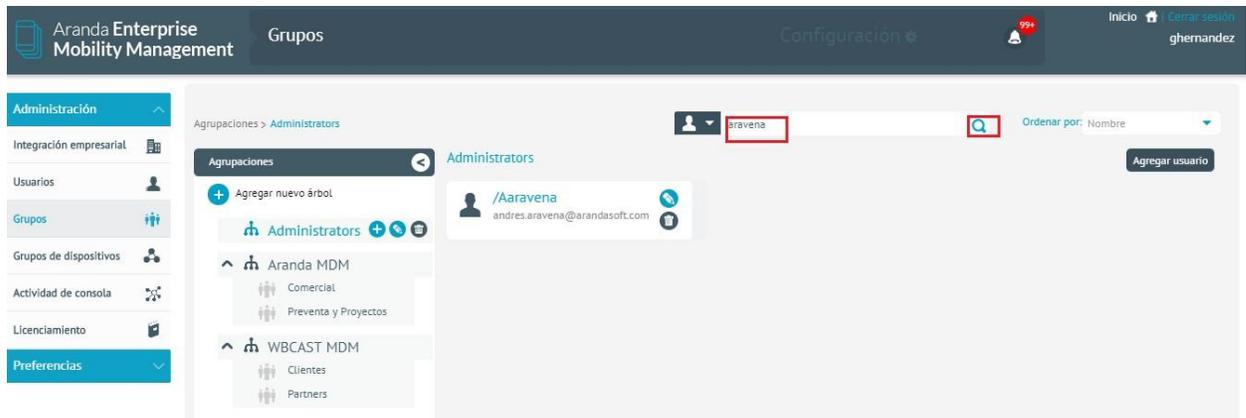


3.3.2. Agregación de usuarios a un grupo

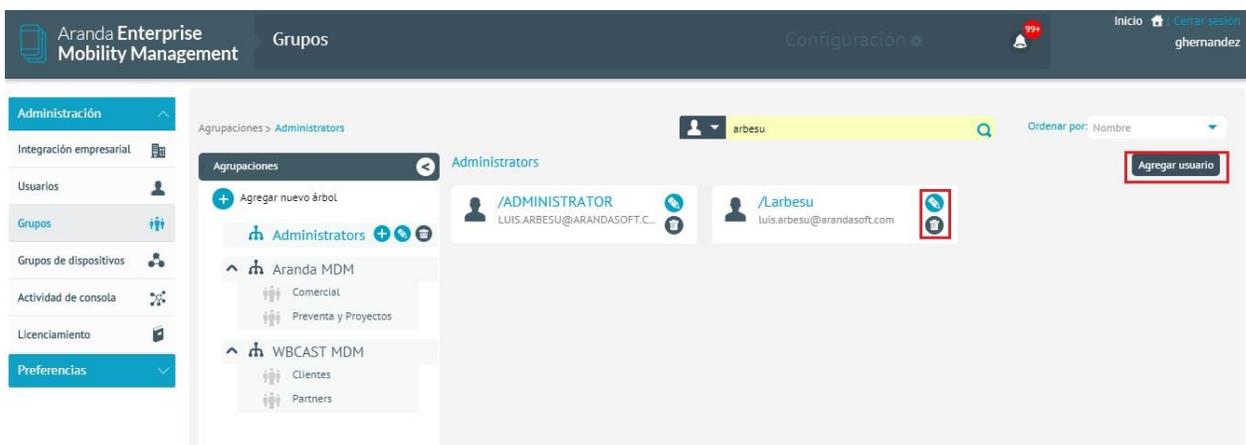
Si desea asociar un usuario a un grupo de clic en **Usuarios** en el selector y luego de clic en **Agregar usuario**.



Ingrese los criterios de búsqueda y haga clic en **Buscar**.



Seleccione los usuarios que desea agregar y luego de clic en **Agregar**.

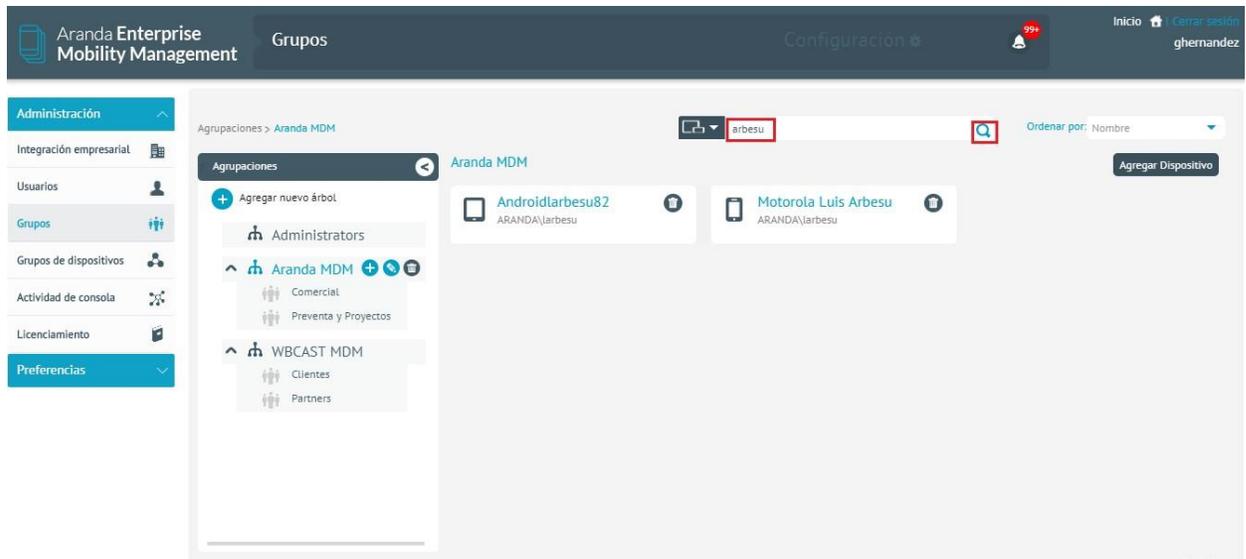


3.3.3. Agregación de dispositivos a un grupo

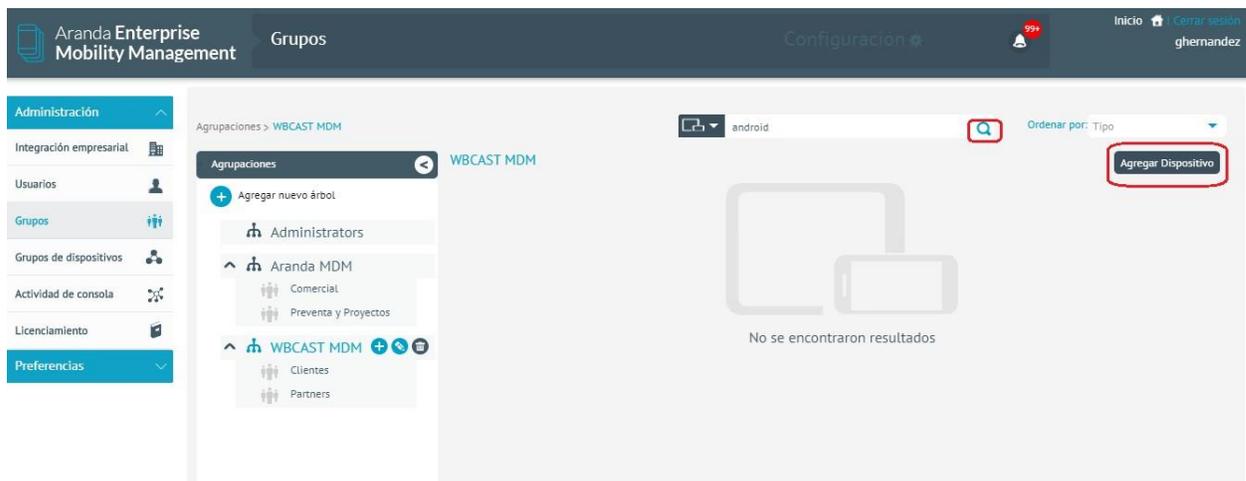
Para asociar un dispositivo a un grupo debe escoger Dispositivos en el selector y luego dar clic en **Agregar dispositivo**.



Ingrese los criterios de búsqueda y de clic en **Buscar**.



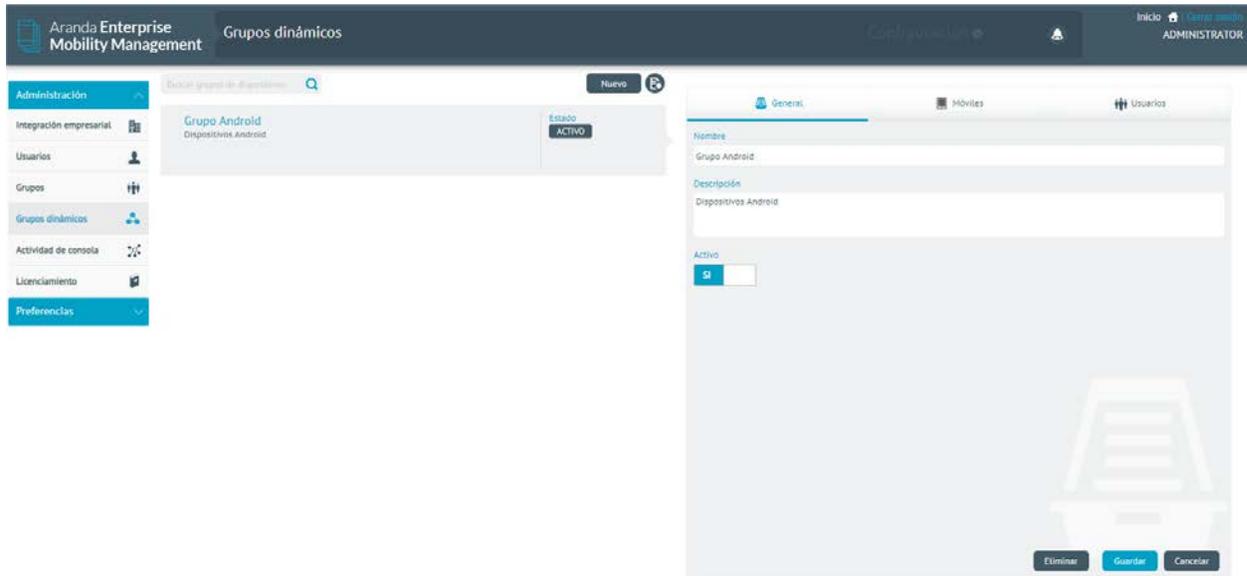
Seleccione los dispositivos que desea agregar y de clic en **Agregar**.



3.4. Grupos Dinámicos

En muchos casos se requiere enviar un comando a muchos móviles que comparten una o varias condiciones específicas. Estas condiciones pueden ser variables o fijas por dispositivo. En estos casos los grupos dinámicos proveen un mecanismo para agrupar por una o varias condiciones. Los grupos dinámicos como su nombre lo indica son totalmente dinámicos con respecto a los dispositivos que agrupan, es decir que los móviles pueden dejar de pertenecer al grupo si cambian una condición importante, por ejemplo, si a un móvil que sea de la compañía se le cambia el tipo de propiedad, automáticamente deja de pertenecer a los grupos que solo incluyan móviles de la compañía. Los grupos dinámicos pueden ser usados al desplegar políticas o conjuntos de reglas.

Para crear grupos dinámicos, de clic en "**Configuración**" en el menú principal y luego en la sección "**Grupos dinámicos**". Allí encontrará una lista ordenada por nombre, la cual puede ser filtrada realizando una búsqueda por nombre. Para crear un grupo de clic en el botón **Nuevo**. Para editar un grupo de clic en el ítem de la lista. En ambos casos aparece al lado derecho una sección con pestañas para editar los datos básicos del grupo y configurarlo.



En la segunda pestaña (Móviles) se pueden especificar las condiciones de pertenencia al grupo relacionadas con el móvil. Aquí se puede filtrar por tipo de propiedad (Compañía o Usuario), Plataforma (iOS o Android), Fabricante, Tipo (Smartphone o Tablet) y versión del sistema operativo. Todas las condiciones que se especifiquen deben ser cumplidas para que el móvil pertenezca al grupo.

General Móviles Usuarios

Propietario
Compañía

Plataforma
iOS

Fabricante
Apple

Tipo
Smartphone

Versión del sistema operativo
iOS 5, iOS 6, iOS 7

- Select All
- iOS 5
- iOS 6
- iOS 7
- iOS 8
- iOS null

Guardar Cancelar

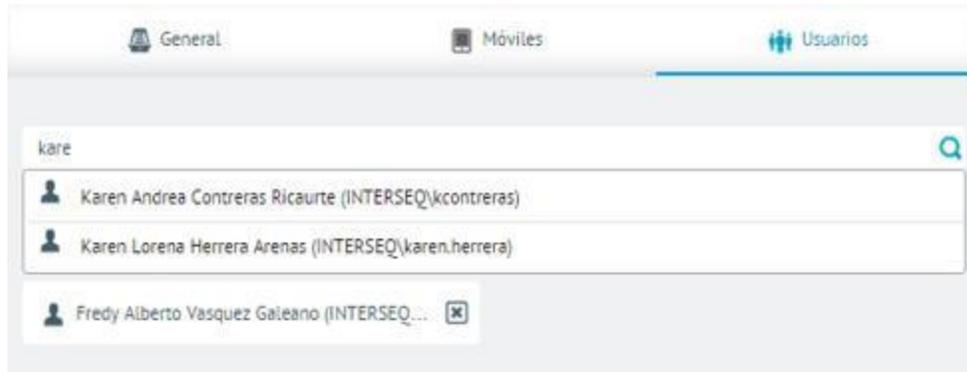
En la tercera pestaña (usuarios) se puede indicar otra alternativa para que los móviles pertenezcan al grupo, y ésta tiene que ver con la persona que porta el dispositivo. Se pueden escoger diferentes usuarios o grupos de usuarios para conformar la condición. Si algún dispositivo es portado por algunos de los usuarios o grupos incluidos, entonces el dispositivo pertenece al grupo.

General Móviles Usuarios

Buscar usuarios o grupos de usuarios

Alfredo Jiménez (ARANDA\ajimenez) x

Diego Rincon (ARANDA\diego.rincon) x

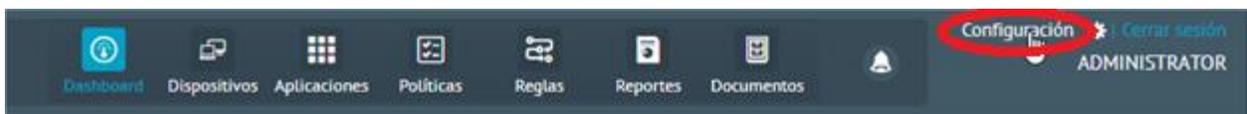


3.5. Actividad de consola

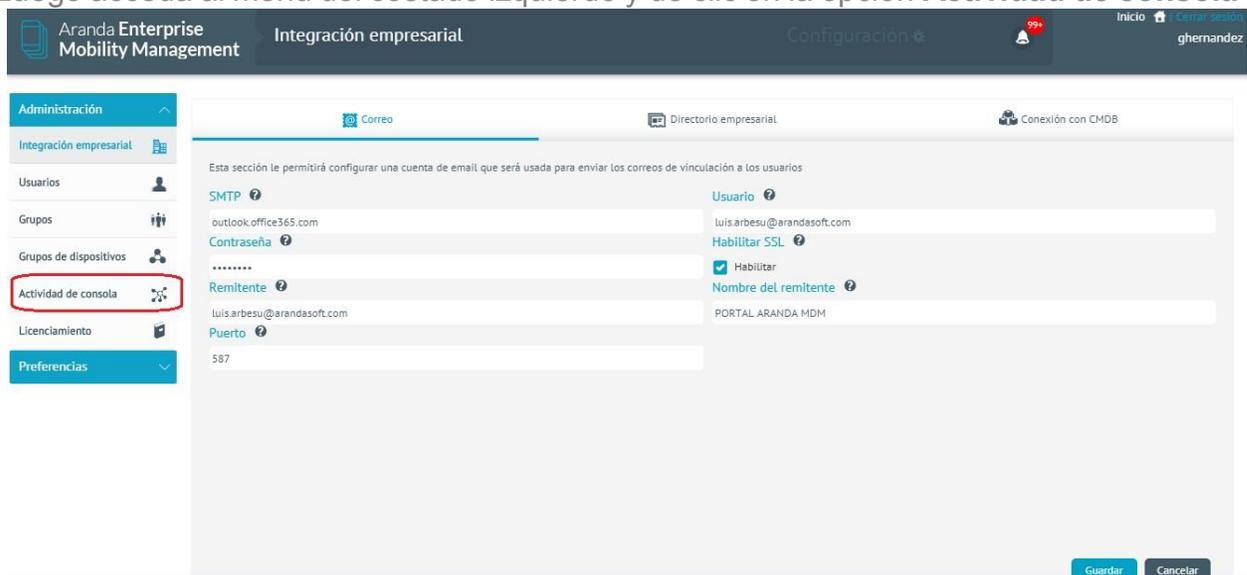
En Configuración hay una sección donde se puede consultar la actividad que se está registrando en la consola, es decir que se puede consultar las acciones que los diferentes usuarios han realizado dentro de la misma. Para cada acción registrada se muestra la siguiente información.

- Día y hora en la que se registró la acción.
- Identificador de la acción ejecutada.
- Usuario de la plataforma que ejecutó la acción.

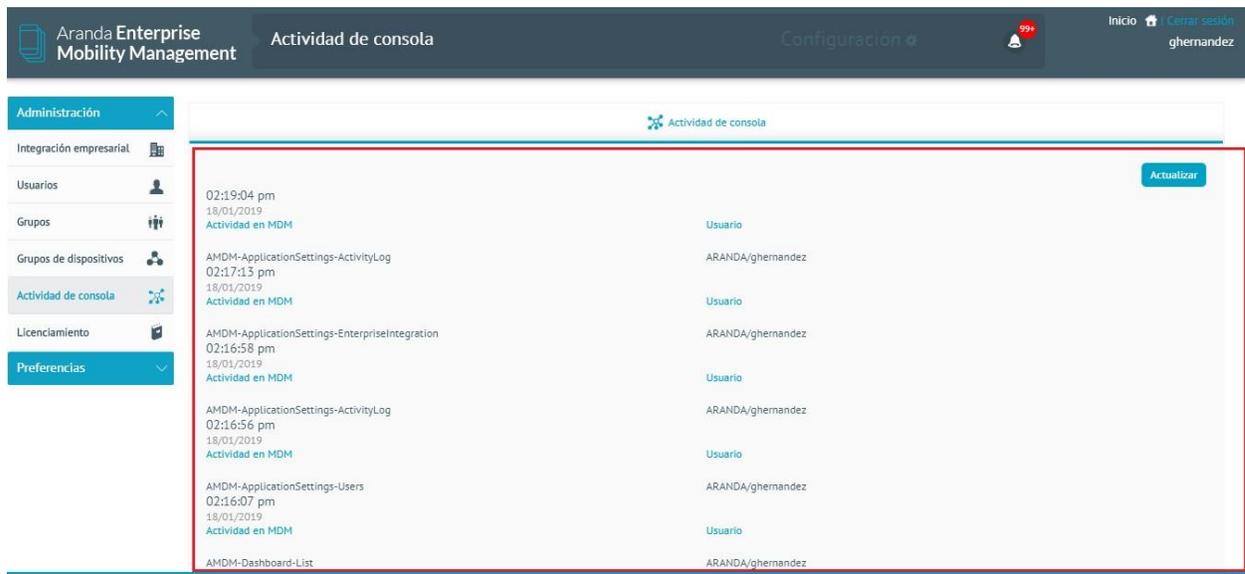
Para acceder a la sección de actividad de consola, de clic en **Configuración** del menú principal.



Luego acceda al menú del costado izquierdo y de clic en la opción **Actividad de consola**



En el costado derecho se muestra el listado de acciones registradas en la consola, si se desea se puede actualizar el listado dando clic en el botón **Actualizar** ubicado en la parte superior derecha del panel del listado.



The screenshot shows the 'Aranda Enterprise Mobility Management' interface. The main content area is titled 'Actividad de consola' and contains a table of activity logs. A red box highlights the table and an 'Actualizar' button in the top right corner. The table lists various system events with their timestamps, dates, and associated users.

Timestamp	Date	Activity	User	
02:19:04 pm	18/01/2019	Actividad en MDM	Usuario	
AMDM-ApplicationSettings-ActivityLog	02:17:13 pm	18/01/2019	Actividad en MDM	ARANDA/ghernandez
AMDM-ApplicationSettings-EnterpriseIntegration	02:16:58 pm	18/01/2019	Actividad en MDM	Usuario
AMDM-ApplicationSettings-ActivityLog	02:16:56 pm	18/01/2019	Actividad en MDM	ARANDA/ghernandez
AMDM-ApplicationSettings-Users	02:16:07 pm	18/01/2019	Actividad en MDM	Usuario
AMDM-Dashboard-List				ARANDA/ghernandez

Los registros se van cargando a través de lazy loading a medida que el usuario navega por el listado cuando el scroll llega a la parte inferior del listado.

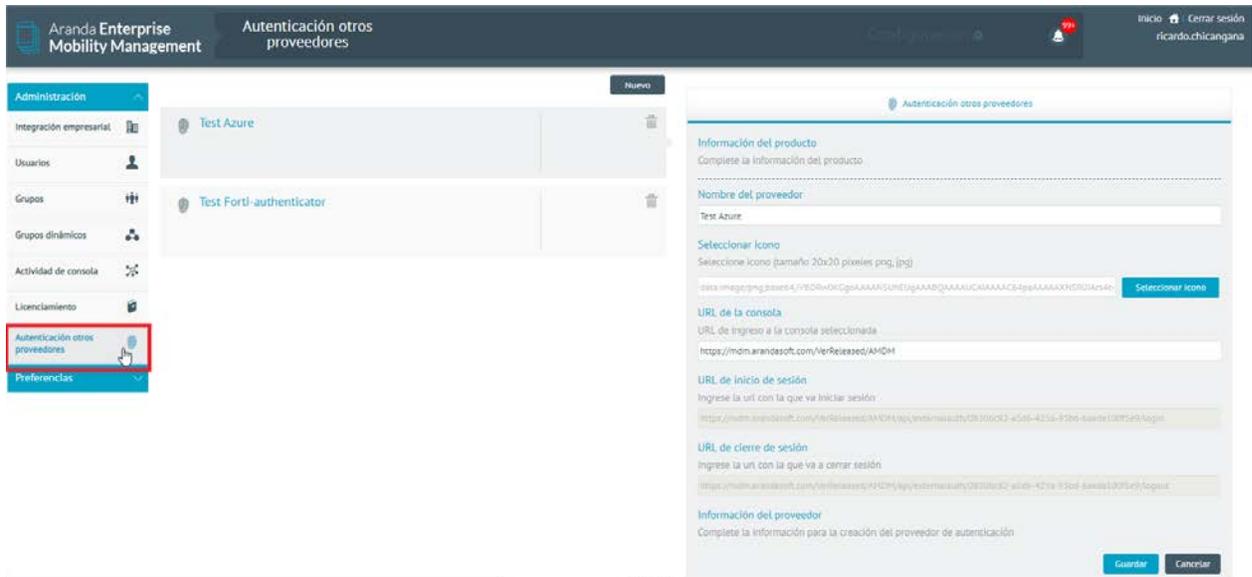
3.6. Licenciamiento

En este módulo ya introducido en el numeral 2.2, se listan y se pueden gestionar las licencias actualmente cargadas en el sistema.

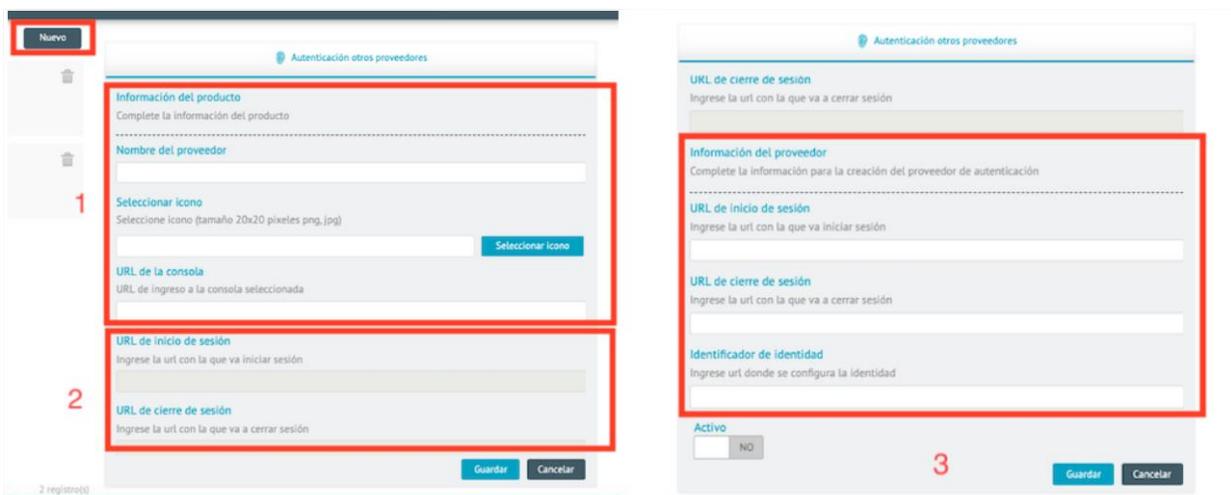
Es importante aclarar que se pueden cargar cuantas licencias se deseen, el sistema sumará el número de dispositivos de todas las licencias vigentes.

3.7. Autenticación otros proveedores

3.7.1. Configuración



Para iniciar la configuración diligencie la siguiente información:



Sección 1:

- **Nombre de la Proveedor:** Nombre de la conexión con la cual se identificará en el listado de proveedores configurados y en el botón ubicado en el login de la herramienta para su respectivo ingreso

- **Seleccionar icono:** Imagen que identificará el proveedor configurado en la pantalla de login.
- **URL de la consola:** Debe ingresar la URL de la consola de AEMM hasta el AMDM (https://[dominio de servidor]/AMDM) Ejm: https://mydominio.com/AMDM

Sección 2:

- URL de inicio de sesión: Esta información de url de inicio se genera automáticamente al ingresar la URL de la consola
- URL de cierre de sesión: Esta información de url de inicio se genera automáticamente al ingresar la URL de la consola

Información del Proveedor

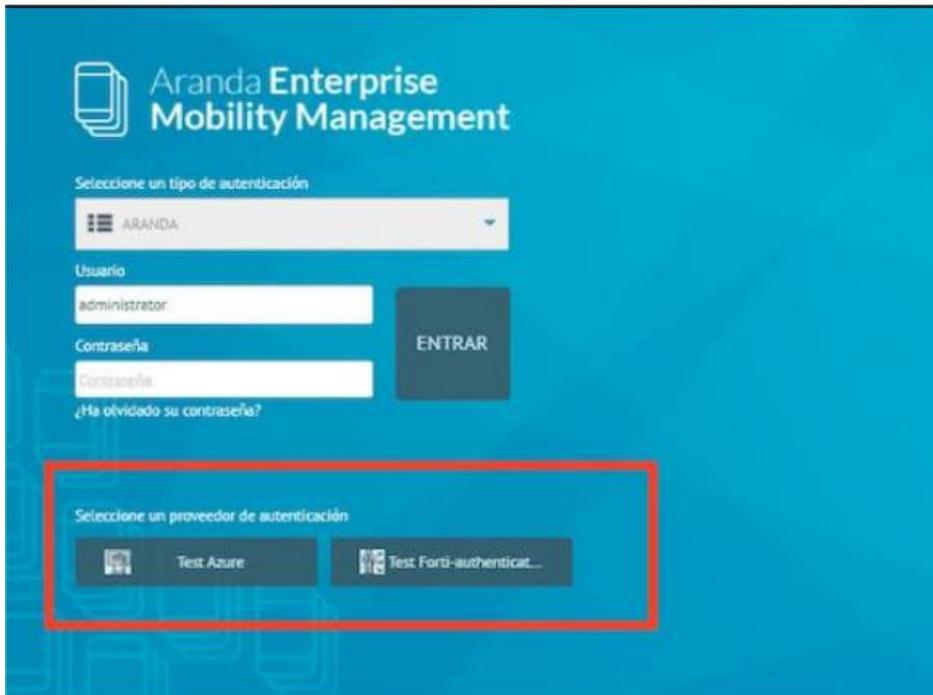
- URL de inicio de sesión: Url de inicio de sesión configurada por el proveedor
- URL de cierre de sesión: Url de fin de sesión configurada por el proveedor
- Identificador de Identidad: Url de identificación de la conexión configurada del sitio

Después de realizar su configuración, haga clic en Guardar, esta configuración se visualizará en el listado de proveedores.



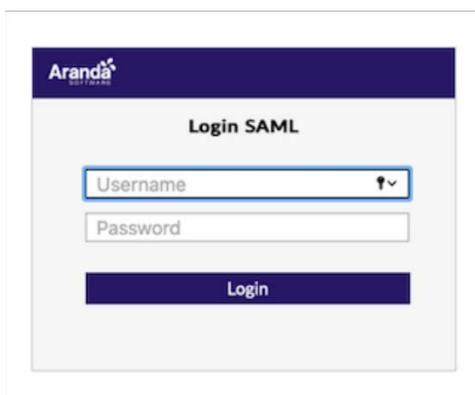
3.7.2. Ingreso por parte del usuario

El usuario se encuentra en el login de la consola AEMM, donde podrá visualizar la información de los proveedores de autenticación, para su ingreso debe hacer clic en el botón del proveedor que requiera



El usuario se encuentra en el login de la consola AEMM, donde podrá visualizar la información de los proveedores de autenticación, para su ingreso debe hacer clic en el botón del proveedor que requiera.

El sitio envía al usuario a una herramienta central de inicio de sesión SSO, el usuario ingresa sus credenciales, estos datos ingresados son validados y notifica a la aplicación que el usuario esta validado.



Una vez autenticado en el proveedor externo se hace una redirección normal a la consola, presentando la pantalla inicial.

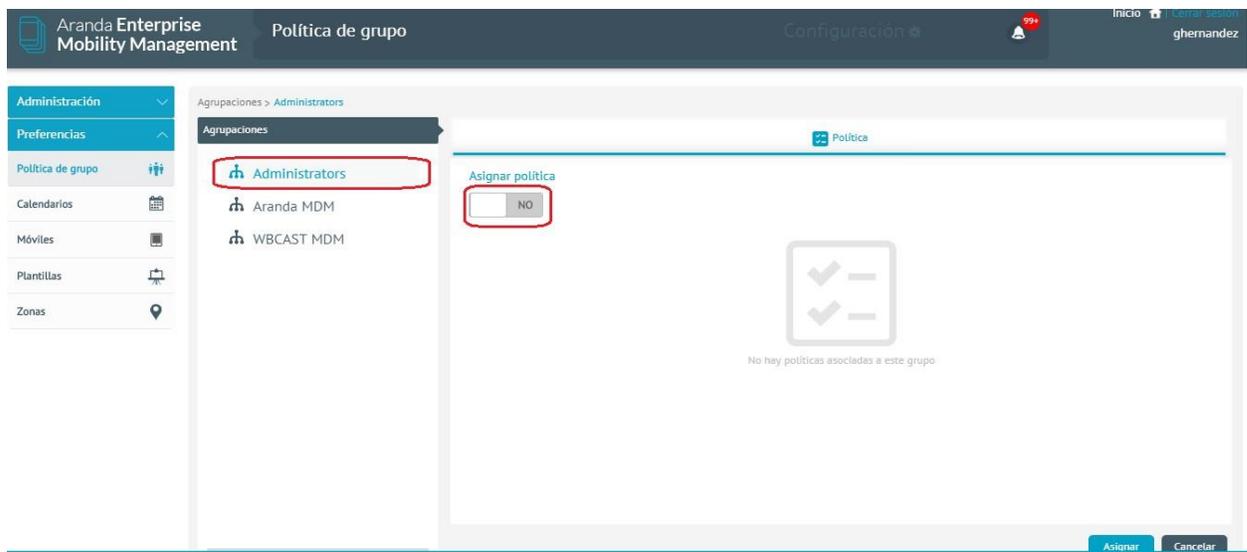
4. PREFERENCIAS

4.1. Política de Grupo

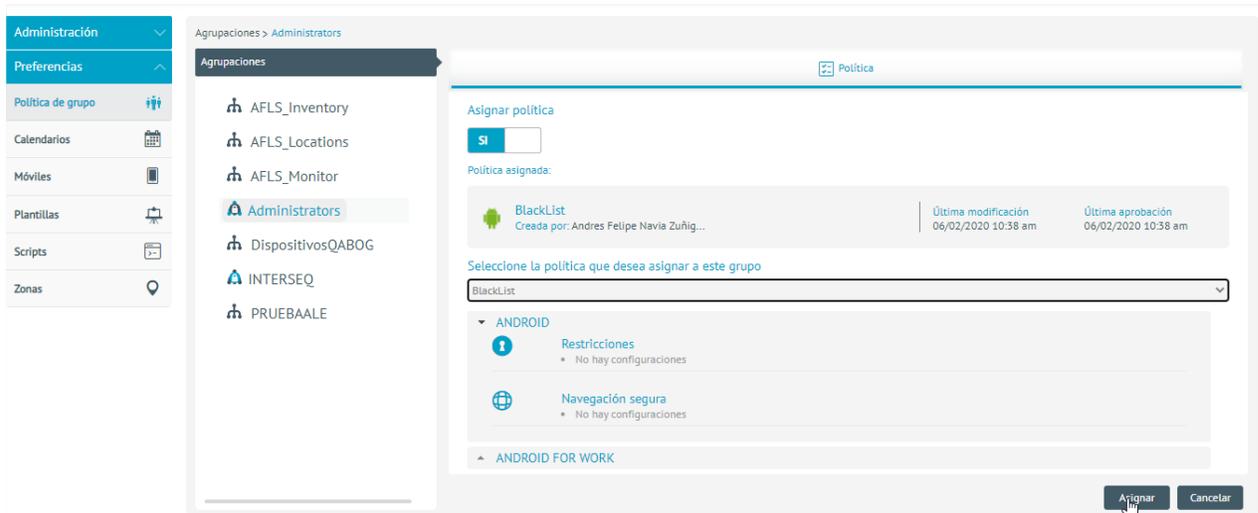
Esta opción le permite asignar la política a asignar a un dispositivo perteneciente al grupo en cuestión.

Esta asignación se realizará en el contexto de acción de regla de cambio de política, en la que se puede escoger la política de grupo, en tanto que, la política asignada en el presente módulo será la que se le asigne al dispositivo cuando la acción de regla se ejecute.

Para configurar la política de grupo acceda al módulo:



Luego escoja el grupo y a continuación la política, luego dé clic en Asignar.

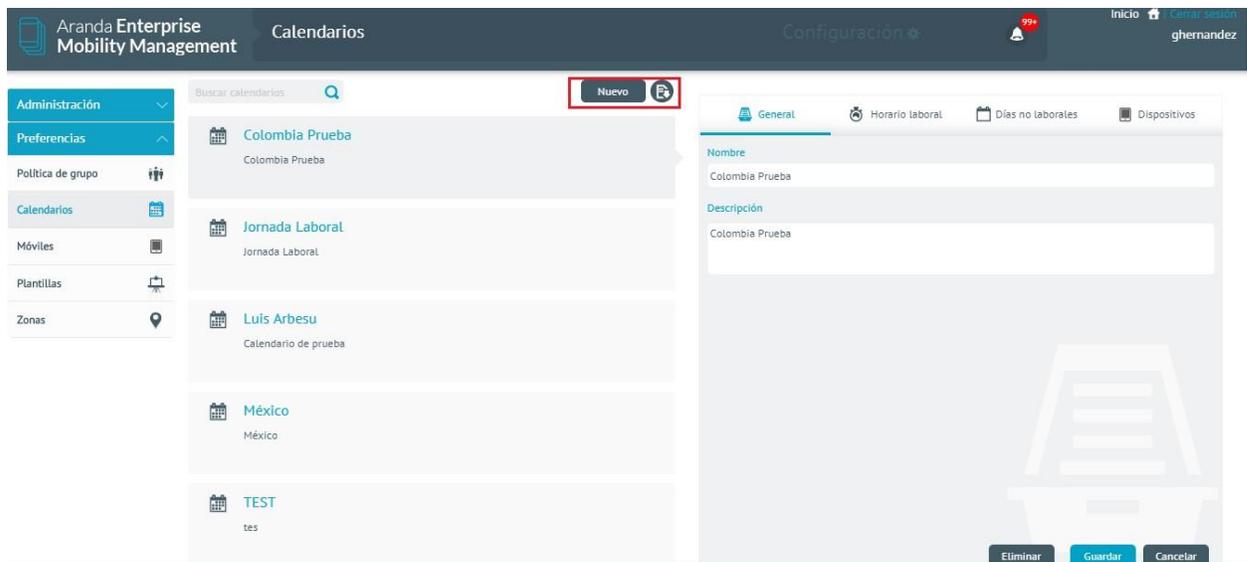


Es preciso aclarar que la política que se escoja solo será enviada a los dispositivos que su plataforma coincida con la de la política.

4.2. Configuración calendarios

Los Calendarios se deben configurar para hacer uso de las reglas de Timefencing (Franjas horarias). A continuación:

Ingresar a calendarios dentro del menú EMM y de clic en **Nuevo**.



Ingrese los datos solicitados y de clic en **Guardar**

Aranda Enterprise Mobility Management | Calendarios | Configuración | Inicio | gherandez

Administración | Preferencias | Política de grupo | Calendarios | Móviles | Plantillas | Zonas

Buscar calendarios

- Colombia Prueba
- Jornada Laboral
- Luis Arbesu
- México
- TEST

General

Nombre: Horario de Preventa

Descripción: Horario personal de preventa

Guardar | Cancelar

4.2.1. Horario laboral

Para configurar las horas laborales de clic en la opción **Horario laboral**.

Aranda Enterprise Mobility Management | Calendarios | Configuración | Inicio | gherandez

Administración | Preferencias | Política de grupo | Calendarios | Móviles | Plantillas | Zonas

Buscar calendarios

- Colombia Prueba
- Jornada Laboral
- Luis Arbesu
- México
- TEST

General | **Horario laboral** | Dias no laborales | Dispositivos

Nombre: Jornada Laboral

Descripción: Jornada Laboral

Eliminar | Guardar | Cancelar

<https://mobile.arandasoft.com/Mobile/Preventa/AMDM/Pages/AMDM/Default.aspx...>

Seleccione las horas laborales de la semana, mediante clic sostenido.

Aranda Enterprise Mobility Management | Calendarios | Configuración | Inicio | Cerrar sesión gherandez

Administración | Preferencias | Política de grupo | Calendarios | Móviles | Plantillas | Zonas

Buscar calendarios

- Colombia Prueba
- Jornada Laboral
- Luis Arbesu
- México
- TEST

General | **Horario laboral** | Días no laborales | Dispositivos

Horario laboral

Define el horario laboral, para seleccionar varias celdas presione la tecla ctrl para no perder la selección

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
05:30 am							
06:00 am							
06:30 am							
07:00 am							
07:30 am							
08:00 am							
08:30 am							
09:00 am							
09:30 am							
10:00 am							

Horario laboral Horario no laboral **Guardar** Cancelar

Luego de clic en la opción **Guardar**.

Aranda Enterprise Mobility Management | Calendarios | Configuración | Inicio | Cerrar sesión gherandez

Administración | Preferencias | Política de grupo | Calendarios | Móviles | Plantillas | Zonas

Buscar calendarios

- Colombia Prueba
- Jornada Laboral
- Luis Arbesu
- México
- TEST

General | **Días no laborales** | Horario laboral | Dispositivos

Días no laborales

Define los días no laborales de todo el año

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
05:30 am							
06:00 am							
06:30 am							
07:00 am							
07:30 am							
08:00 am							
08:30 am							
09:00 am							
09:30 am							
10:00 am							

Horario laboral Horario no laboral **Guardar** Cancelar

4.2.2. Días no laborales

Para configurar los días en los que no se labora de todo el año, de clic en la opción **Días no laborales**.

Aranda Enterprise Mobility Management | Calendarios | Configuración | Inicio | Cerrar sesión gherandez

Administración | Preferencias | Políticas de grupo | Calendarios | Móviles | Plantillas | Zonas

Buscar calendarios

- Colombia Prueba
- Jornada Laboral
- Luis Arbesu
- México
- TEST

General | Horario laboral | **Días no laborales** | Dispositivos

Horario laboral

Defina el horario laboral, para seleccionar varias celdas presione la tecla ctrl para no perder la selección

Lunes | Martes | Miércoles | Jueves | Viernes | Sábado | Domingo

05:30 am
06:00 am
06:30 am
07:00 am
07:30 am
08:00 am
08:30 am
09:00 am
09:30 am
10:00 am

Horario laboral | Horario no laboral | Guardar | Cancelar

De clic sobre el día que desea marcar como no laboral e ingrese el dato solicitado

Aranda Enterprise Mobility Management | Calendarios | Configuración | Inicio | Cerrar sesión gherandez

Administración | Preferencias | Políticas de grupo | Calendarios | Móviles | Plantillas | Zonas

Buscar calendarios

- Colombia Prueba
- Jornada Laboral
- Luis Arbesu
- México
- TEST

General | Horario laboral | **Calendario** | Dispositivos

Calendario

Defina los días no laborales en cada uno de los meses del año

2019

Enero 2019 | Febrero 2019

Do	Lu	Ma	Mi	Ju	Vi	Sá	Do	Lu	Ma	Mi	Ju	Vi	Sá
											1	2	
6	7						6	7	8	9			
13	14						13	14	15	16			
20	21	22	23	24	25	26	17	18	19	20	21	22	23
27	28	29	30	31			24	25	26	27	28		

Marzo 2019 | Abril 2019

Do Lu Ma Mi Ju Vi Sá | Do Lu Ma Mi Ju Vi Sá

1 2 | 1 2 3 4 5 6

3 4 5 6 7 8 9 | 7 8 9 10 11 12 13

Fecha seleccionada: 2019-2-6 | Nombre o descripción del día | Aceptar

Guardar | Cancelar

https://mobile.arandasoft.com/Mobile_Preventa/AMDM/Peqes/AMDM/Default.asp...

Luego de clic en la opción **Guardar**.

Aranda Enterprise Mobility Management | Calendarios | Configuración | Inicio | gherandez

Administración | Preferencias | Políticas de grupo | Calendarios | Móviles | Plantillas | Zonas

Buscar calendarios | Nuevo

Colombia Prueba
Colombia Prueba

Jornada Laboral
Jornada Laboral

Luís Arbesu
Calendario de prueba

México
México

TEST
tes

General | Horario laboral | **Días no laborales** | Dispositivos

Calendario
Defina los días no laborales en cada uno de los meses del año

2019

Enero 2019							Febrero 2019						
Do	Lu	Ma	Mi	Ju	Vi	Sá	Do	Lu	Ma	Mi	Ju	Vi	Sá
												1	2
6	7								6	7	8	9	
13	14						13	14	15	16			
20	21	22	23	24	25	26	17	18	19	20	21	22	23
27	28	29	30	31			24	25	26	27	28		

Marzo 2019							Abril 2019						
Do	Lu	Ma	Mi	Ju	Vi	Sá	Do	Lu	Ma	Mi	Ju	Vi	Sá
					1	2							
							1	2	3	4	5	6	
3	4	5	6	7	8	9	7	8	9	10	11	12	13

Fecha seleccionada: 2019-2-6
Nombre o descripción del día | Aceptar

Guardar | Cancelar

https://mobile.arandasoft.com/Mobile_Preventa/AMDM/Pages/AMDM/Default.asp...

4.2.3. Dispositivos

Para asociar un calendario, dé clic en la opción **Dispositivos**

The screenshot shows the 'Aranda Enterprise Mobility Management' interface. The main menu on the left includes 'Administración', 'Preferencias', 'Calendarios', 'Móviles', 'Plantillas', and 'Zonas'. The 'Calendarios' section is active, displaying a list of calendars: 'Colombia Prueba', 'Jornada Laboral', 'Luis Arbesu', 'México', and 'TEST'. The right-hand panel is titled 'Configuración' and has tabs for 'General', 'Horario laboral', 'Días no laborales', and 'Dispositivos'. The 'Dispositivos' tab is selected and highlighted with a red box. Below the tabs, there is a search bar and a list of devices. A date picker is open, showing the date '2019-2-6' selected, with an 'Aceptar' button. At the bottom right, there are 'Guardar' and 'Cancelar' buttons.

Para realizar la búsqueda de usuarios y/o dispositivos, seleccione el que desea agregar, y luego de clic en **Guardar**.

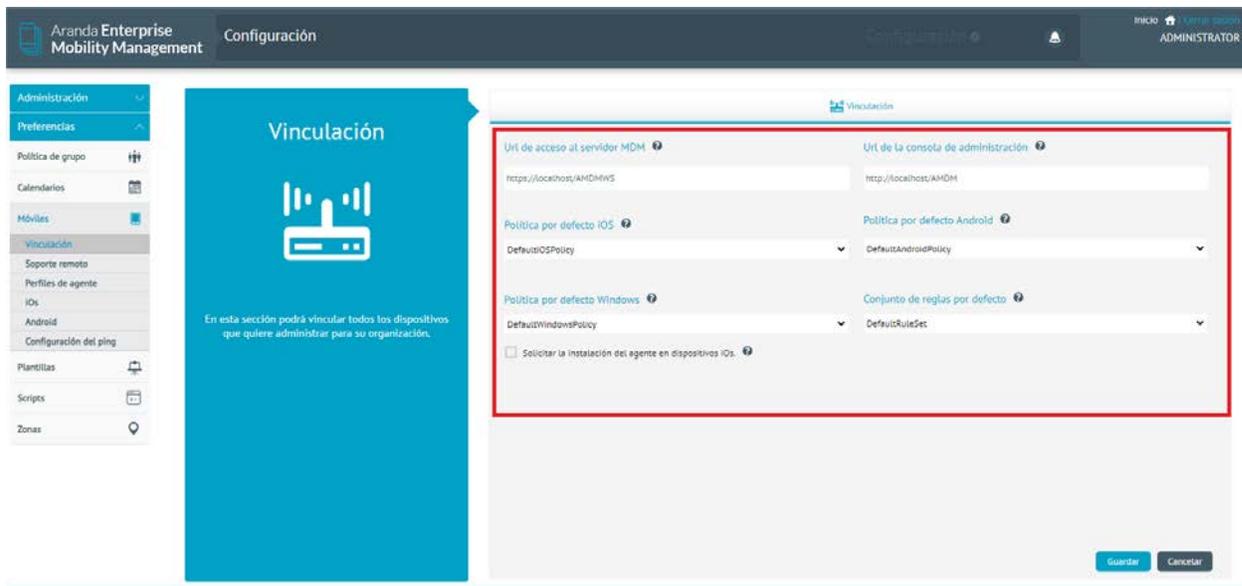
This screenshot shows the same interface as the previous one, but with the search results for devices. The search bar contains the text 'arbesu'. The results list is highlighted with a red box and includes the following items: 'Androidlarbesu119', 'Androidlarbesu191', 'Androidlarbesu82', 'Galaxy S4', 'Motorola Luis Arbesu', and 'Luis Carlos Arbesu (ARANDA)(arbesu)'. The 'Dispositivos' tab remains selected.

4.3. Móviles

4.3.1. Vinculación

En esta sección de configuran las opciones para realizar la vinculación de los dispositivos ante el servidor AEMM. Se pueden diligenciar las siguientes propiedades:

- **Url de acceso al servidor MDM:** Url que se utilizará para establecer comunicación entre los dispositivos y el servidor AEMM, los dispositivos deben de poder alcanzar esta url para poderse vincular al servidor.
- **Url de la consola de administración:** Url de la consola desde donde se hace la administración de los dispositivos y se usa para realizar invitaciones de vinculación vía correo electrónico.
- **Política por defecto iOS:** Política que será aplicada a los dispositivos de la plataforma iOS cuando éstos se vinculen.
- **Política por defecto Android:** Política que será aplicada a los dispositivos de la plataforma Android cuando éstos se vinculen.
- **Política por defecto Windows:** Política que será aplicada a los dispositivos de la plataforma Windows cuando éstos se vinculen.
- **Conjunto de reglas por defecto:** Conjunto de reglas que será aplicado a todo dispositivo que se vincule.
- **Casilla de verificación “Solicitar la instalación del agente en dispositivos iOS”:** Casilla que al marcarla realiza la acción de envío de comando de instalación automáticamente cuando un dispositivo iOS ha realizado la vinculación tipo web.



4.3.2. Soporte Remoto

En esta sección de pueden configurar las opciones para sesiones de control remoto hacia dispositivos:

- **Solicitar confirmación en dispositivo móvil antes de iniciar sesión:** Al estar marcada esta casilla la sesión solicitará confirmación por parte del usuario del dispositivo para iniciarse.
- **Solicitar clave en dispositivo móvil antes de iniciar sesión:** Al estar marcada esta casilla, en dispositivo al iniciar sesión se generará un código numérico de 6 dígitos que se tendrá que digitar correctamente en consola para iniciar efectivamente la sesión.

Marque o desmarque las casillas de acuerdo a lo requerido y luego haga clic en “Aplicar”.

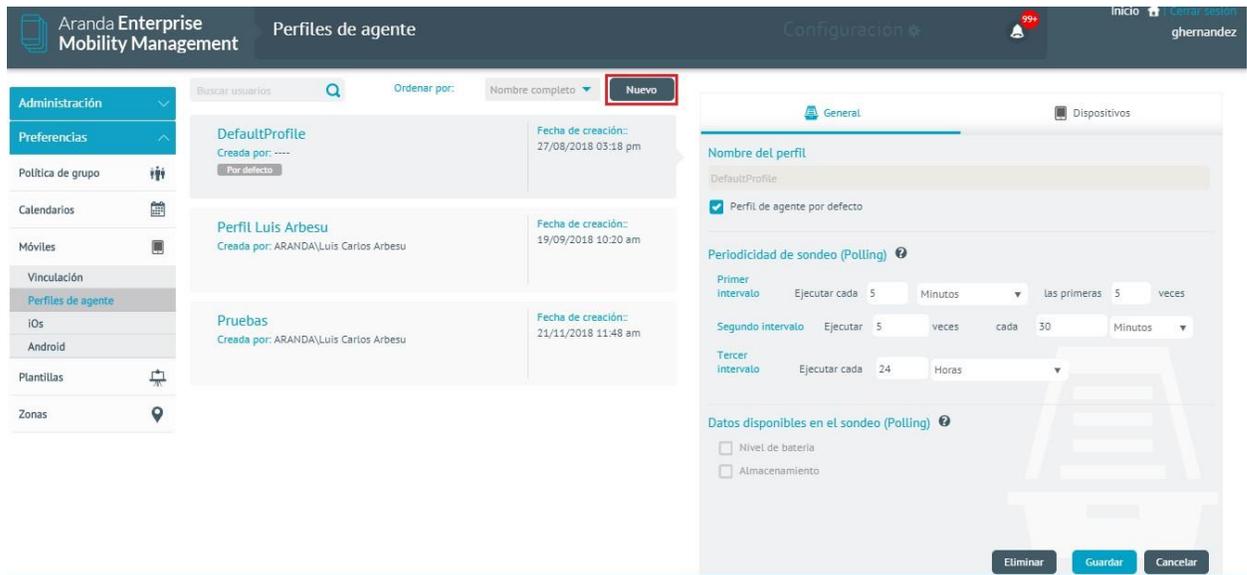
The screenshot shows the 'Configuración' (Configuration) page for 'Soporte remoto' (Remote Support) in the Aranda Enterprise Mobility Management system. The interface includes a sidebar menu with options like 'Administración', 'Preferencias', 'Política de grupo', 'Calendarios', 'Móviles', 'Vinculación', 'Soporte remoto', 'Perfiles de agente', 'iOs', 'Android for work', 'Configuración del ping', 'Aplicaciones del sistema android', 'Plantillas', 'Scripts', and 'Zonas'. The main content area is titled 'Soporte remoto' and contains two checked checkboxes: 'Solicitar confirmación en dispositivo móvil antes de iniciar sesión' and 'Solicitar clave en dispositivo móvil antes de iniciar sesión'. Below the checkboxes are 'Aplicar' and 'Cancelar' buttons. A blue callout box on the left explains that this section is for configuring mobile device confirmation for remote support requests.

4.3.3. Perfiles de Agente

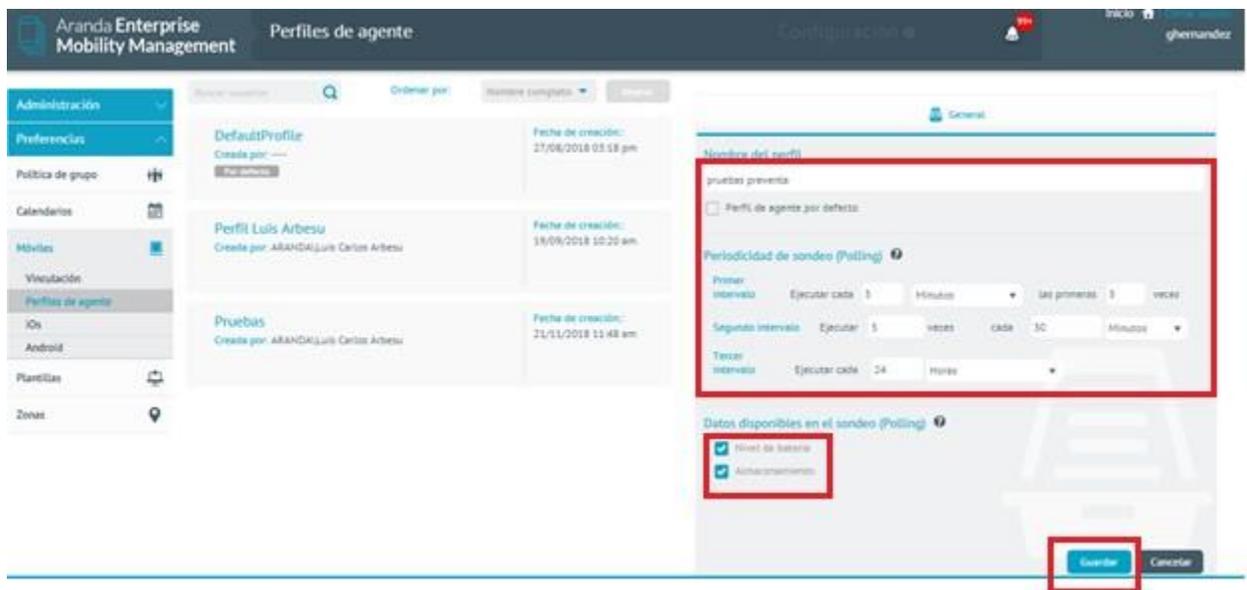
Esta sección se presenta la configuración disponible para la funcionalidad de “polling”, desde los dispositivos, que consiste en que cada cierto periodo de tiempo el dispositivo por sí mismo, sin necesidad de una notificación push, contacte al servidor de AEMM, en busca de comandos pendientes. Adicionalmente este contacto son servidor se puede aprovechar para entregar cierta información configurable de estado del dispositivo.

4.3.3.1. Creación de un perfil de agente

Para crear un perfil de agente de clic en **Nuevo**



Luego diligencie la siguiente información y de clic en **Guardar**



Los campos presentados corresponden a las tres etapas consecutivas del polling desde los dispositivos:

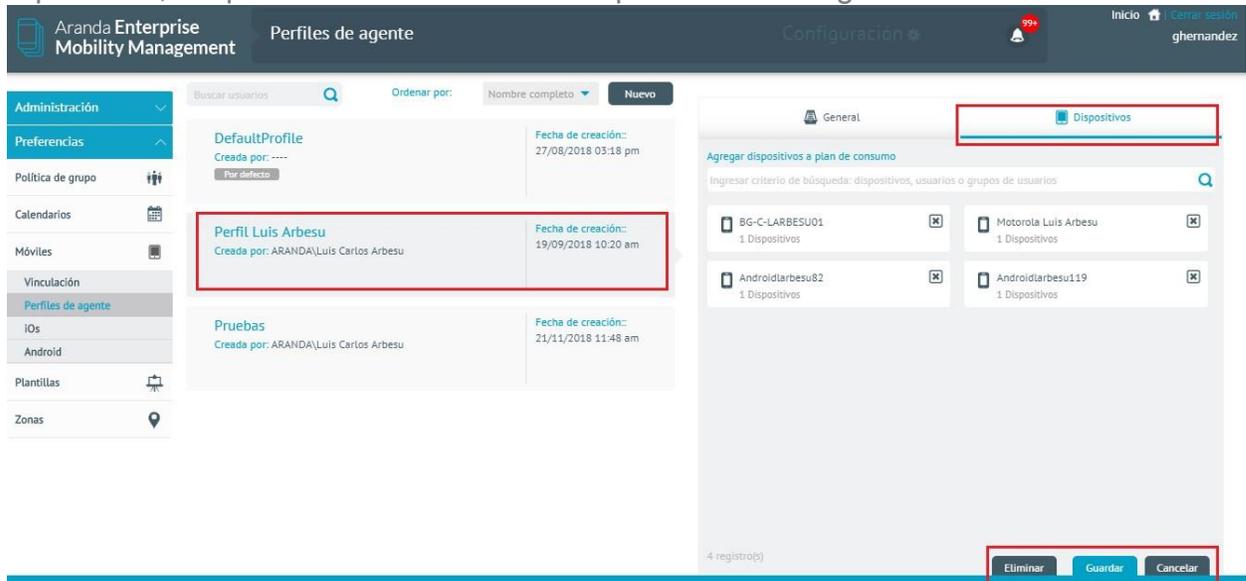
Primer intervalo: Primera etapa, donde se puede configurar el intervalo de tiempo y la cantidad de veces a ejecutar.

Segundo intervalo: Primera etapa, donde se puede también configurar el intervalo de tiempo y la cantidad de veces a ejecutar.

Tercer intervalo: Tercera etapa, en la que sólo se puede configurar el intervalo de tiempo, ya que este es el intervalo que quedará permanentemente una vez se hayan superado las dos primeras etapas.

4.3.3.2. Asociación de dispositivos

De clic sobre alguna de las reglas previamente creadas y seleccione la pestaña dispositivos, allí podrá asociar o eliminar dispositivos a la regla.



The screenshot shows the 'Perfiles de agente' configuration page in the Aranda Enterprise Mobility Management system. The 'Dispositivos' tab is selected, and a list of devices is displayed. The 'Perfil Luis Arbesu' profile is highlighted, and the 'Dispositivos' tab is also highlighted. The 'Eliminar', 'Guardar', and 'Cancelar' buttons are visible at the bottom right.

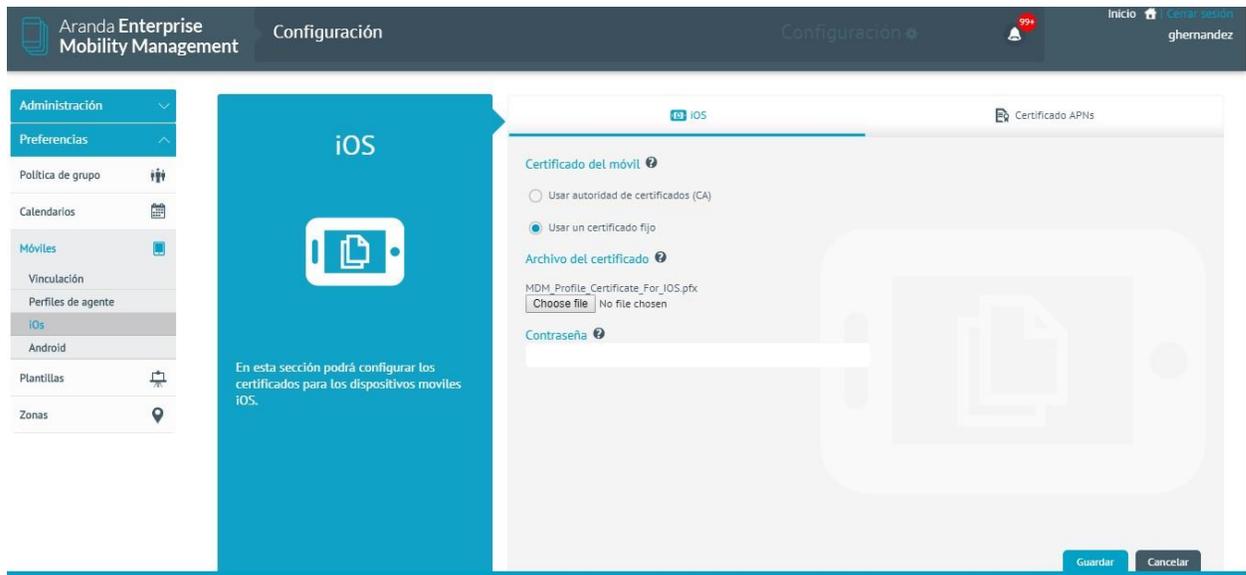
4.3.4. iOS

En esta sección se pueden configurar las opciones correspondientes para la gestión de dispositivos de la plataforma iOS

4.3.4.1. Pestaña "iOS"

En esta sección se puede configurar el certificado con el que se validarán los perfiles MDM iOS instalados en los dispositivos, se puede hacer de dos formas:

- **Usando autoridad de certificados (CA):** Esta opción permite configurar una url de un servidor donde se generarán los certificados de validación para los móviles.
- **Certificado fijo:** Si elige la opción de certificado fijo, se usará un único certificado para todos los móviles. En esta opción viene precargado un certificado que puede usarse sin problemas para validar los perfiles iOS MDM para los dispositivos.



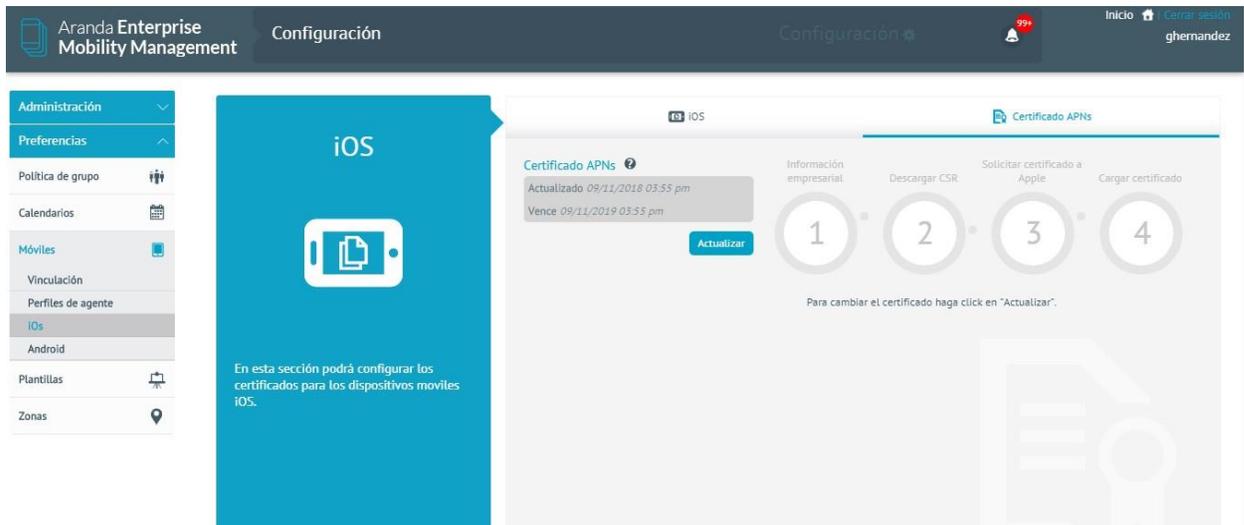
4.3.4.2. Certificado APNs

En esta sección se puede configurar el certificado APN (Apple Push Notification), que es utilizado para enviar las notificaciones push a los perfiles MDM a instalarse en los dispositivos durante la vinculación.

Para configurar el certificado APN siga los siguientes pasos:

Creación de un Certificado APN Nuevo

a. Ingrese a **certificado APNs** y de clic en **Generar**.



Aranda Enterprise Mobility Management Configuración Configuración Inicio Cerrar sesión ghermanez

Administración
Preferencias
Política de grupo
Calendarios
Móviles
Vinculación
Perfiles de agente
iOS
Android
Plantillas
Zonas

iOS

En esta sección podrá configurar los certificados para los dispositivos móviles iOS.

Certificado APNs

Actualizado 09/11/2018 03:55 pm
Vence 09/11/2019 03:55 pm

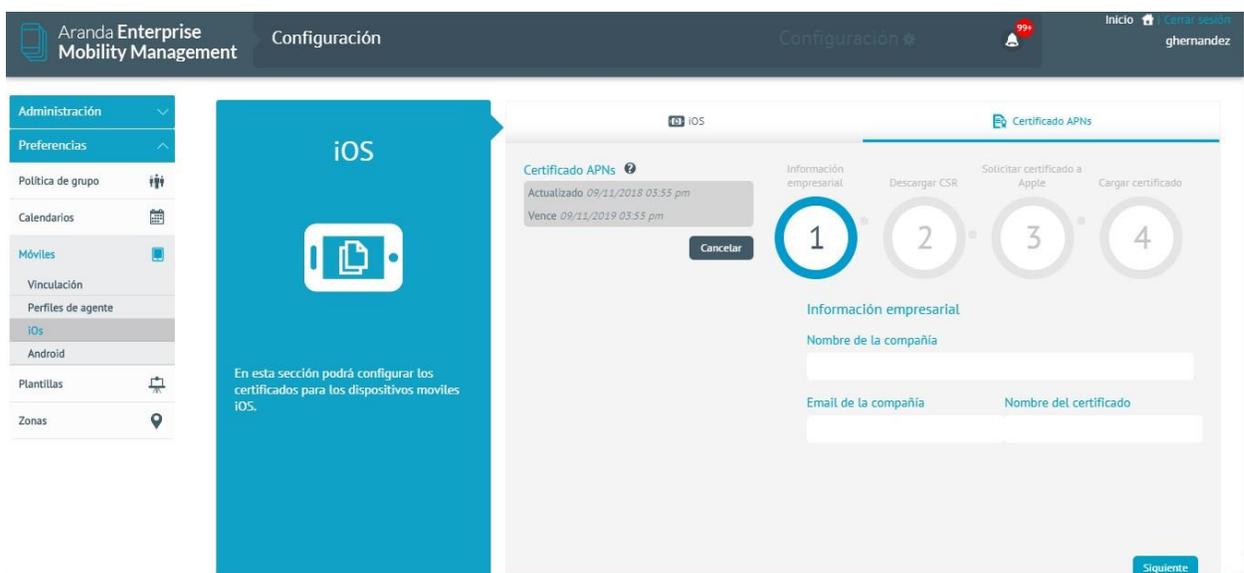
Actualizar

Información empresarial Descargar CSR Solicitar certificado a Apple Cargar certificado

1 2 3 4

Para cambiar el certificado haga clic en "Actualizar".

b. Luego, ingrese el nombre y correo de la compañía junto con el nombre del certificado.



Aranda Enterprise Mobility Management Configuración Configuración Inicio Cerrar sesión ghermanez

Administración
Preferencias
Política de grupo
Calendarios
Móviles
Vinculación
Perfiles de agente
iOS
Android
Plantillas
Zonas

iOS

En esta sección podrá configurar los certificados para los dispositivos móviles iOS.

Certificado APNs

Actualizado 09/11/2018 03:55 pm
Vence 09/11/2019 03:55 pm

Cancelar

1 2 3 4

Información empresarial

Nombre de la compañía

Email de la compañía Nombre del certificado

Siguiente

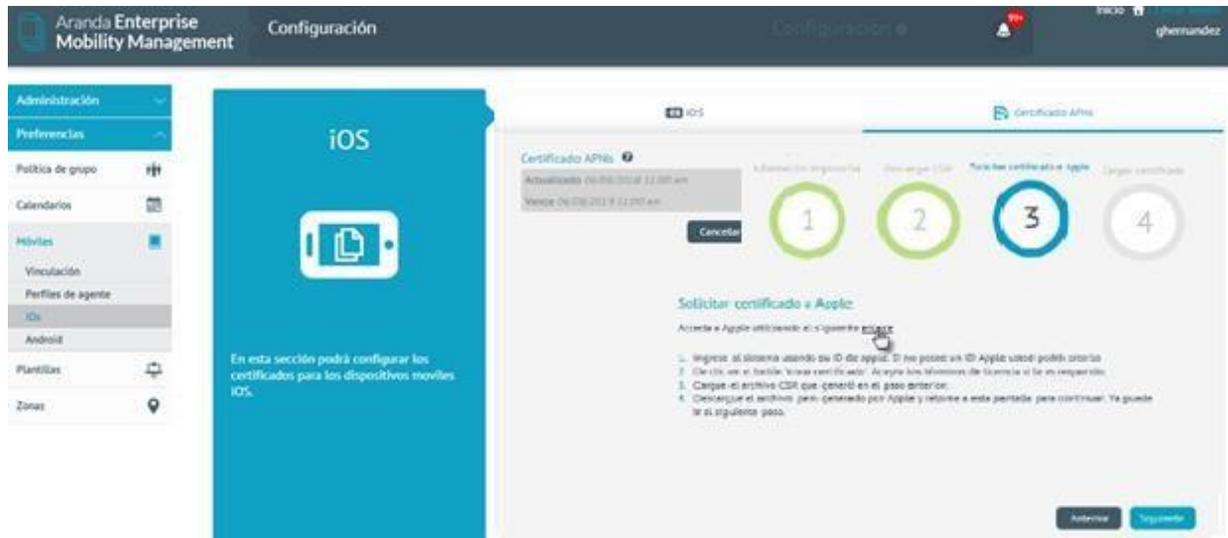
c. En el siguiente paso se descargará automáticamente el archivo CSR que deberá guardar.



- d. Luego envíe el archivo CSR a su representante en Aranda a través de correo electrónico.



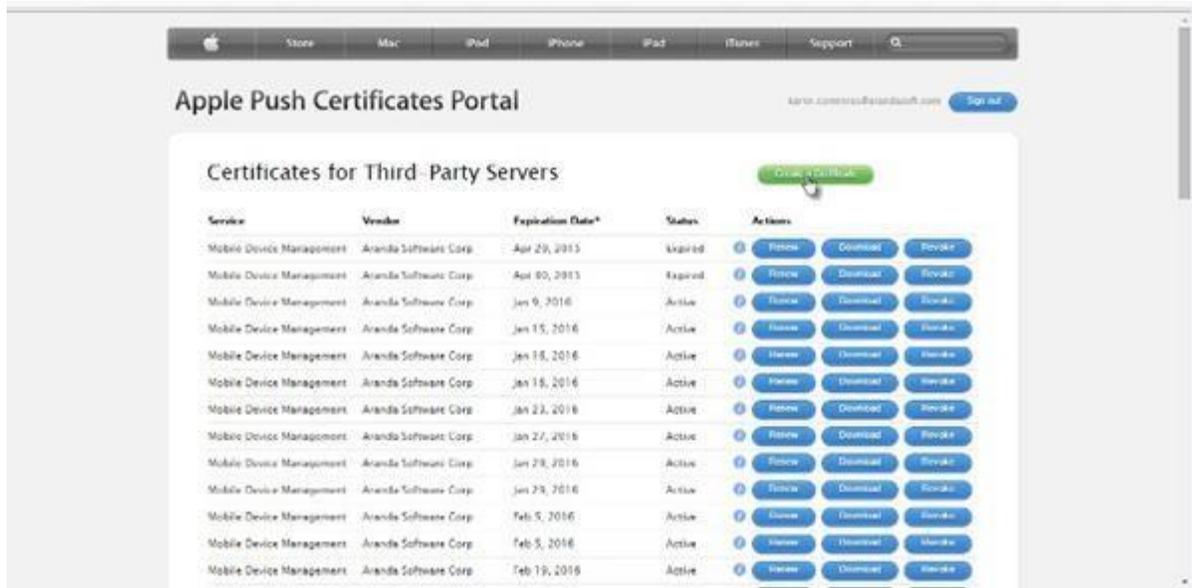
- e. Ingrese a la página de Apple para generar el certificado APNs



f. Digite su Apple ID y contraseña



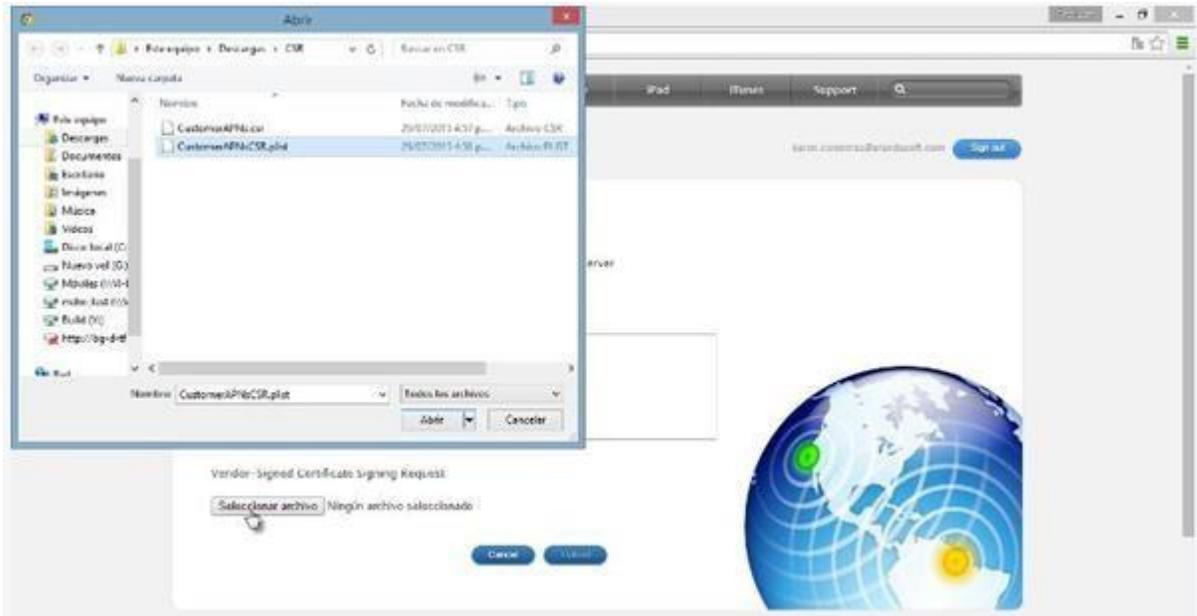
g. Luego de clic en la opción **Crear certificado**



h. Acepte términos y condiciones.



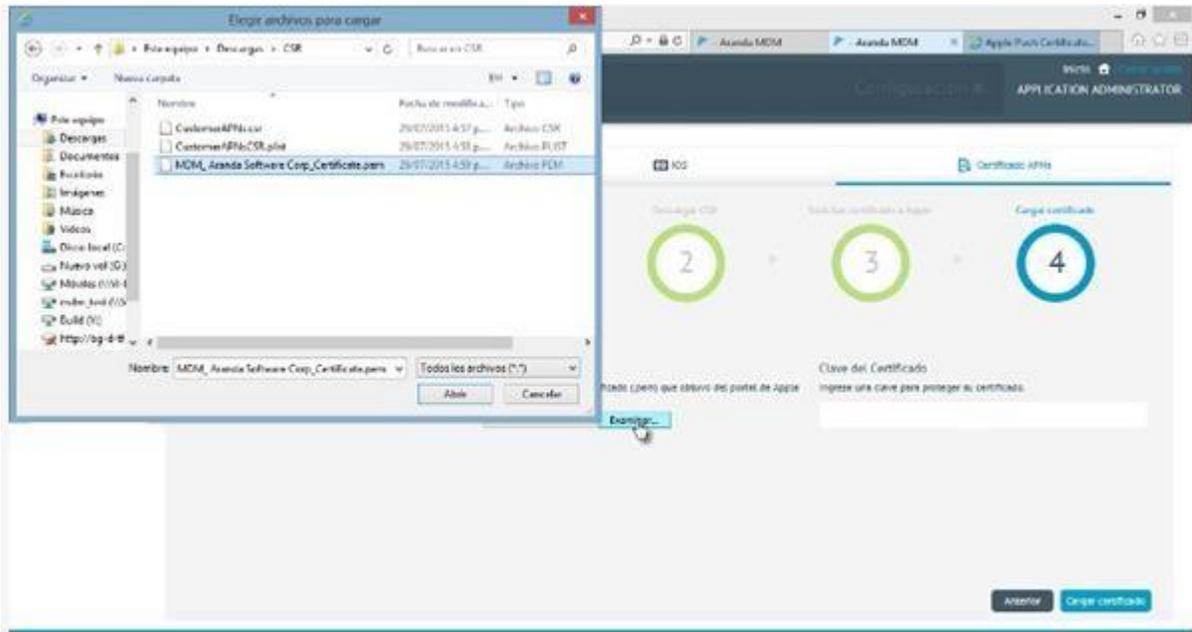
i. Seleccione el archivo “PLIST”, que recibió por correo electrónico del representante en Aranda.



- j. Escriba una breve descripción del certificado que se está creando, esto con el objetivo de identificarlo en el futuro. Descargue y guarde el archivo PEM que se genera.



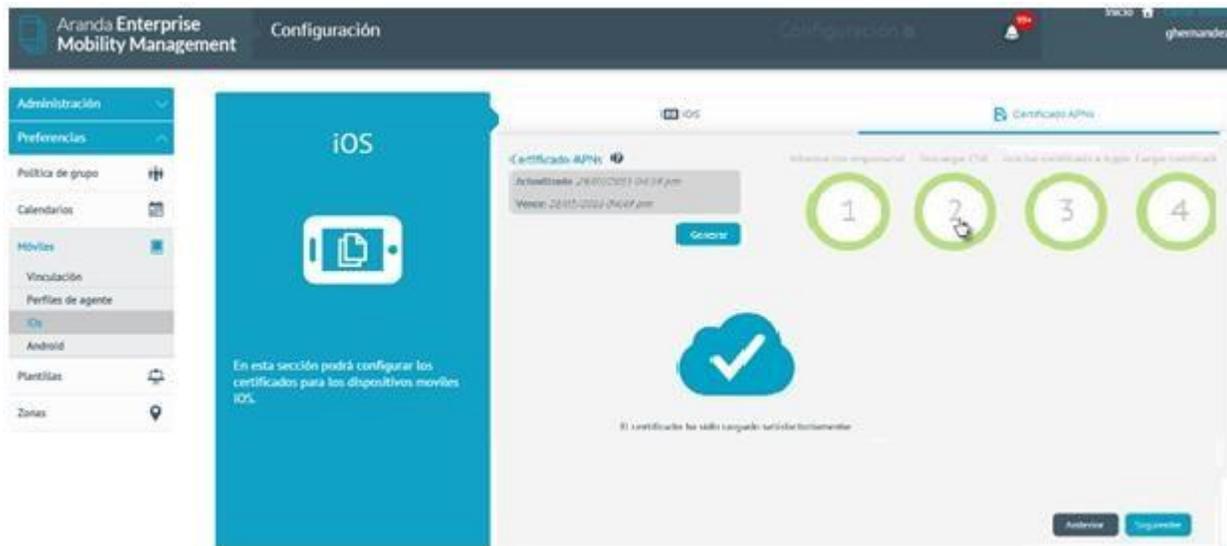
- k. Continúe dentro de la consola, y ahora adjunte el archivo “PEM” que fue generado en el paso anterior.



l. Luego de clic en **Cargar certificado**.



m. El certificado debe quedar cargado exitosamente.



El certificado creado y cargado en el servidor AEMM tendrá validez de un año, contado a partir su generación en la plataforma de APN Push Notificación de Apple.

Este certificado se asocia a las subsiguientes vinculaciones de dispositivos de la plataforma iOS en tanto que no puede reemplazarse con un certificado nuevo, acto tal que tendría como consecuencia el aislamiento de los dispositivos del servidor AEMM y su derivada imposibilidad de recibir y procesar comandos.

Este certificado creado tiene que ser renovado antes de su vencimiento y para tal cuando se crea se pone una alerta de sistema que realiza un recordatorio un mes antes del vencimiento del certificado.

Si no se hace el procedimiento de renovación a tiempo, ocasionará un efecto semejante al de cambiar el certificado por otro nuevo, que es el aislamiento total e irreversible de los dispositivos ya vinculados y que usen el presente certificado APN.

En el siguiente numeral se detalla el proceso de renovación del certificado APN.

Renovación de un certificado APN previamente creado

Ejecute los pasos a,b,c,e,f del proceso anterior (Creación de un Certificado APN Nuevo) y continuación realice lo siguiente:

Una vez en la plataforma de APN de Apple ubique el registro del certificado en cuestión y haga clic en “Renew” (Renovar). Para la identificación del registro en cuestión puede usar la descripción corta ingresada al momento de su creación, esto en el caso de que posea más de un registro en su cuenta de APN.



A continuación, ejecute los pasos h, i, j, k, l, m del numeral anterior, para completar el proceso.

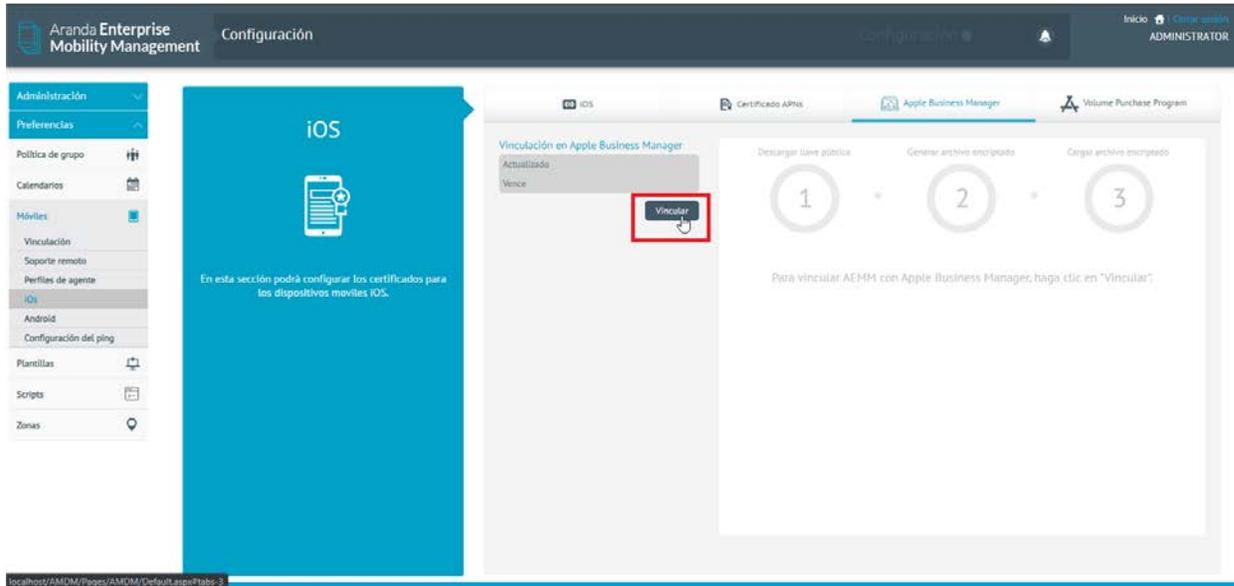
El certificado renovado tendrá el mismo periodo de validez de 1 año y deberá también ser renovado antes que expire, para no alcanzar las consecuencias ya descritas.

4.3.4.3. *Apple Business Manager (ABM)*

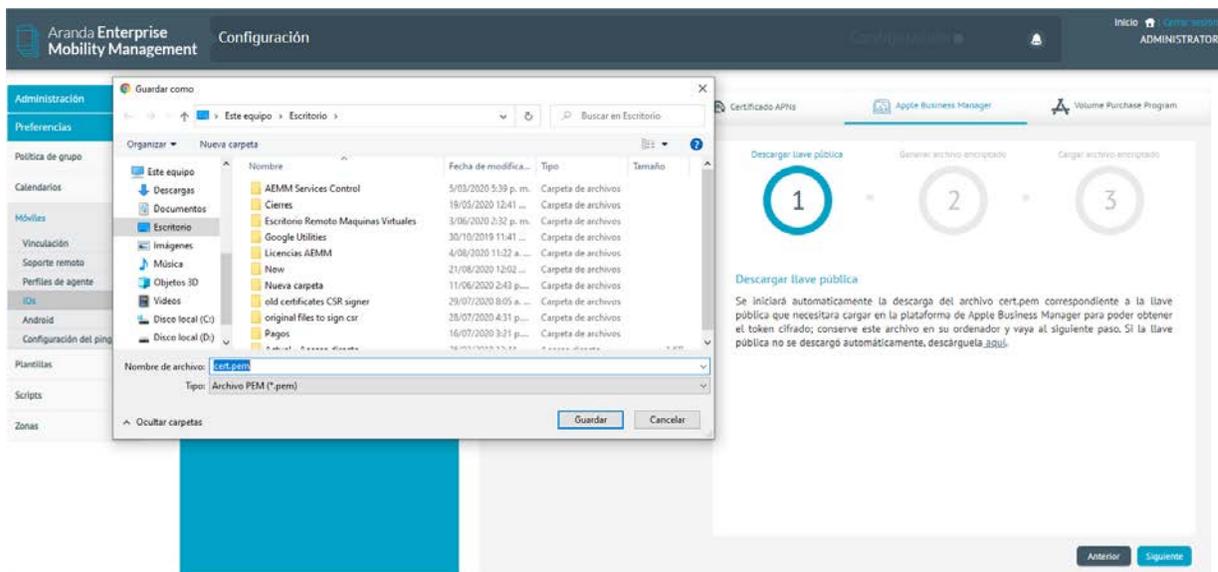
Apple Business Manager es una plataforma para dispositivos Apple que permite una mejor y eficiente gestión, ofreciendo diversas alternativas entre las que se destacan: Supervisión automática, Vinculación de fábrica, más efectivas restricciones, entre otras.

Para activar esta funcionalidad es necesario tener una cuenta vigente en la plataforma de Apple Business Manager (<https://business.apple.com/>) y realizar los siguientes pasos:

Navegue hasta la pestaña Apple Business Manager y haga clic en Vincular



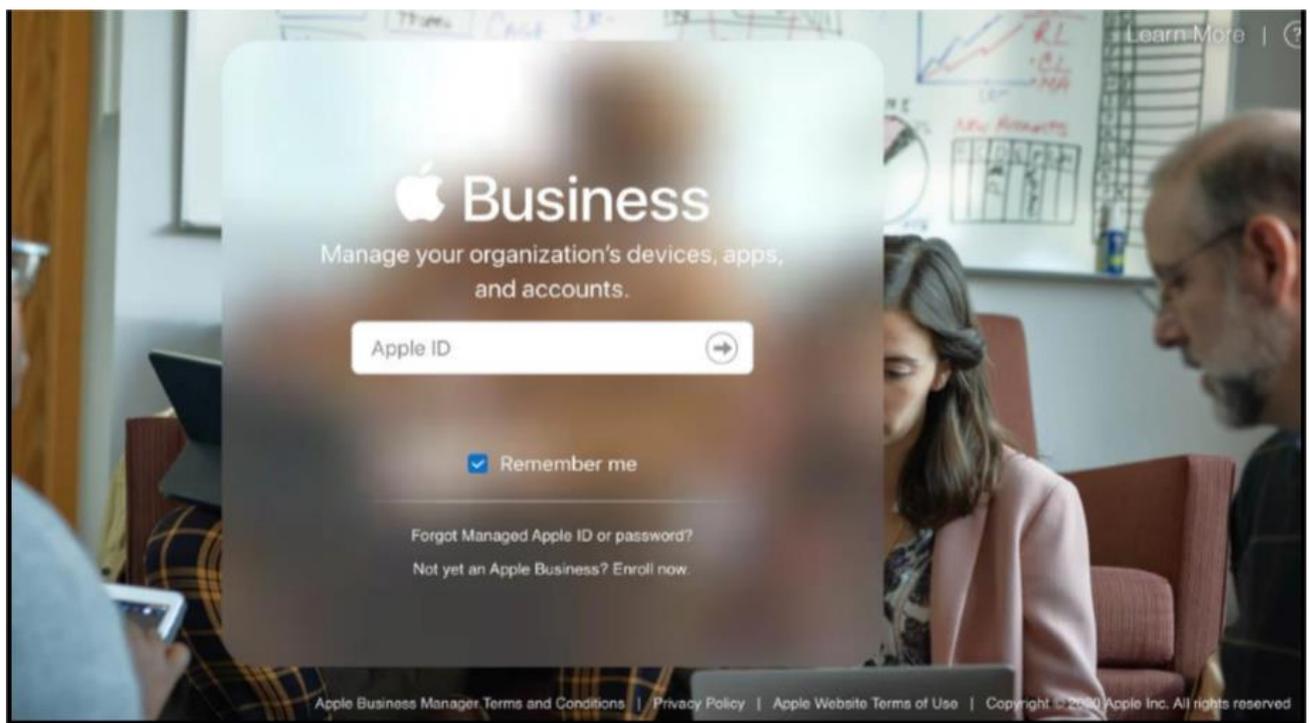
Guarde el archivo cert.pem que identificará la instancia del servidor AEMM de manera única. Guárdelo en un lugar seguro y haga clic en siguiente.



A continuación, se darán las indicaciones correspondientes para vincular la consola AEMM con la llave pública descargada en el paso anterior, en la consola de administración de Apple Business Manager.

The screenshot shows the 'Configuración' (Configuration) page for 'Aranda Enterprise Mobility Management'. The left sidebar contains a navigation menu with options like 'Administración', 'Preferencias', 'Política de grupo', 'Calendarios', 'Móviles', 'Vinculación', 'Soporte remoto', 'Perfiles de agente', 'iOS', 'Android', 'Configuración del ping', 'Plantillas', 'Scripts', and 'Zonas'. The main content area is titled 'iOS' and features a blue banner with a smartphone icon and the text: 'En esta sección podrá configurar los certificados para los dispositivos móviles iOS.' Below this, there are three steps for generating an encrypted archive: 1. 'Descargar clave pública', 2. 'Generar archivo encriptado', and 3. 'Cargar archivo encriptado'. The second step is currently active. A list of instructions for step 2 is provided: 1. Iniciar sesión en el portal web del Programa Apple Business Manager. 2. Ir a Configuración > Configuración de la administración de dispositivos > Agregar servidor MDM. 3. Ingresar Nombre del servidor MDM: Aranda EMM y Cargar la clave pública cert.pem que se descargó en el paso anterior; finalmente Guardar para finalizar la creación. 4. Seleccionar el servidor Aranda EMM y Descargar Identificador (archivo encriptado en formato .p7m).

Ingresar a la consola de Apple Business Manager <https://business.apple.com/> e ingresar ésta.



Una vez dentro de la consola de administración de ABM diríjase a la opción **Configuración**, y ahí seleccione **Configuración de la administración de dispositivos**.

The screenshot displays the Apple Business Manager console interface. On the left is a navigation sidebar with categories like 'Organización', 'Actividad', 'Ubicaciones', 'Personas', 'Cuentas', 'Funciones', 'Dispositivos', 'Asignaciones de disp...', 'Historial de asignación', 'Contenido', and 'Apps y libros'. The 'Configuración' option is highlighted at the bottom. The main content area is divided into two columns. The left column contains 'Configuración personal' (Mi perfil, Apps y libros) and 'Configuración de la organización' (Información de inscripción, Cuentas, Configuración de la administración de dispositivos - highlighted, Servidores MDM). The right column shows 'Configuración de la administración de dispositivos' with a purple icon, '2 dispositivos', and an 'Agregar servidor MDM' button. Below this is the 'Números de cliente' section with instructions on adding client numbers or IDs.

Seleccione **Agregar servidor MDM**, llene el campo **Nombre del servidor MDM** y cargue el archivo de la llave pública que se obtuvo en la consola de AEMM

Información del servidor MDM

Nombre del servidor MDM

Permitir el uso de este Servidor MDM para dar de baja dispositivos. [Más información](#)

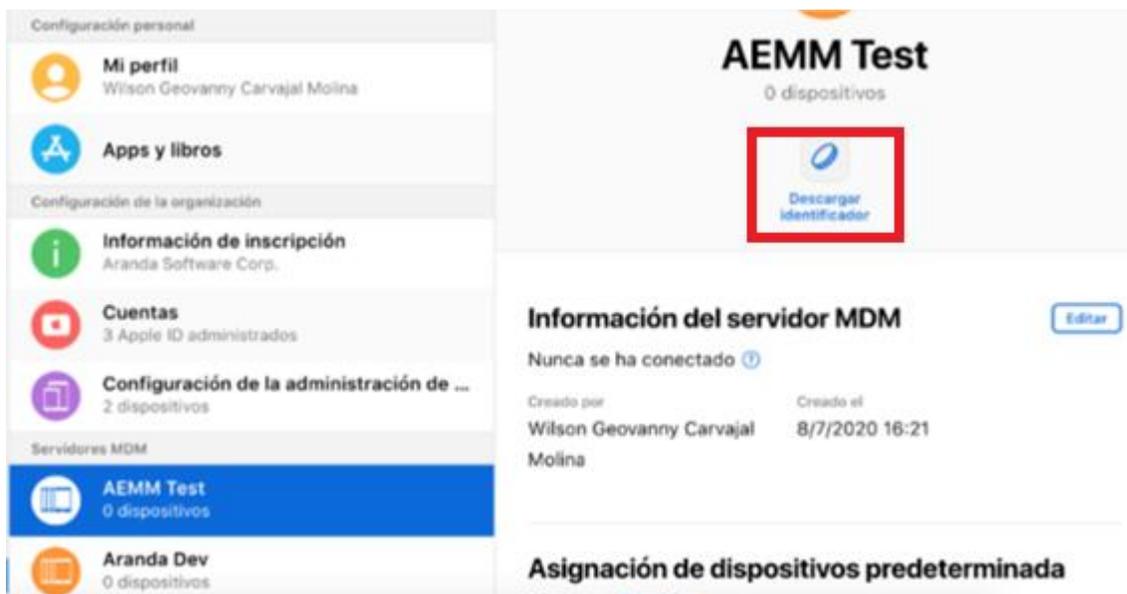
Configuración del servidor MDM

Cargar la clave pública [?](#)

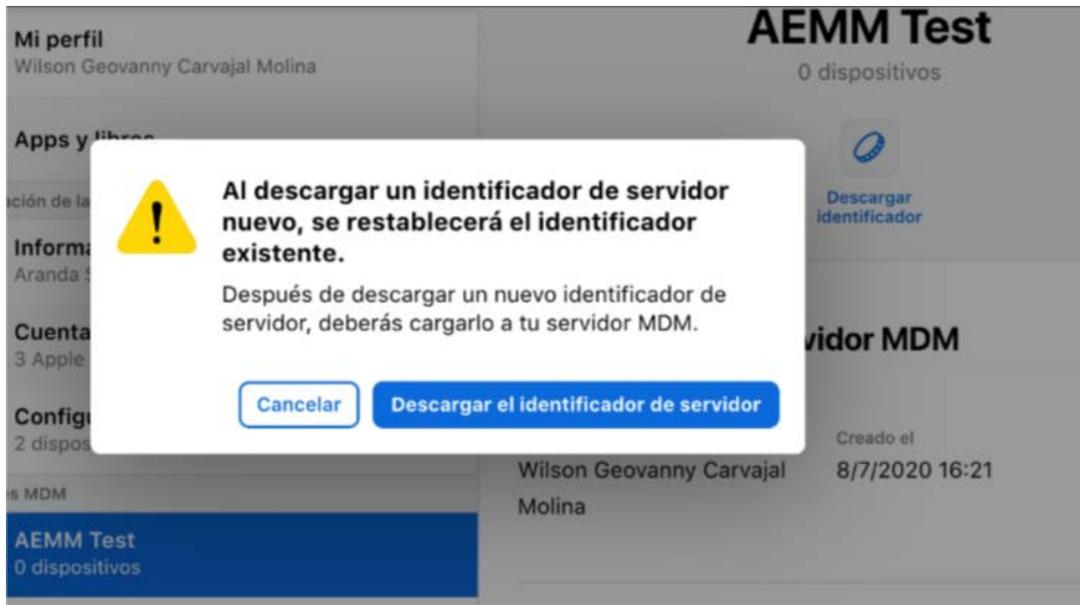


Generar un identificador de servidor nuevo

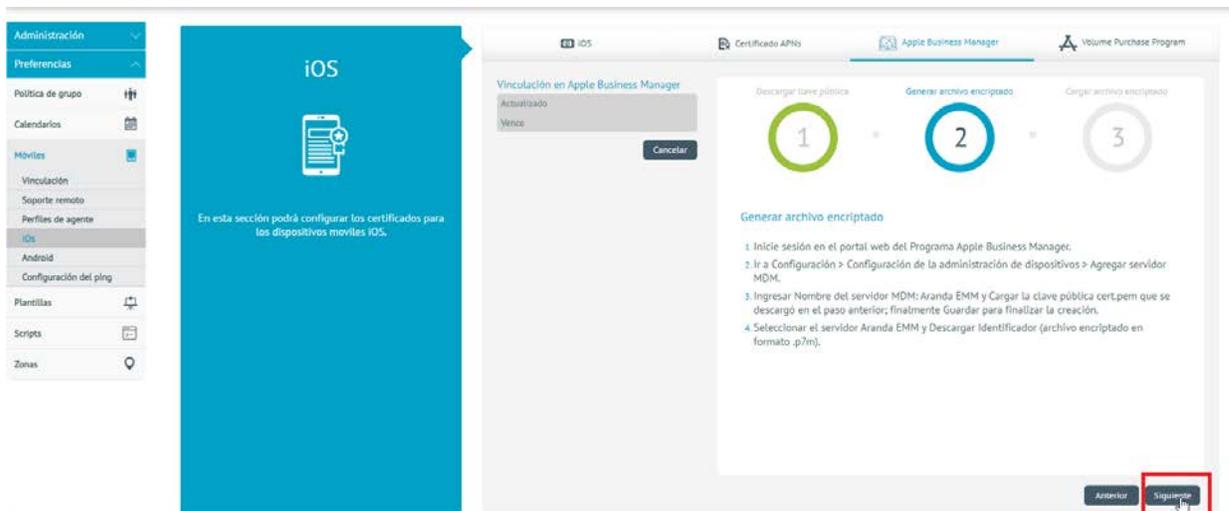
Seleccione Guardar y para finalizar descargue del archivo con extensión p7m en la opción **Descargar identificador**.



The screenshot shows the 'AEMM Test' MDM server configuration page in the Settings app. The left sidebar contains navigation options: 'Configuración personal' (Mi perfil, Apps y libros), 'Configuración de la organización' (Información de inscripción, Cuentas, Configuración de la administración de ...), and 'Servidores MDM' (AEMM Test, Aranda Dev). The main content area shows the server name 'AEMM Test' with '0 dispositivos'. A red box highlights the 'Descargar identificador' button. Below this, the 'Información del servidor MDM' section shows 'Nunca se ha conectado' and details: 'Creado por Wilson Geovanny Carvajal Molina' and 'Creado el 8/7/2020 16:21'. At the bottom, there is a section for 'Asignación de dispositivos predeterminada'.

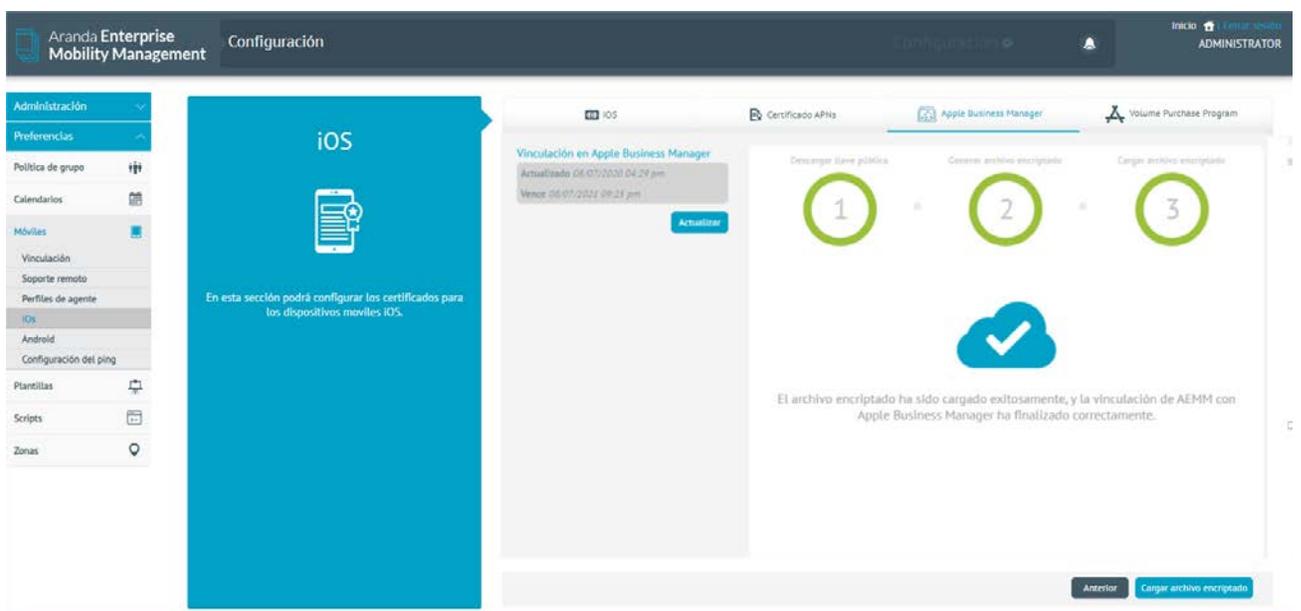
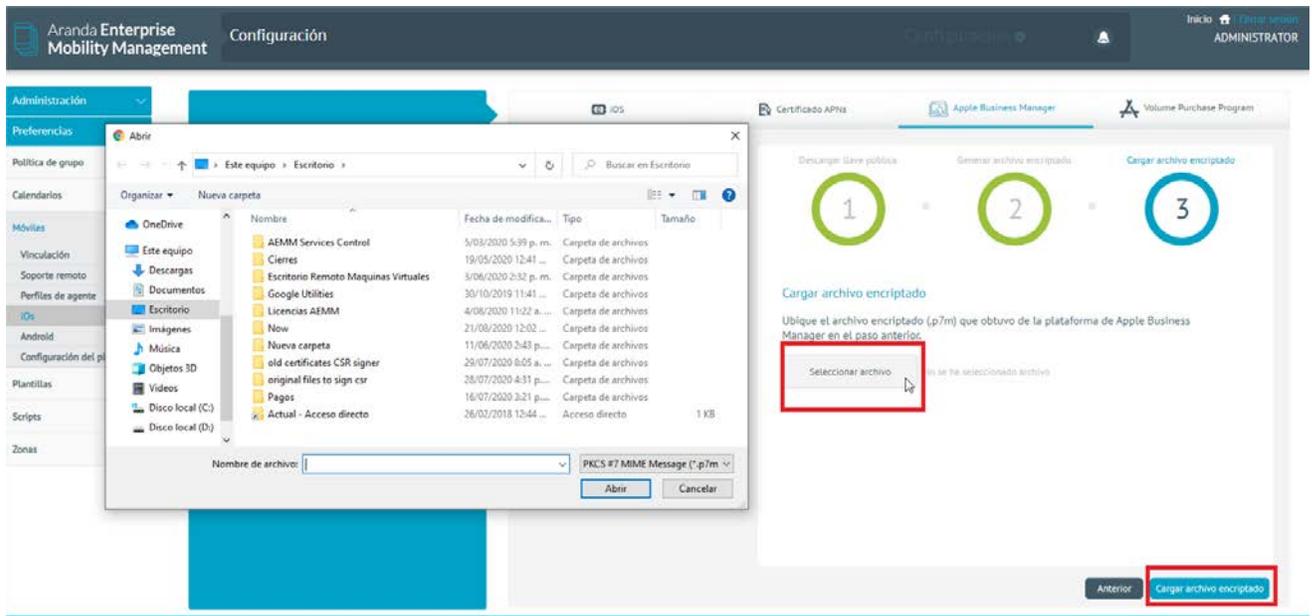


De vuelta en la consola de AEMM haga clic en siguiente



Luego proceda a cargar en la consola AEMM el archivo de extensión p7m descargado de la consola de administración de Apple Business Manager. Haga clic en el botón Seleccionar archivo y cargue el archivo de extensión p7m.

Después de seleccionar el archivo, haga clic en el botón Cargar archivo encriptado



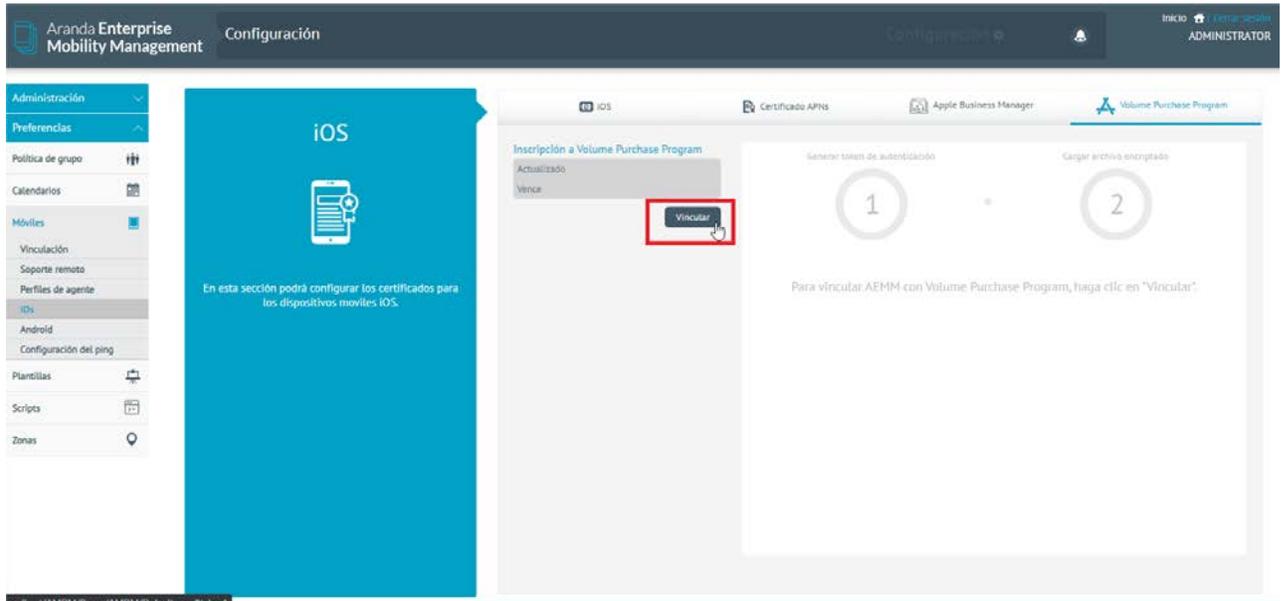
4.3.4.4. Volume Purchase Program (VPP)

Volume Purchase Program de Apple es una plataforma que permite administrar de manera centralizada y eficiente las aplicaciones, libros y demás contenidos ofrecidos en la tienda de iTunes.

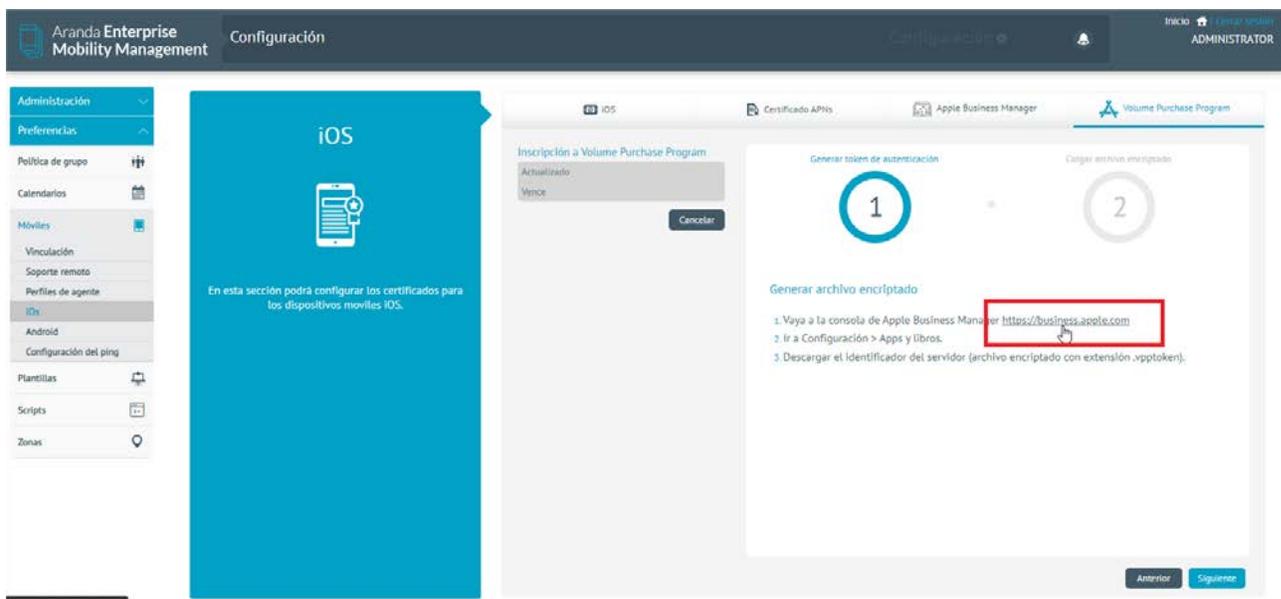
AEMM ofrece la compatibilidad con VPP a nivel de administración de aplicaciones, licencias de aplicaciones y asignación de licencias a dispositivos vinculados a través de Apple Business Manager (ABM).

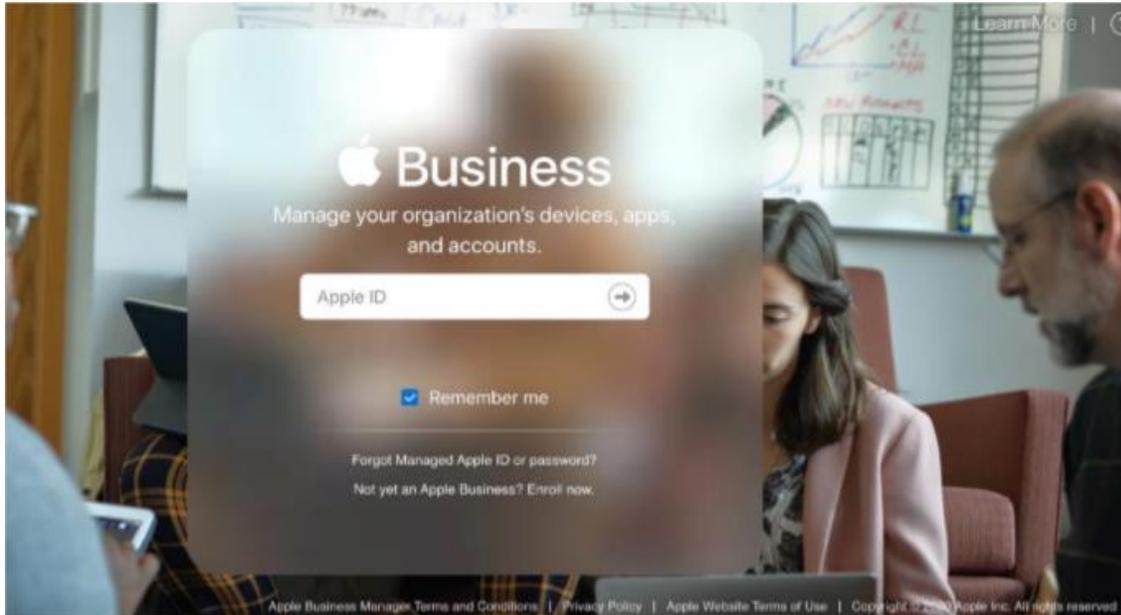
Para vincular el servidor AEMM con VPP realice las siguientes acciones:

En la pestaña Volume Purchase Program, haga clic en **Vincular**



Conforme a las instrucciones que se muestran diríjase a la consola de Apple Business Manager, para generar el token de autenticación



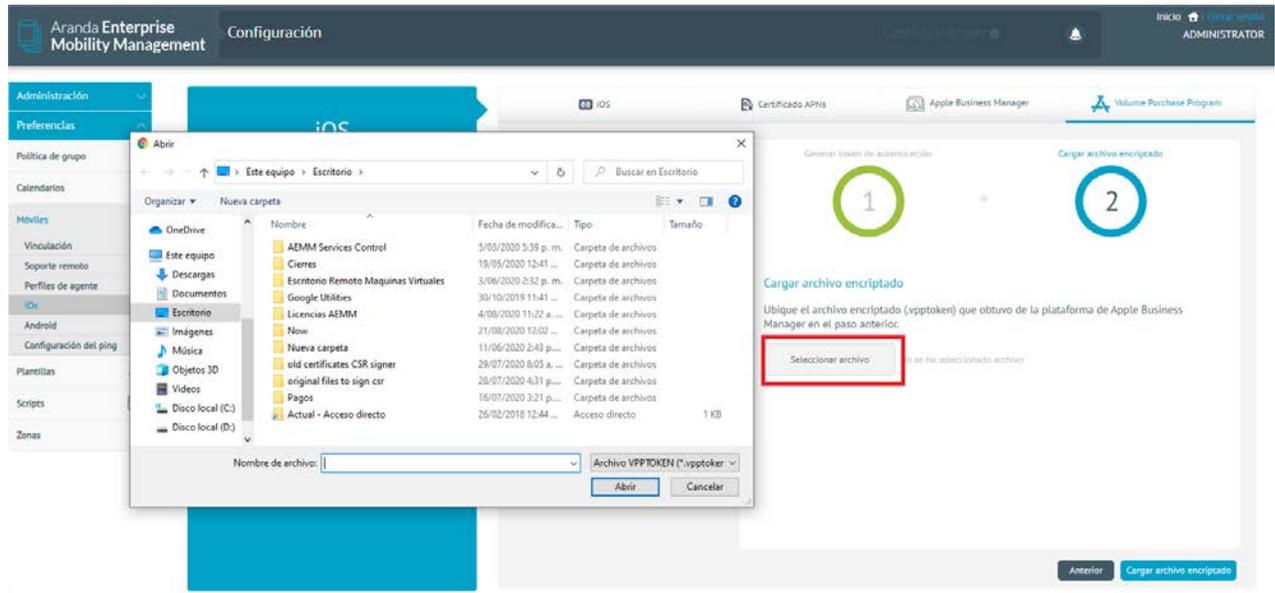


Una vez dentro de la consola de administración de ABM diríjase a la opción **Configuración > Apps y Libros**, allí visualizará la identificación de los servidores configurados; haga clic en **Descargar**.

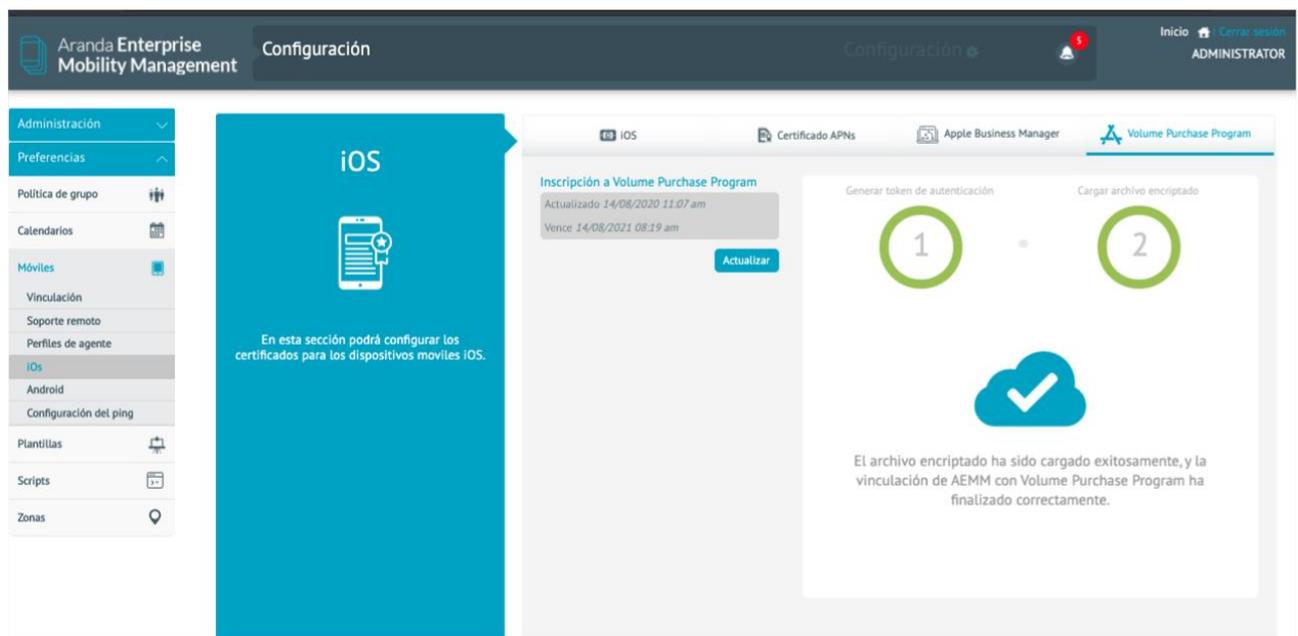
Ubicación	Identificador de servidor
Aranda Software Corp.	Descargar

Guarde el archivo descargado en un lugar seguro, diríjase a la consola de AEMM y haga clic en **Siguiente**.

El paso siguiente es cargar el archivo descargado de la consola ABM del paso anterior, haga clic en el botón **Seleccione archivo** y cargue el archivo.



Por último, haga clic en **Cargar archivo encriptado** para finalizar el proceso



Al actualizar la página y hacer clic en el botón **Sincronizar licencias**, el sistema realizará una asignación automática de licencias del agente AEMM para iOS en los dispositivos que se encuentran vinculados por ABM.

Finalmente, usted observará datos correspondientes a las licencias de Aranda EMM, tales como su estado (disponibles y en uso), la fecha de inscripción del VPP y su vencimiento. Recuerde que las licencias tienen una duración de 1 año.

También aparece una opción para descargar un archivo de resultados, que indica a cuáles dispositivos se les asignó la licencia y a cuáles no.

En consola AEMM:

The screenshot displays the Aranda Enterprise Mobility Management console. The top navigation bar includes 'Aranda Enterprise Mobility Management', 'Configuración', and user information. The left sidebar lists various management options. The main content area is titled 'iOS' and contains a blue informational panel. The 'Volume Purchase Program' tab is selected, showing a table for 'Inscripción a Volume Purchase Program' with columns for 'Actualizado' and 'Vencer'. Below this is a 'Licencias de Aranda MDM Agent' section with a table showing 'Disponibles' (1998) and 'En uso' (2). A 'Sincronizar licencias' button is located at the bottom right of the main content area.

En consola ABM – VPP

The screenshot displays the Aranda EMM Agent console interface. On the left, a sidebar menu includes sections like 'Business', 'Organización', 'Actividad', 'Ubicaciones', 'Personas', 'Cuentas', 'Funciones', 'Dispositivos', 'Asignaciones de dis...', 'Historial de asignaci...', 'Contenido', and 'Apps y libros'. The main area shows a list of installed and available apps:

- Facebook**: 2 en uso, 8 disponibles, USD 0.00
- WhatsApp Messenger**: 3 en uso, 57 disponibles, USD 0.00
- Instagram**: 10 disponibles, USD 0.00
- Aranda EMM Agent**: 2 en uso, 1998 disponibles, USD 0.00 (highlighted)
- Beer24**: 2 en uso, 8 disponibles, USD 0.00
- Aranda MDM Content Manage...**: 3 en uso, 77 disponibles, USD 0.00
- Aranda Secure Web Browser**: 30 disponibles, USD 0.00

On the right, the 'Aranda EMM Agent' app details are shown, including a 'Comprar licencias' section with a form to assign licenses to a location, a price of USD 0.00, and a quantity of 0. Below this is an 'Administrar licencias' table:

Ubicación	En uso	Disponibil...
Aranda Software Corp.	2	1998
Total	2	1998

Aspectos a tener presente:

- Antes de realizar la sincronización debe haber licencias disponibles de la aplicación de Aranda EMM en ABM para los dispositivos que se vayan a asignar.
- La aplicación Aranda EMM Agent debe estar importada en el módulo de aplicaciones de la consola de AEMM.

4.3.5. Android for work

En esta sección podrá configurar las opciones necesarias para activar la compatibilidad con el entorno de trabajo empresarial para dispositivos Android, llamado Android for Work (AFW).

4.3.5.1. Pestaña “Android For Work”

Android For Work o actualmente llamado Android Enterprise es una Infraestructura y Plataforma Integrada para la gestión de dispositivos Android, creada por Google.

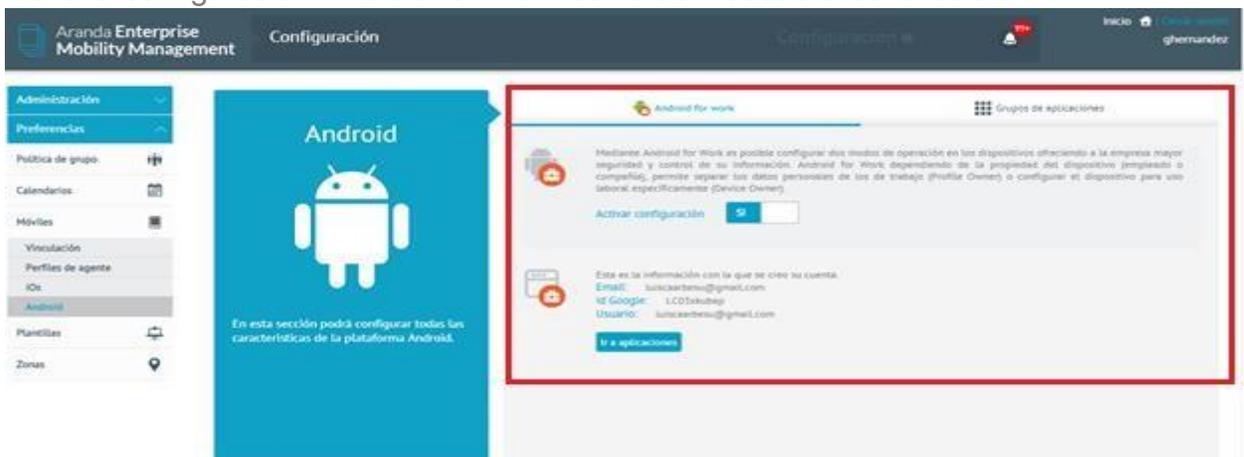
AFW ofrece funcionalidades de gestión de dispositivos a nivel de aplicaciones, restricciones y configuraciones que permiten a AEMM tener un mayor control sobre los dispositivos de la plataforma Android.

Para el uso de AFW en AEMM se deben de seguir los siguientes pasos:

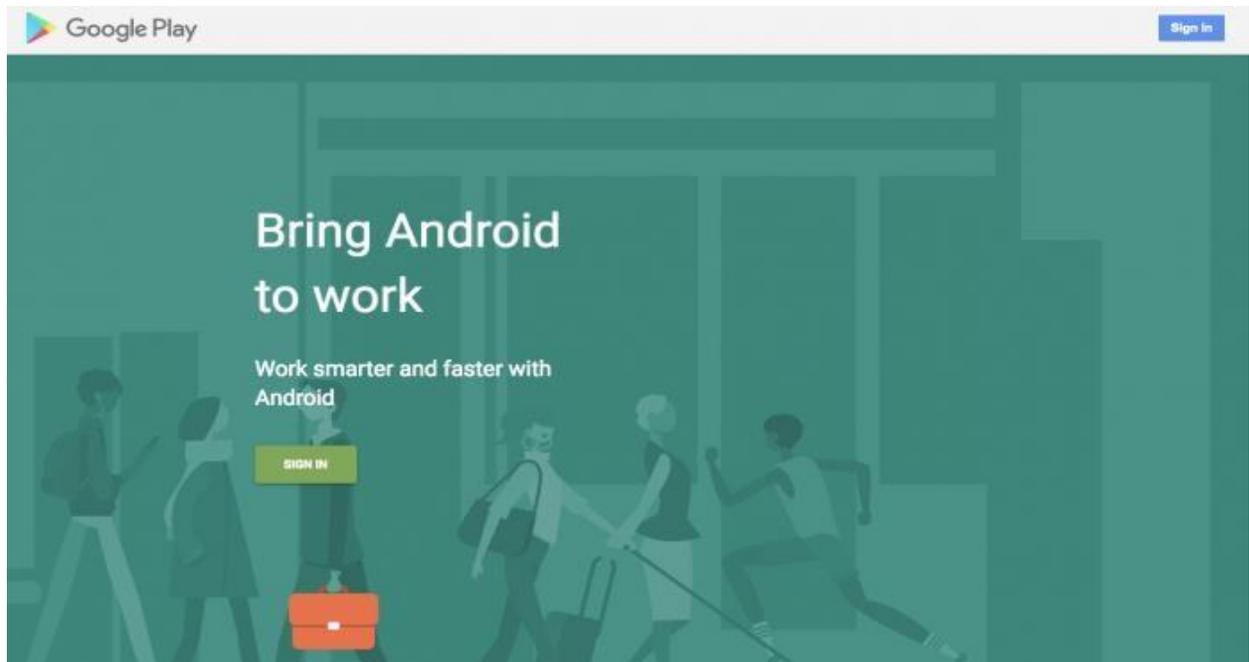
Seleccione **configuración** en la parte superior derecha de la consola, luego dentro de la sección **preferencias** en el costado izquierdo, seleccione **Móviles**, dentro de esta sección de clic en **Android**.



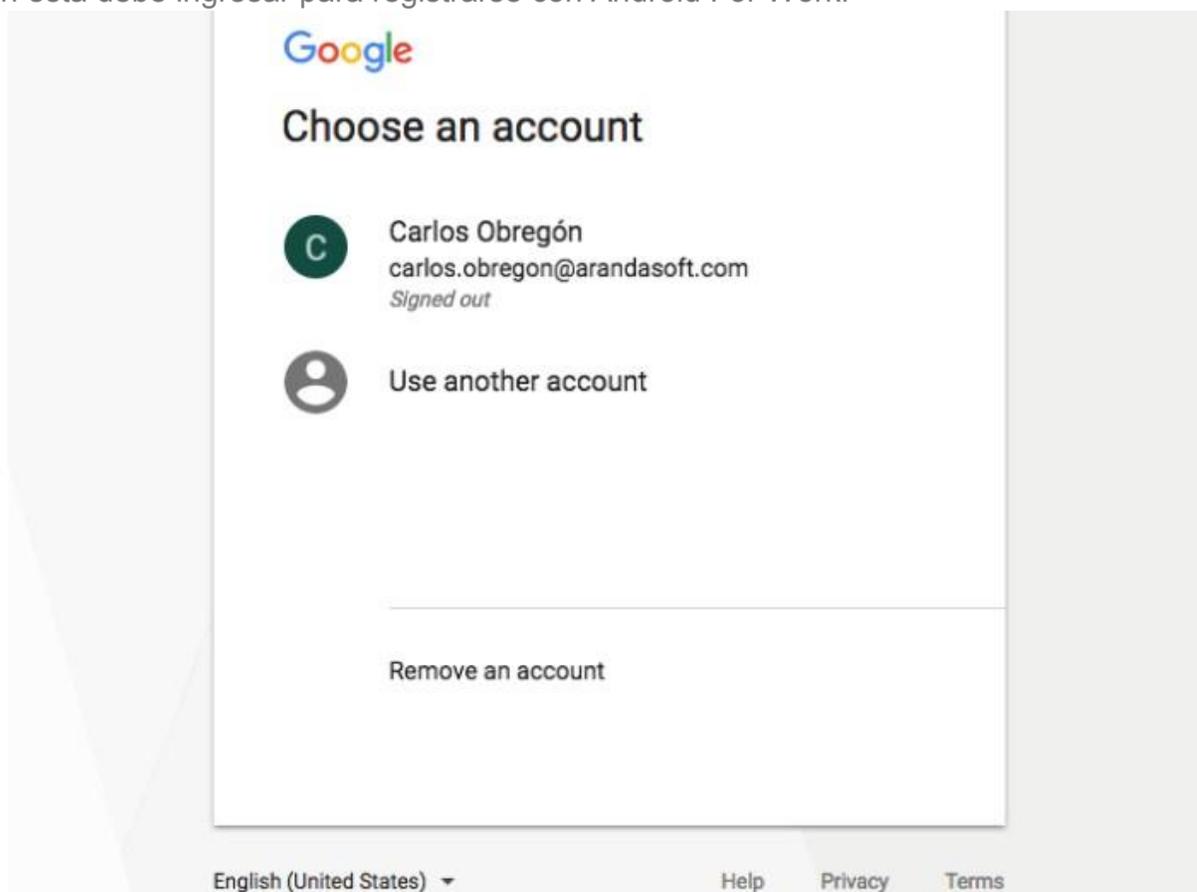
Active la configuración Android for Work como se muestra a continuación.



Siga la guía de activación de google.



Dentro de esta activación es necesario una cuenta administradora de la organización. Con esta debe ingresar para registrarse con Android For Work.



Luego diligencie el formulario de registro solicitado por google y confirme el registro



Si el proceso es exitoso, la consola EMM se debe ver de la siguiente forma:



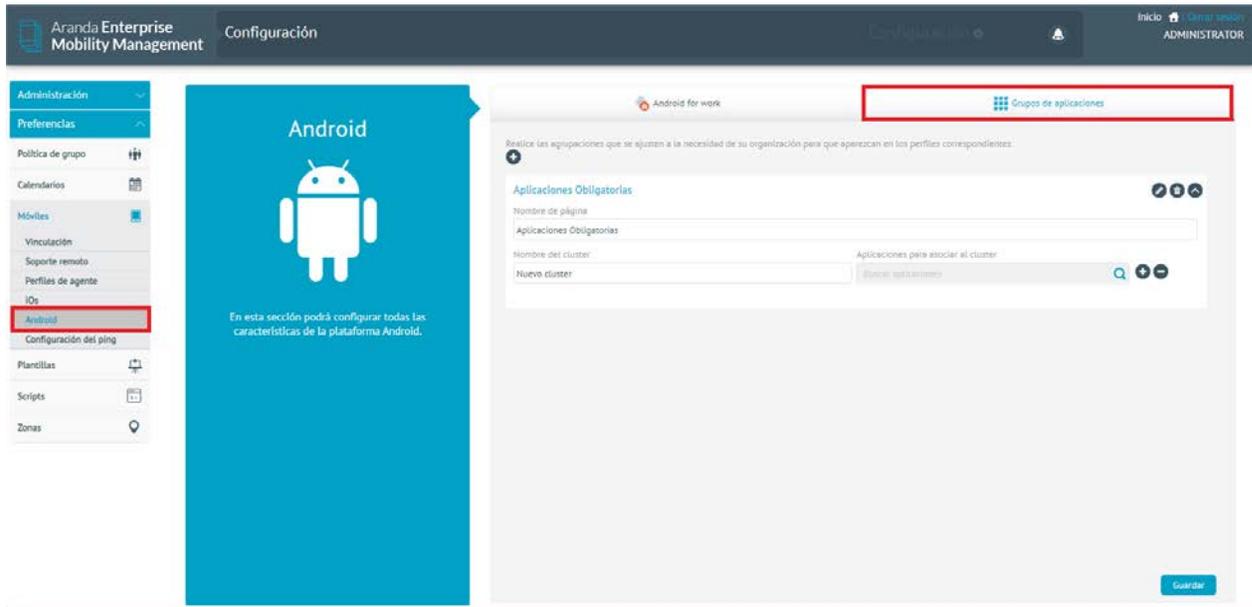
4.3.5.2. Grupos de Aplicaciones en Android For Work

Los grupos de aplicaciones en Android For Work son una característica ofrecida por Google para ordenar en páginas y clústeres (secciones) las aplicaciones que han sido aprobadas para AFW.

Las páginas son como su nombre lo indica, páginas que son navegables en la tienda administrada por AFW en los dispositivos, y los clústeres son secciones dentro de las páginas donde se colocarán ya las aplicaciones aprobadas en AFW.

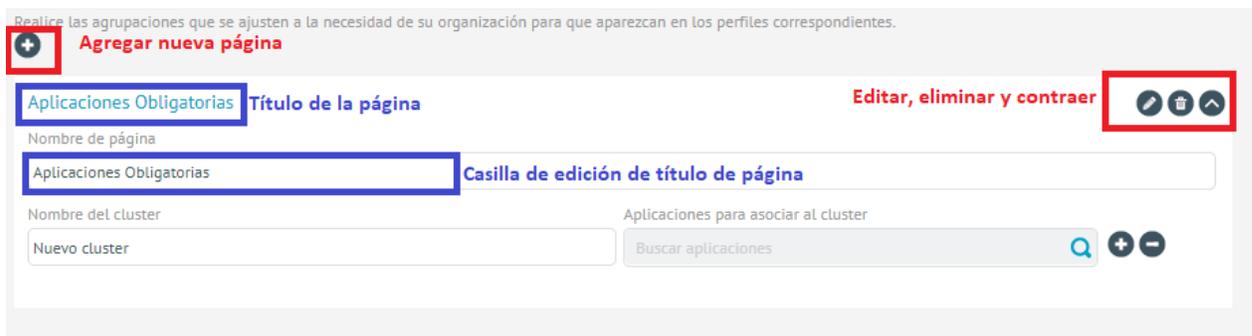
Las páginas y clústeres configurados aquí se reflejarán en la distribución de la tienda administrada para todos los dispositivos Android que hayan sido vinculados bajo cualquiera de las modalidades que ofrece AFW.

Para gestionar los grupos de aplicaciones diríjase a la pestaña **Grupos de aplicaciones** en la sección **Android**.



Esta sección está dividida en 2 partes anidadas: Gestión de páginas y Gestión de clústeres.

Gestión de páginas



Para la gestión de páginas se presentan los siguientes controles:

- Botón de agregar nueva página: Agrega una nueva página y la coloca en última posición

- Editar página: Activa los controles internos para editar título y clústeres contenidos en la página
- Eliminar página: Elimina toda la página y los clústeres contenidos en ella.
- Contraer página: Contrae la visualización de la página, dejando visible su título únicamente.

Gestión de Clústeres

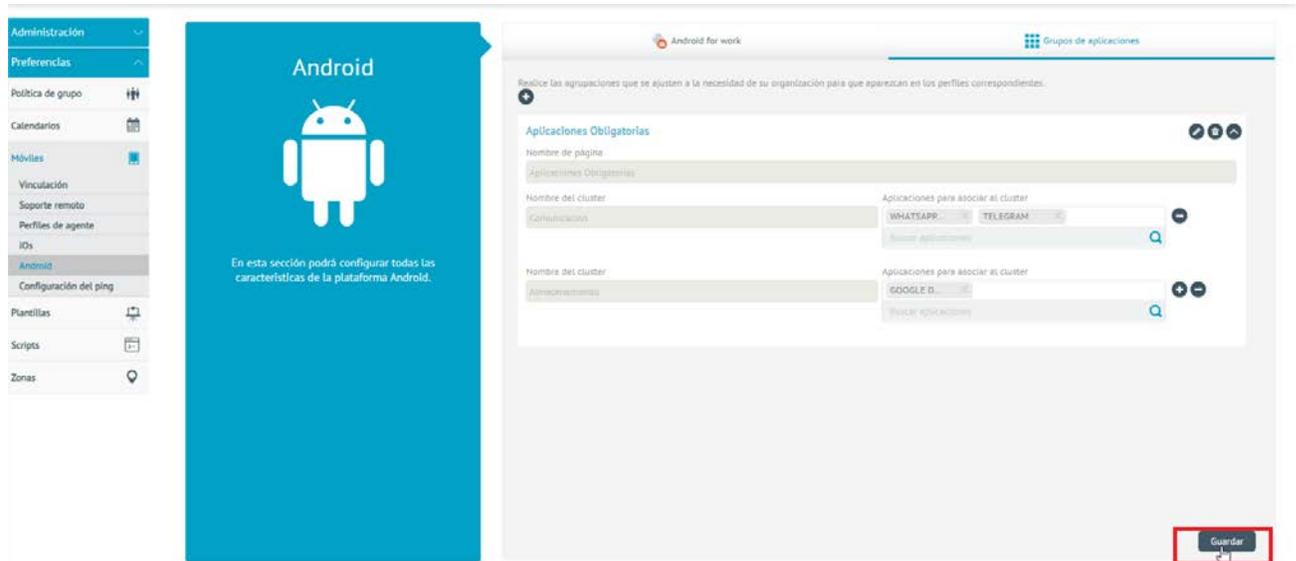
The screenshot shows a user interface for managing clusters. It features two main input fields: 'Nombre del cluster' (Cluster Name) and 'Aplicaciones para asociar al cluster' (Applications to associate with the cluster). The 'Nombre del cluster' field contains the text 'Nuevo cluster' and is highlighted with a blue border. Below it is the label 'Casilla de edición del nombre del clúster'. The 'Aplicaciones para asociar al cluster' field contains the text 'Buscar aplicaciones' and a search icon, and is also highlighted with a blue border. Below it is the label 'Casilla de búsqueda de aplicaciones aprobadas en AFW'. To the right of the search field are two buttons: a plus sign (+) and a minus sign (-), both highlighted with a red border. To the right of these buttons is the text 'Agregar, eliminar clúster'.

Para la gestión de clústeres se presentan los siguientes controles:

- Agregar clúster: Agrega un clúster a la página y lo coloca en la última posición. Este control solo es visible para el último clúster.
- Eliminar clúster: Elimina el clúster actual
- Casilla de edición de nombre de clúster: Se presenta el nombre actual del clúster, con posibilidad de editarlo.
- Casilla de búsqueda de aplicaciones aprobadas en AFW: Al escribir en esta casilla se realiza una búsqueda coincidente en las aplicaciones actualmente aprobadas en AFW, y se despliegan las coincidencias con la posibilidad de agregarlas al clúster.

Gestiones Finales

Una vez se haya hecho la configuración de páginas y clústeres es preciso guardar la configuración hecha para que se aplique a los dispositivos, esto se hace dando clic en el botón guardar.



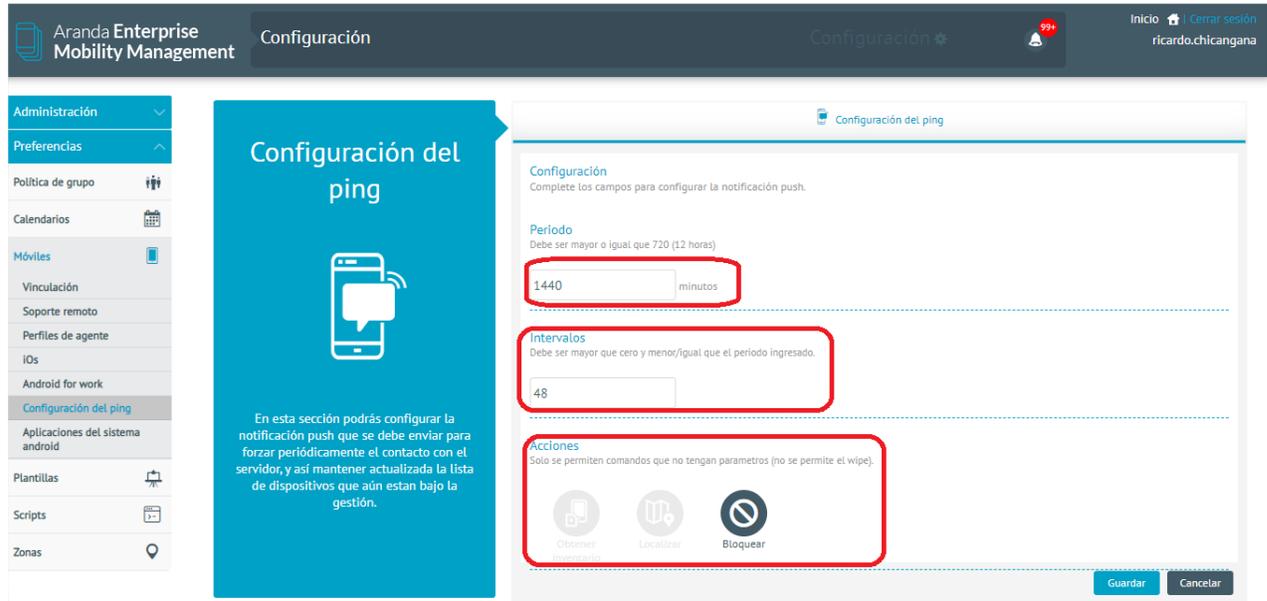
Si todas las aplicaciones aprobadas para AFW no han sido incluidas en la configuración de páginas y clústeres, se creará automáticamente una página adicional llamada “Otras Aplicaciones”, con un clúster por defecto en el que se incluirán el resto de aplicaciones.

Puede tardar algún intervalo de tiempo en que las tiendas administradas se actualicen con la configuración realizada en servidor, esto depende de la calidad de conectividad que tenga cada dispositivo con la tienda administrada de Google.

4.3.6. Configuración del Ping

En esta sección se puede configurar la notificación push que se debe enviar a los dispositivos para forzar periódicamente el contacto con el servidor, y así mantener actualizado la lista de dispositivos gestionados.

Para configurar el ping diligencie las siguientes opciones:



Configuración del ping

En esta sección podrás configurar la notificación push que se debe enviar para forzar periódicamente el contacto con el servidor, y así mantener actualizada la lista de dispositivos que aún están bajo la gestión.

Configuración
Complete los campos para configurar la notificación push.

Periodo
Debe ser mayor o igual que 720 (12 horas)

1440 minutos

Intervalos
Debe ser mayor que cero y menor/igual que el periodo ingresado.

48

Acciones
Solo se permiten comandos que no tengan parámetros (no se permite el wipe).

Obtener inventario Localizar Bloquear

Guardar Cancelar

- **Periodo:** Duración de un ciclo de ping hacia todos los dispositivos. Tras finalizar este intervalo todos los dispositivos han recibido al menos una notificación push.
- **Intervalos:** Cantidad de grupos de dispositivos en los que se dividirá el conjunto total de dispositivos vinculados. Esto para no encolar todas las notificaciones push al tiempo, sino basadas en esta cantidad de grupos.
- **Acciones:** Comandos que se encolaran antes de enviar la notificación push a cada dispositivo, se pueden escoger comandos de: Inventario, Localización y bloqueo de pantalla.

Una vez realizada las anteriores configuraciones haga clic en “Guardar”, para persistir y activar el mecanismo de ping.

4.3.7. Aplicaciones del sistema Android

En esta sección de pueden gestionar los nombres de paquetes utilizados para ser visualizados en dispositivos Android en modo de vinculación AFW Device Owner.

Estos paquetes son usados en la sección de aplicaciones del módulo de políticas y en la sección kiosco del mismo módulo.

Los paquetes agregados serán enviados a los dispositivos como parte de la política que incluya los ítems ya nombrados.

El dispositivo “destapará” las aplicaciones correspondientes a los nombres de paquetes aquí configurados.

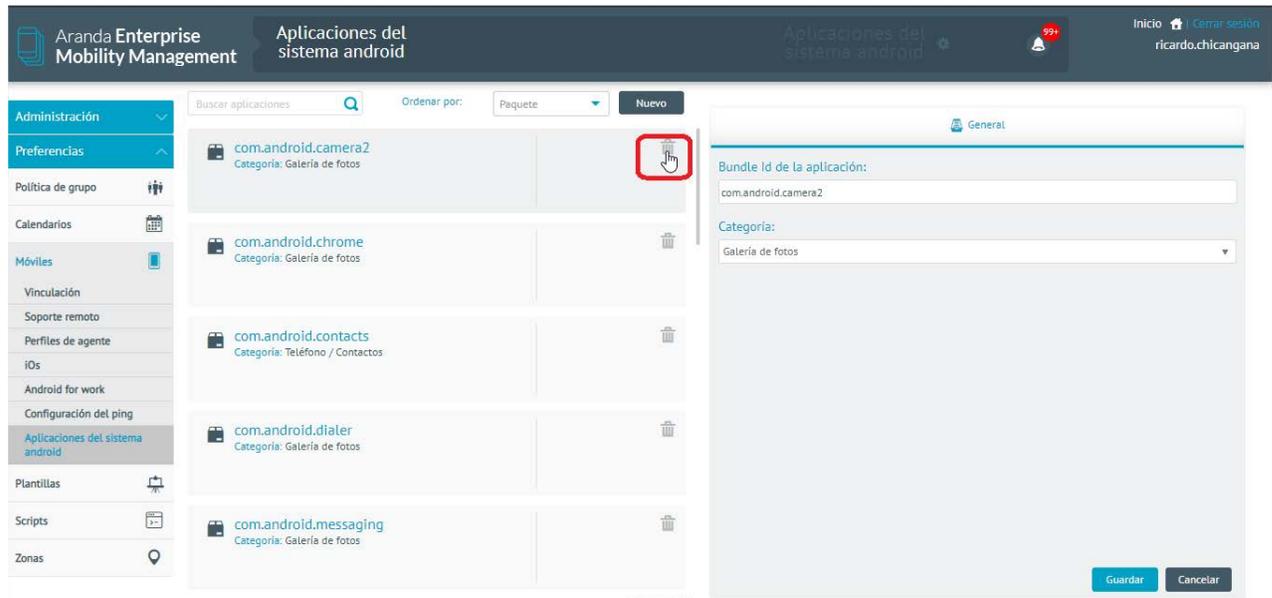
Para configurar un nuevo paquete haga clic en Nuevo y a continuación diligencie los datos de Bundle Id de la aplicación y Categoría, para persistir la información dé clic en Guardar.

The screenshot shows the 'Aplicaciones del sistema android' section. A table lists several packages with their Bundle IDs and categories. The 'Nuevo' button is highlighted in red. The right-hand form is also highlighted in red, showing the 'Bundle Id de la aplicación' field with the value 'com.android.camera2' and the 'Categoría' dropdown menu set to 'Galería de fotos'. The 'Guardar' button at the bottom right of the form is also highlighted in red.

Para editar un paquete existente ubíquelo en la lista de paquetes y actualice sus datos, luego haga clic en Guardar.

The screenshot shows the same interface as the previous one, but now the 'com.android.camera2' package is selected in the list, indicated by a red box and a mouse cursor. The right-hand form is also highlighted in red, showing the 'Bundle Id de la aplicación' field with the value 'com.android.camera2' and the 'Categoría' dropdown menu set to 'Galería de fotos'. The 'Guardar' button at the bottom right of the form is also highlighted in red.

Para eliminar un paquete haga clic en el ícono de eliminar del registro del paquete en cuestión.



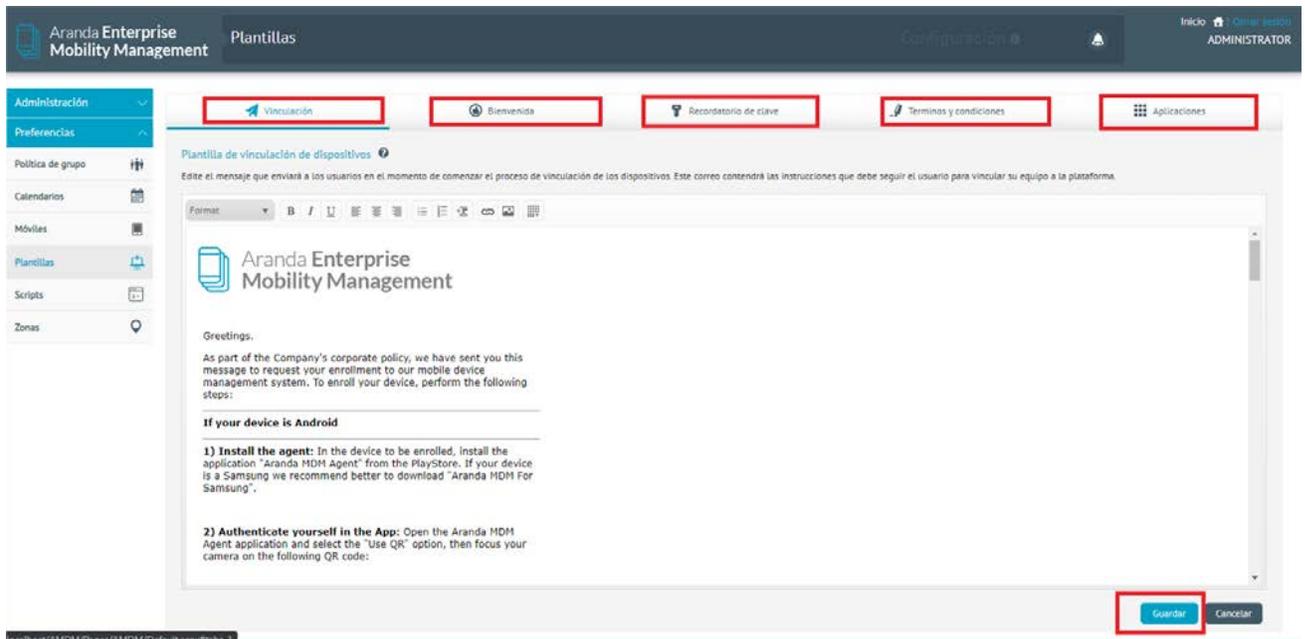
4.4. Plantillas

En esta sección podemos configurar el contenido de los correos electrónicos enviados por el servidor AEMM, al realizar ciertas acciones.

Dentro de las plantillas de correo podemos configurar las siguientes opciones:

- Bienvenida: Este nos permite configurar un saludo y el envío de confirmación del nombre de usuario y contraseña.
- Recordatorio de clave: Este nos envía una respuesta automática de la clave cuando esta es olvidada.
- Términos y condiciones: Nos permite configurar en el mensaje el correspondiente párrafo con los términos y condiciones.
- Aplicaciones: Nos envía información acerca de alguna aplicación.

Para configurar algunas de las secciones antes mencionadas, de clic en alguna de estas, luego realice los cambios pertinentes y por último haga clic en **Guardar**.

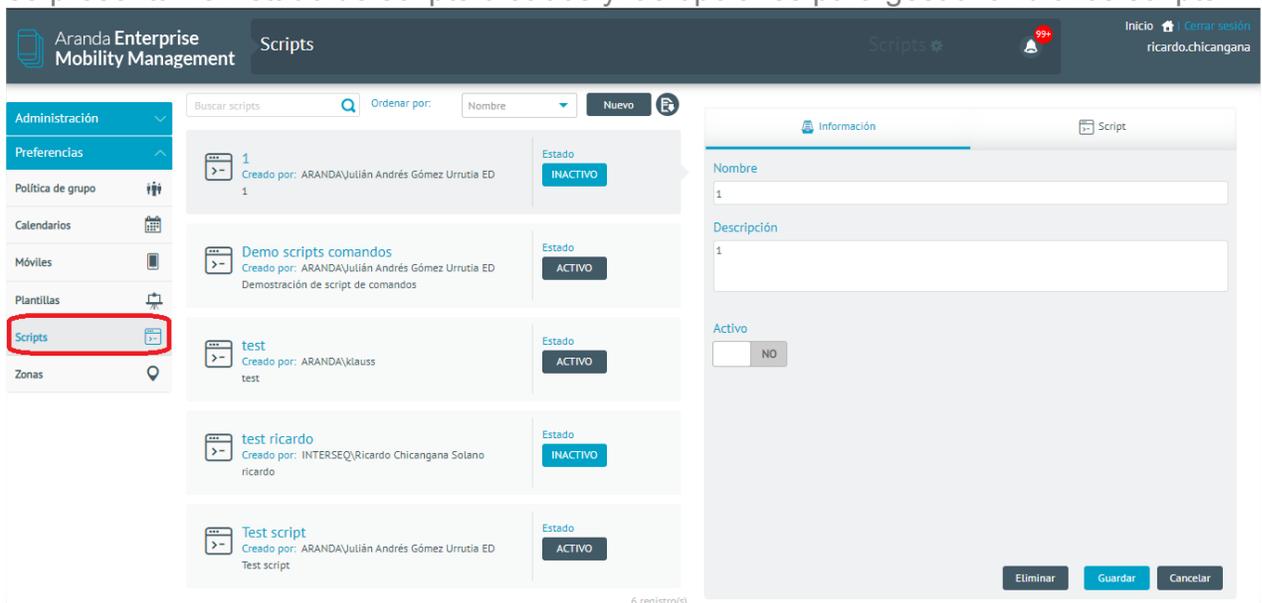


Por defecto AEMM provee plantillas por defecto para cada una de las secciones disponibles.

4.5. Scripts

Los scripts son series secuenciales de comandos que son ejecutables sobre uno o varios dispositivos mediante un proyecto de gestión.

Para configurar scripts se debe de ingresar al módulo destinado para tal, en esta pantalla se presentan el listado de scripts creados y las opciones para gestionar dichos scripts:



4.5.1. Creación de scripts

Para crear un nuevo script haga clic en “Nuevo”, y a continuación se le solicitarán los datos de Nombre (nombre único del script), Descripción (Descripción corta del script) y Estado (Activo/Inactivo).

The screenshot shows a web interface for managing scripts. At the top, there is a search bar labeled 'Buscar scripts' and a dropdown menu for 'Ordenar por:' set to 'Nombre'. A red box highlights a 'Nuevo' button with a plus icon. Below this is a list of five scripts, each with a terminal icon, a name, a creator, and a status button (e.g., 'INACTIVO' or 'ACTIVO'). To the right, a modal form titled 'Información' is open, also highlighted with a red box. It contains three fields: 'Nombre' (empty), 'Descripción' (empty), and 'Activo' (a radio button with 'NO' selected). At the bottom right of the form are 'Guardar' and 'Cancelar' buttons.

Luego de diligenciar los datos solicitados, haga clic en guardar. Luego de esto se habilitará la pestaña “Script”, donde se creará la secuencia de comandos.

This screenshot shows the same 'Información' form, but the 'Script' tab is now selected and highlighted with a red box. The 'Nombre' field contains the text 'Script de enrolamiento'. The 'Descripción' field contains the text 'Se debe ejecutar para instalar el agente'. The 'Activo' field now has a radio button with 'SI' selected.

4.5.2. Edición del Script

Para la edición del script como tal acceda a la pestaña “Script”, donde se presentará la interfaz de edición de los comandos a incluir.



Información Script

Ingrese la serie de comandos que ejecutará su script en el dispositivo

[? Instrucciones de sintáxis y comandos ver documentación](#)

```
1 text prueba scripts release 9.17
2 install com.facebook.katana
3
4
5
6
7
8
9
10
11
```

VERIFICAR

Guardar Cancelar

En esta interfaz se pueden ingresar los comandos a incluir, en la secuencia de ejecución deseada.

Como ayuda para la correcta escritura en cuanto a estructura y sintaxis, se pone a disposición el botón “Verificar”, el cual valida la secuencia de órdenes escritas y presenta un mensaje claro y visible ante el evento de encontrarse algún error o por el contrario si la secuencia esta correcta.

Información

Script

Ingrese la serie de comandos que ejecutará su script en el dispositivo

[? Instrucciones de sintáxis y comandos ver documentación](#)

```
1 text prueba scripts release 9.17  
2 install com.facebook.katana  
3  
4  
5  
6  
7  
8  
9  
10  
11
```

✓ Script exitoso

VERIFICAR

Guardar

Cancelar

Información

Script

Ingrese la serie de comandos que ejecutará su script en el dispositivo

[? Instrucciones de sintáxis y comandos ver documentación](#)

```
1 text prueba scripts release 9.17
2 install com.facebook.katana
3 ttt
4
5
6
7
8
9
10
11
```

 Script fallido

VERIFICAR

 Error en línea 3. El comando ingresado no existe, o no está habilitado para ser ejecutado en script de comandos.

Guardar

Cancelar

4.5.3. Comandos disponibles para scripts

La siguiente tabla describe los comandos disponibles actualmente para incluirse en scripts.

Script	Descripción	Cantidad de Parámetros	Ejemplo
text	Muestra un mensaje en el timeline del dispositivo (No es el mensaje que se envía al dispositivo, este comando no interactúa directamente con el dispositivo)	Los necesarios	text Inicio de prueba de scripts de comandos
copy	Copia un elemento (archivo o carpeta) de una ruta origen a una ruta destino en el dispositivo	2	copy ruta/origen ruta/destino
del	Elimina un elemento (archivo o carpeta) del dispositivo	1	del ruta/elemento
start	Ejecuta una aplicación en el dispositivo	1	start com.facebook.katana
install	Instala una aplicación en el dispositivo	1	install com.facebook.katana
uninstall	Desinstala una aplicación del dispositivo	1	uninstall com.facebook.katana
validateVersion	Verifica la versión de una aplicación específica instalada en un dispositivo	2	validateVersion com.facebook.katana 1.2
policy	Envía un comando de política	1	polcy DefaultPolicy

4.5.4. Eliminación de scripts

Para eliminar un script ubíquelo en el listado y haga clic en “Eliminar”

Se debe de tener en cuenta que, para la eliminación de un script de comandos, es necesario que este no se encuentre vinculado con ningún proyecto de gestión.

The screenshot displays the Aranda Software interface. On the left, a list of scripts is shown with the following details:

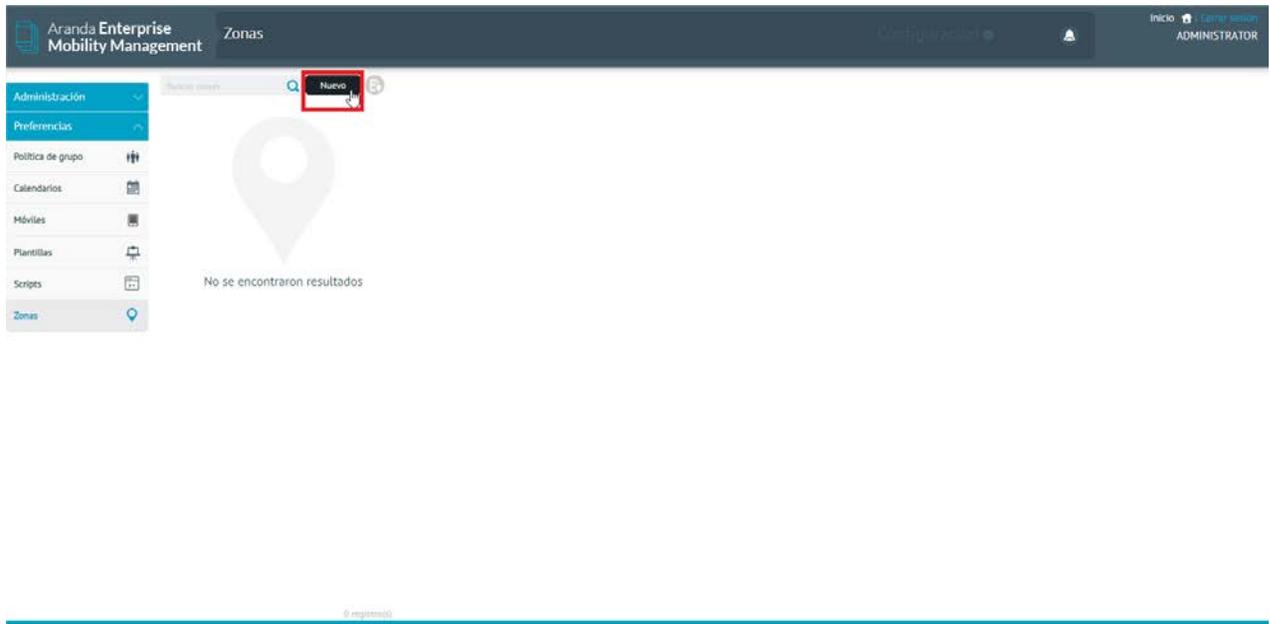
Script Name	Created By	Status
1	ARANDA\Julián Andrés Gómez Urrutia ED	INACTIVO
Demo scripts comandos	ARANDA\Julián Andrés Gómez Urrutia ED	ACTIVO
test	ARANDA\klaus	ACTIVO
test ricardo	INTERSEQ\Ricardo Chicangana Solano ricardo	INACTIVO
Test script	ARANDA\Julián Andrés Gómez Urrutia ED	ACTIVO

The first script, '1', is highlighted with a red box. On the right, the 'Información' (Information) tab for a script is shown. The 'Nombre' (Name) field contains '1', and the 'Descripción' (Description) field contains '1'. At the bottom of the information panel, the 'Eliminar' (Delete) button is highlighted with a red box, along with 'Guardar' (Save) and 'Cancelar' (Cancel) buttons.

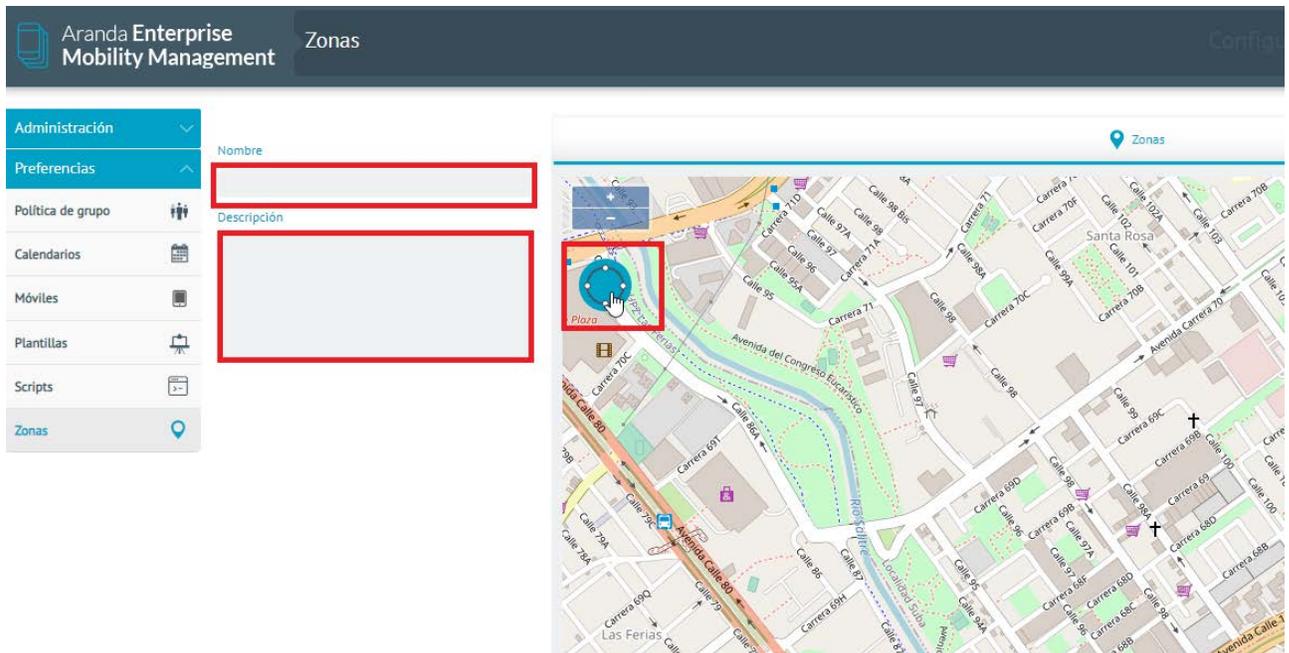
4.6. Zonas

La sección de zonas se destina para gestionar las zonas que posteriormente serán utilizadas en la configuración de conjuntos de reglas que tengan ítem de “Geofencing” (Frontera geográfica).

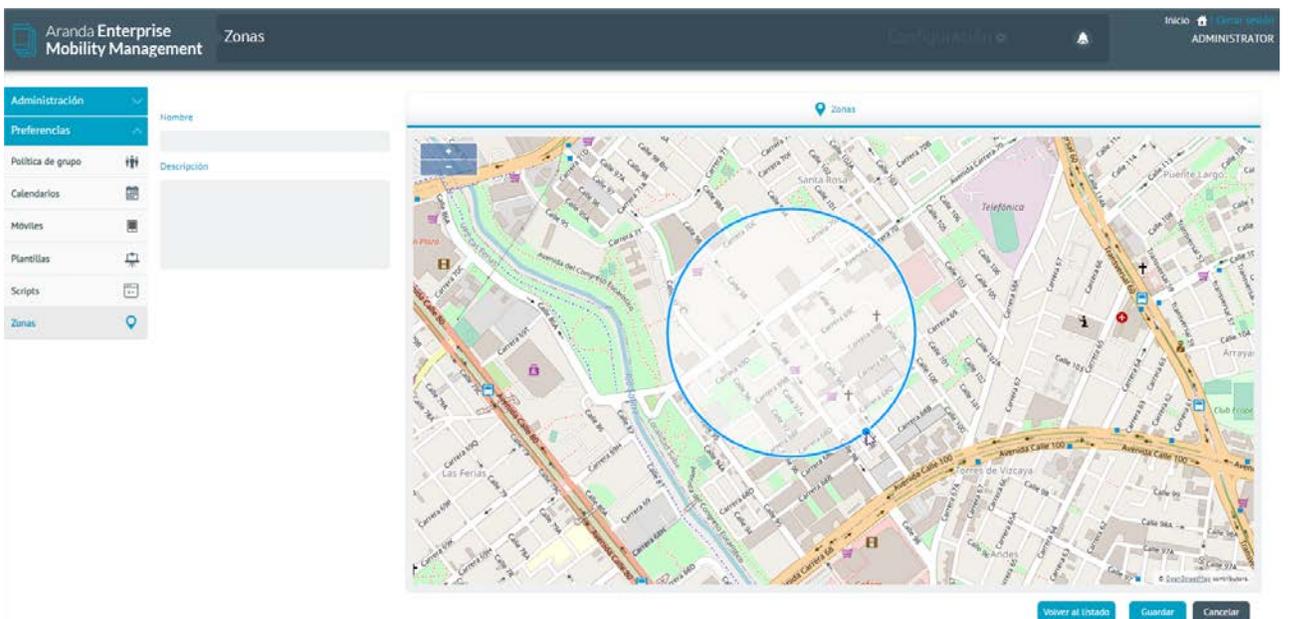
Para configurar una zona geográfica acceda a la sección de zonas y haga clic en **Nuevo**.



Ingrese los datos solicitados y de clic en el círculo azul para delimitar la zona.

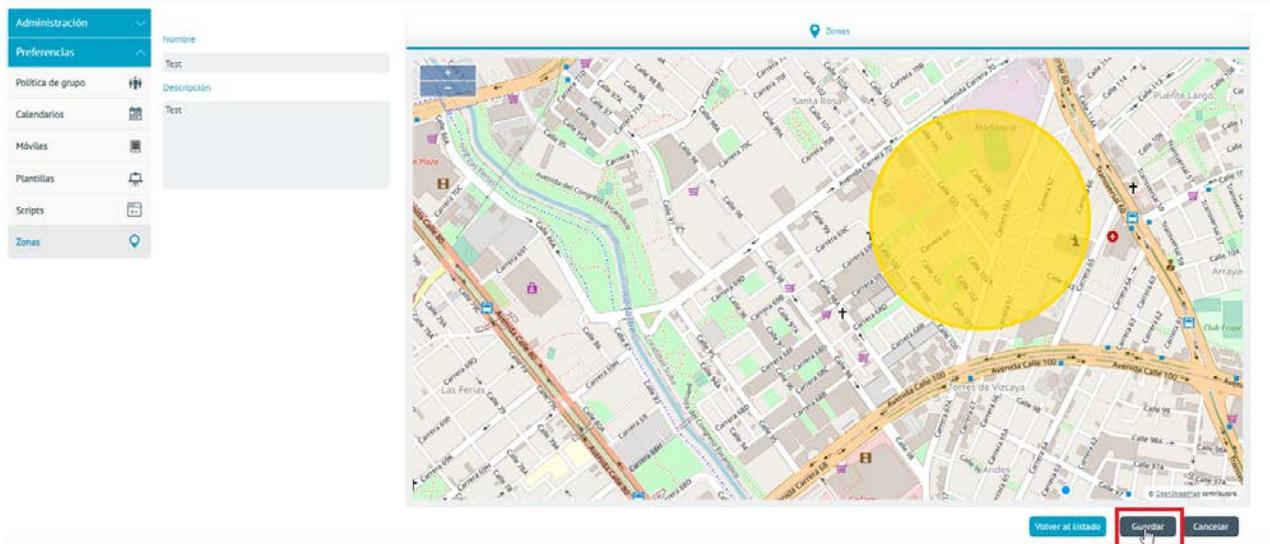


Luego haga un clic y suelte para marcar el centro de la zona, y luego mueva el ratón para ampliar o disminuir la zona, y luego un clic final para terminar de dibujar la zona.



Si desea puede editar la zona ya dibujada, dando clic sostenido en su centro para cambiarla de lugar o dando clic sostenido en su borde para cambiar el tamaño.

Si da un clic por fuera de la zona ya dibujada el proceso empezara de nuevo.
Por último, haga clic en **Guardar** para persistir la zona.



5. VINCULACIÓN DE DISPOSITIVOS

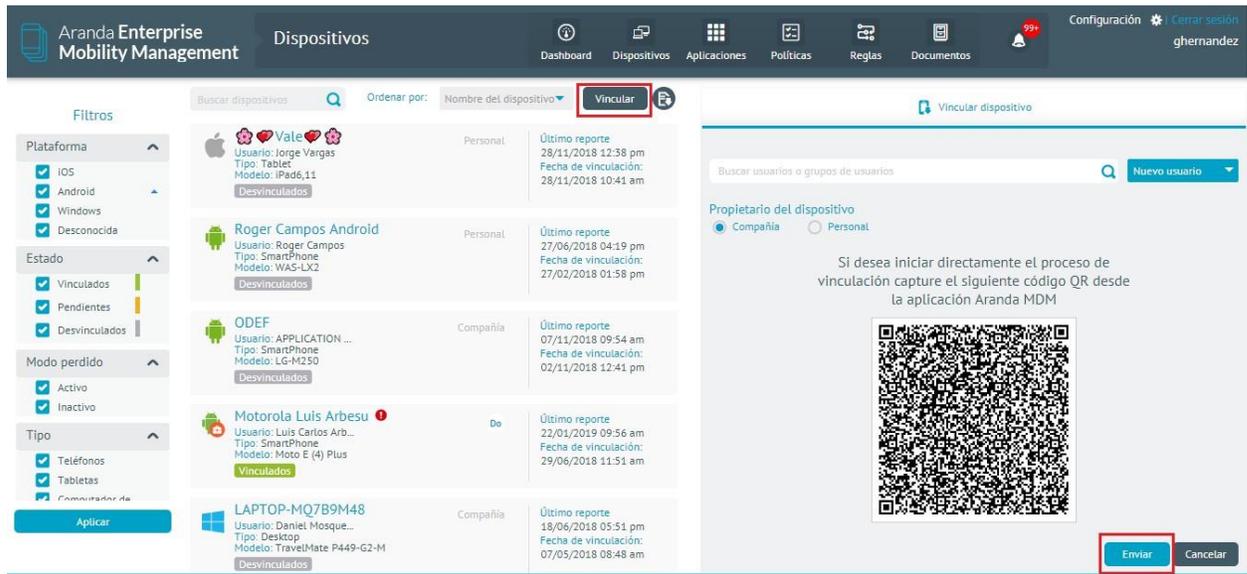
5.1. Android

Para la plataforma Android se tienen disponibles en la tienda de Google Play las siguientes aplicaciones de Agente de Aranda, que permiten la vinculación de dispositivos hacia el servidor AEMM

- **ArandaEMM**: Agente genérico para Android, que permite la vinculación de cualquier dispositivo Android
- **ArandaEMM for Samsung**: Agente diseñado para gestionar dispositivos Samsung usando la gestión avanzada que ofrece Knox.
- **ArandaEMM for LG**: Agente diseñado para gestionar dispositivos LG, usando la gestión ofrecida por LG Gate.
- **ArandaEMM for Cyrus**: Agente diseñado para gestionar dispositivos Cyrus, incluye la firma de fabricante de Cyrus.
- **ArandaEMM for Panasonic**: Agente diseñado para gestionar dispositivos Panasonic, incluye la firma de fabricante de Panasonic.

5.1.1. Vinculación desde consola Web

Se debe seleccionar el botón **Vincular**, luego aparecerá en la parte derecha un código QR que contiene la información del servidor y dominio para continuar el proceso.



Para capturar el código QR se abre la aplicación móvil, y se selecciona la opción **Ingresar código QR**



La aplicación usa la cámara del dispositivo para realizar la captura del código, este se detecta de forma automática, después de que la aplicación captura la información del

código, realiza la validación del servidor y el dominio y deja al usuario en la vista para ingresar las credenciales correspondientes (usuario y contraseña).



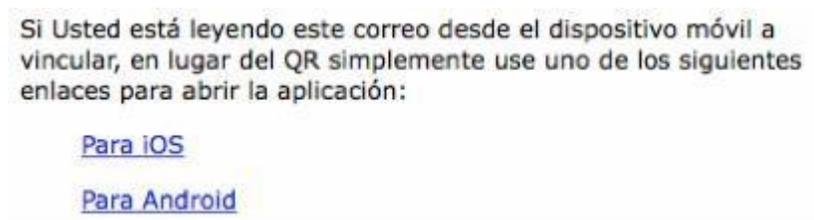
5.1.2. Vinculación desde el correo de invitación

Para enviar un correo de invitación, ingrese a la consola web y seleccione la opción **Vincular**, en la parte derecha de la pantalla ingrese el usuario o grupo de usuarios a los cuales desea enviar el correo, cuando tenga la lista de usuarios seleccione el botón **Enviar** ubicado en la parte inferior.

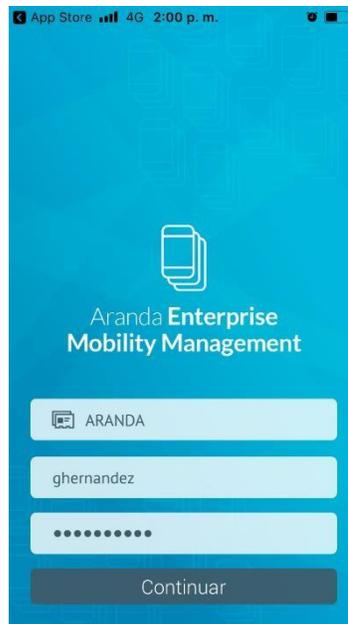
El (Los) usuario(s) recibirá(n) un correo con unas instrucciones a seguir para vincular el dispositivo, desde el correo se puede realizar la vinculación del dispositivo de tres formas diferentes.

5.1.3. Vinculación usando link

En el correo hay un mensaje como el presentado en la imagen:



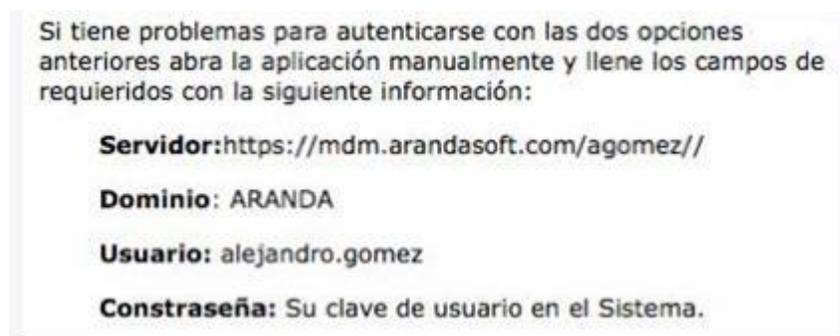
Los dos links contienen la información necesaria para que el sistema realice el proceso de validación de servidores de forma automática y deje al usuario en la vista de autenticación.



El proceso continuo de la misma forma sin importar la opción seleccionada, y se explica en la sección **Continuación del proceso**.

5.1.4. Vinculación ingresando la información de forma manual

En la parte inferior del correo se indica al usuario la información de servidor, dominio y usuario.



Esta información puede ser ingresada manualmente desde la aplicación ingresando a la opción **Ingresar URL de servidor**.



La aplicación presenta la vista para ingresar la dirección del servidor EMM.



Cuando el servidor validó que la dirección ingresada es correcta la aplicación deja al usuario en la vista de autenticación para que ingrese las credenciales de usuario y contraseña.



El proceso continúa de la misma forma sin importar la opción seleccionada, este se explica a continuación.

Después de ingresar las credenciales de autenticación y que el sistema valide que estas son correctas, se presenta la vista de términos y condiciones.



Cuando el usuario selecciona la opción **Acepto los términos y condiciones** y presiona el botón **Continuar**, el sistema actualiza esta información y permite que el usuario avance al siguiente paso del proceso que varía dependiendo del sistema operativo.

5.2. Android for Work

Si la compatibilidad con Android for Work fue habilitada haciendo el respectivo proceso descrito en el numeral 4.3.5.1, estará ya disponible la vinculación de los dispositivos Android compatibles con Android for Work.

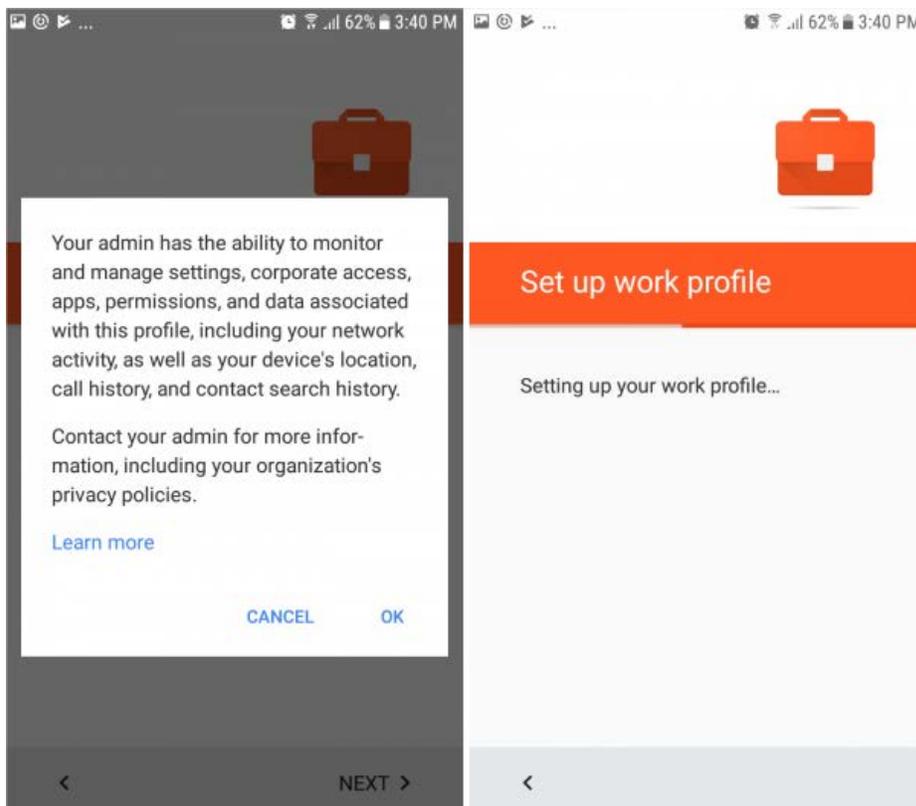
Los agentes descritos en el numeral 5.1 son compatibles con vinculación Android for Work (AFW).

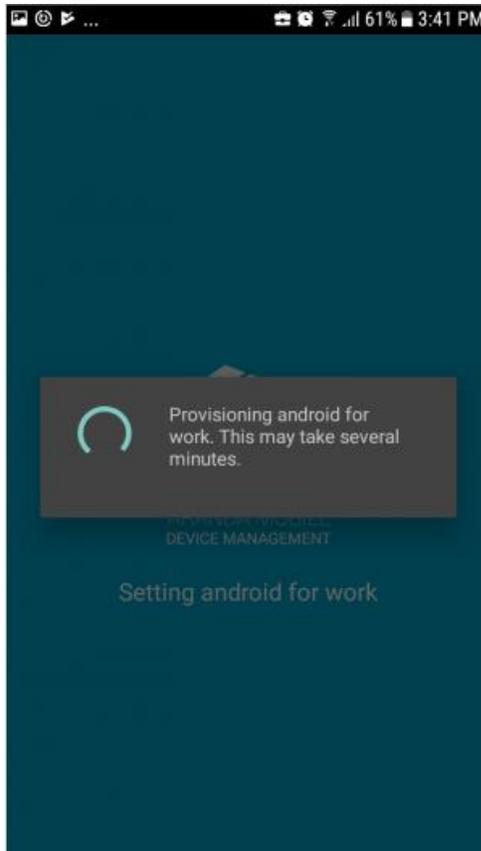
AFW ofrece dos modos de vinculación Profile Owner y Device Owner.

5.2.1. Vinculación AFW Profile Owner

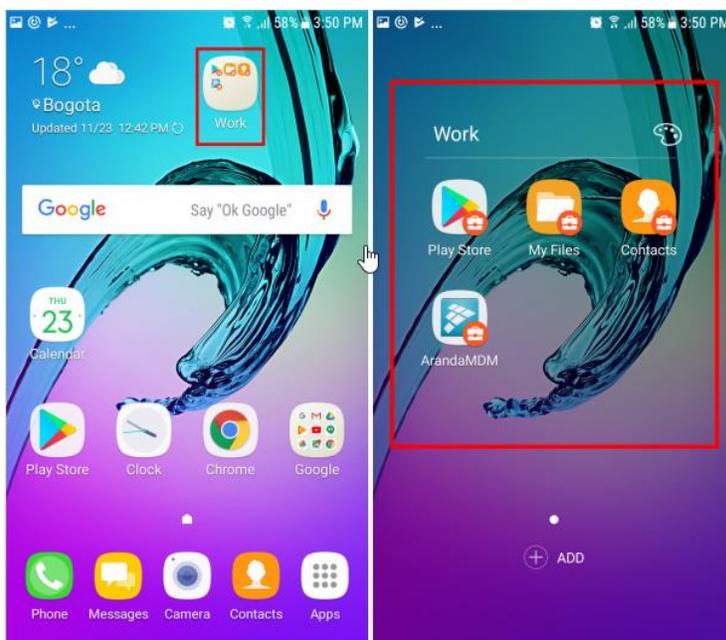
El modo AFW Profile Owner ofrece una vinculación donde el servidor AEMM tendrá control de una sección separada del dispositivo, llamada Perfil de Trabajo. Este tipo de vinculación se recomienda cuando el dispositivo es propiedad del usuario y no puede administrarse en su totalidad.

Este modo de vinculación es muy similar a la descrita en la sección 5.1. La diferencia radica en las pantallas que se presentan al usuario donde se indica que se está activando en el dispositivo el perfil de trabajo.

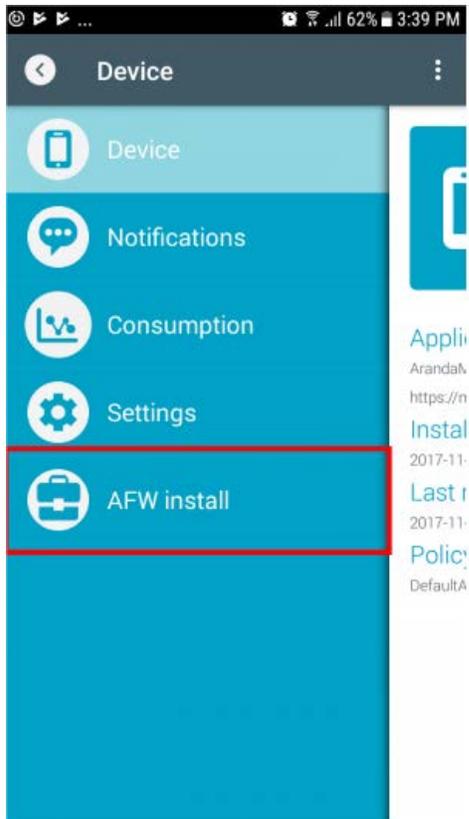




Una vez terminado el proceso de creación del perfil de trabajo, se creará una sección separada en el menú de aplicaciones del dispositivo identificada como trabajo y donde las aplicaciones ahí presentes tendrán una distinción en la esquina inferior derecha que indica que son parte del perfil de trabajo.



Existe otro escenario posible para poder instalar AFW en el modo profile owner, este se da cuando los usuarios finales ya tienen instalado el agente y en la consola se activa la configuración de AFW, cuando esto sucede el agente da la opción al usuario final de preparar el dispositivo para instalar AFW en su dispositivo.



5.2.2. Vinculación AFW Device Owner

El modo de vinculación AFW Device Owner ofrece una gestión completa del dispositivo por parte del servidor AEMM. Este tipo de vinculación es recomendada cuando los dispositivos son propiedad de la empresa.

Para acceder al modo device owner es necesario disponer de dispositivos nuevos y/o realizarles un reseteo de fábrica.

Para este proceso es necesario conocer el identificador DPC (DPC id), que identifica el agente que administrará el dispositivo. La siguiente tabla describe cada uno de los agentes con su DPC id correspondiente:

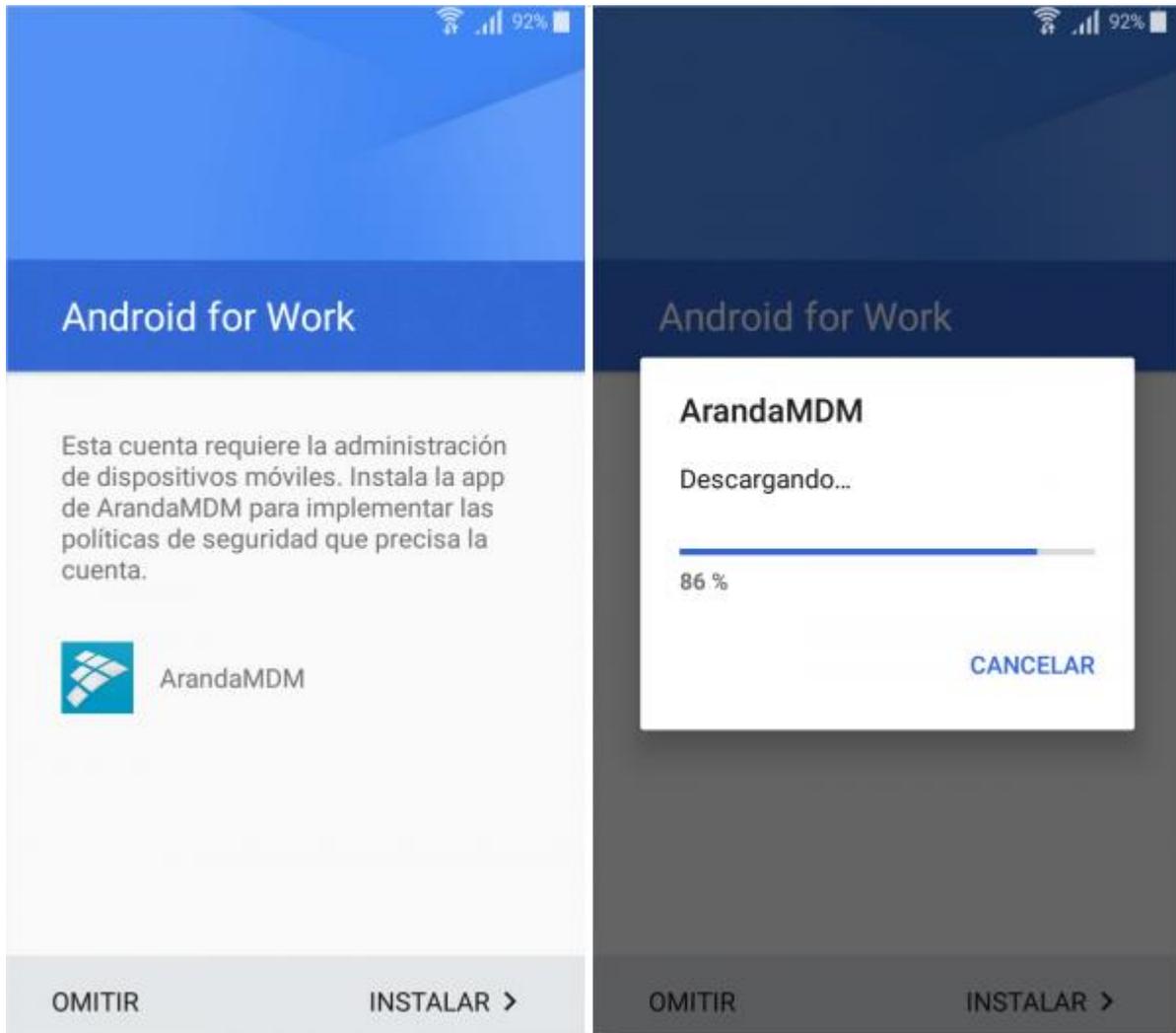
Agente	Identificador DPC
ArandaEMM	afw#arandamdm
AradaEMM for Samsung	afw#arandamdmknox
ArandaEMM for LG	afw#arandamdlge
ArandaEMM for Cyrus	afw#arandamdmcyrus

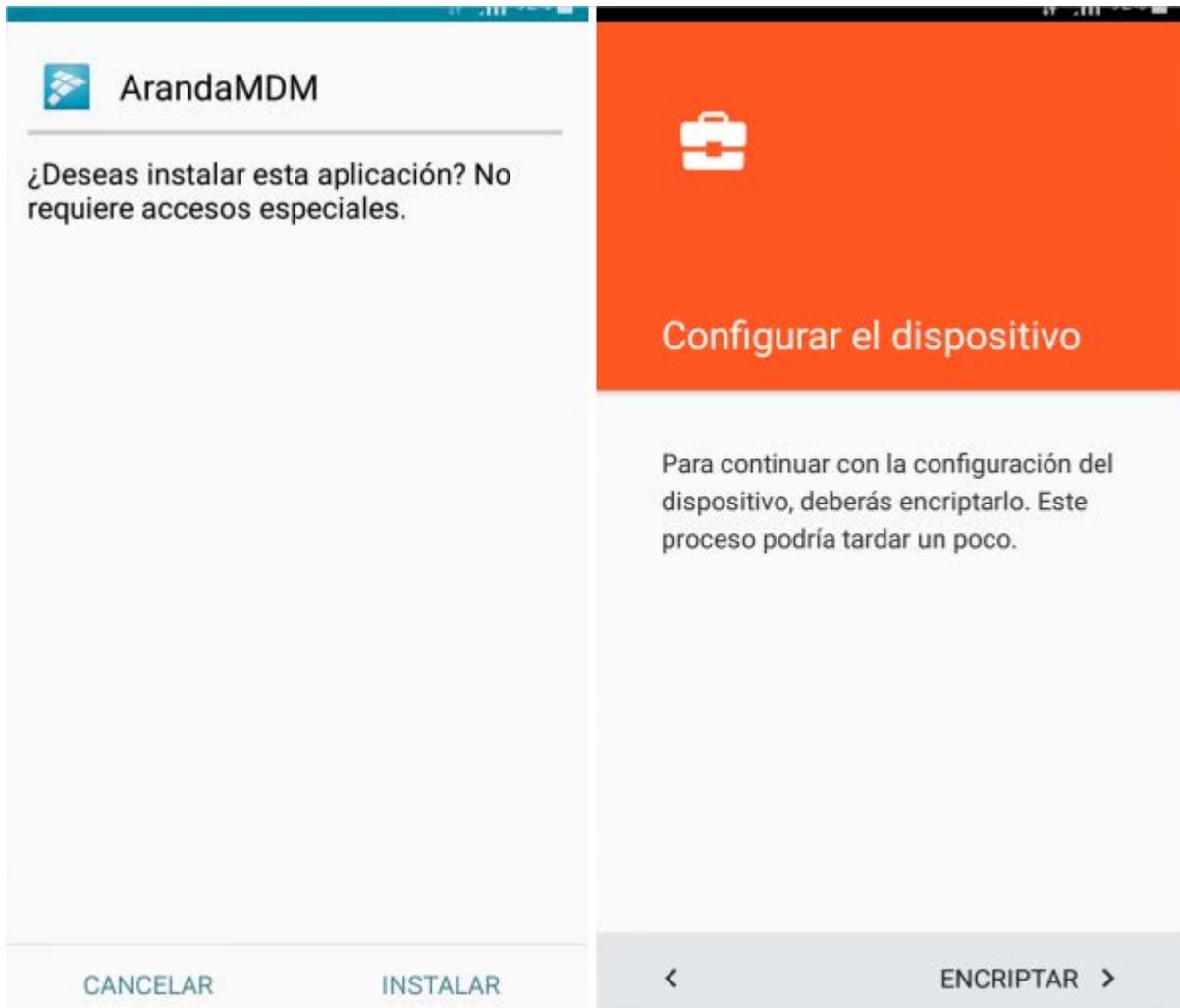
Para iniciar la vinculación es indispensable conectar el dispositivo a Internet, bien sea por datos móviles o agregando una red wifi.

Como ya se dijo el dispositivo debe estar nuevo o restaurado de fábrica, una vez se solicite una cuenta de google para iniciar la configuración inicial del dispositivo, se debe de ingresar uno de los identificadores DPC descritos en la anterior tabla, esto dependiendo del fabricante del dispositivo.



Luego de ingresar el DPC id el sistema operativo iniciará la descarga del agente correspondiente.





Luego de preparado el dispositivo para AFW Device Owner se seguirá con el proceso de vinculación normal descrito en el numeral 5.1

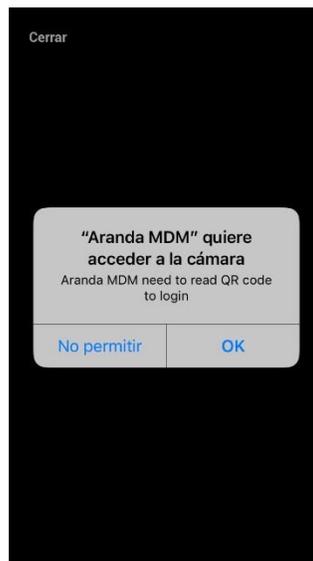
5.3. iOS

Escoja la forma en la que va vincular el dispositivo, hay dos opciones disponibles:

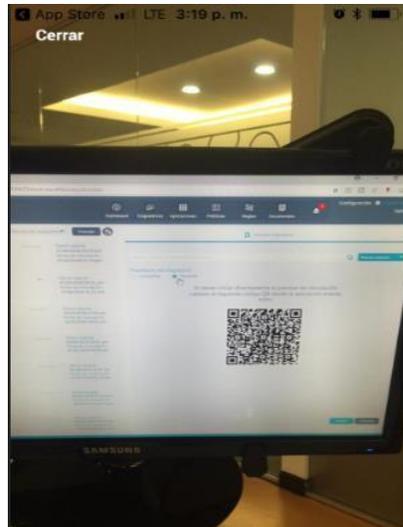
- Ingresar código QR
- Ingresar URL de Servidor



En este caso la opción escogida fue ingresar código QR, después pues de este paso usted observará la siguiente pantalla.



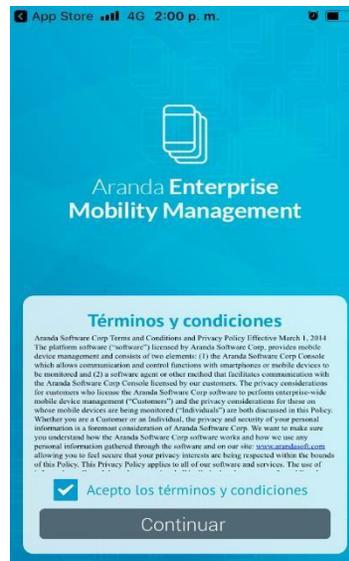
Escanee el código QR desde la consola web de Aranda Mobile Device Management



Llene los espacios con el usuario y contraseña previamente creado por el administrador, y luego de clic en **continuar**.



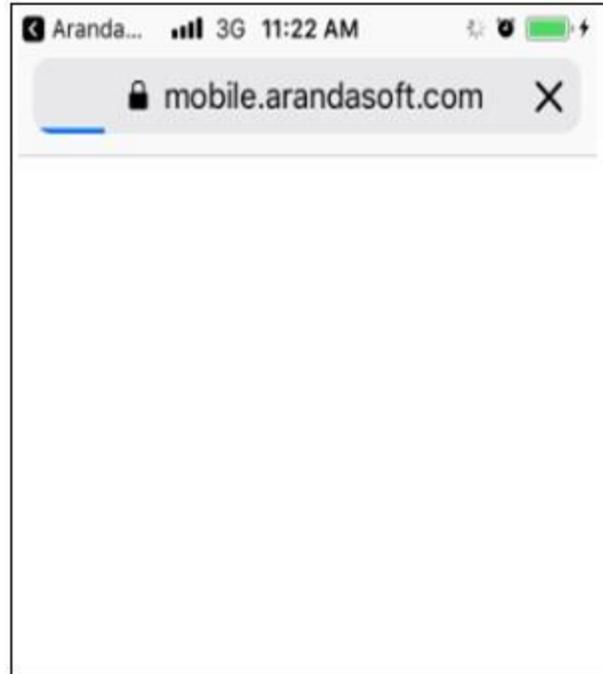
Después de esto acepte los términos y condiciones y de clic en **continuar**.



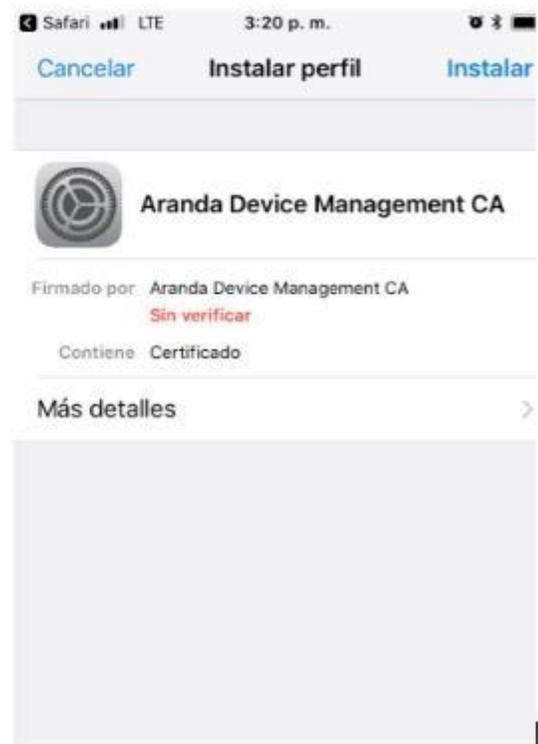
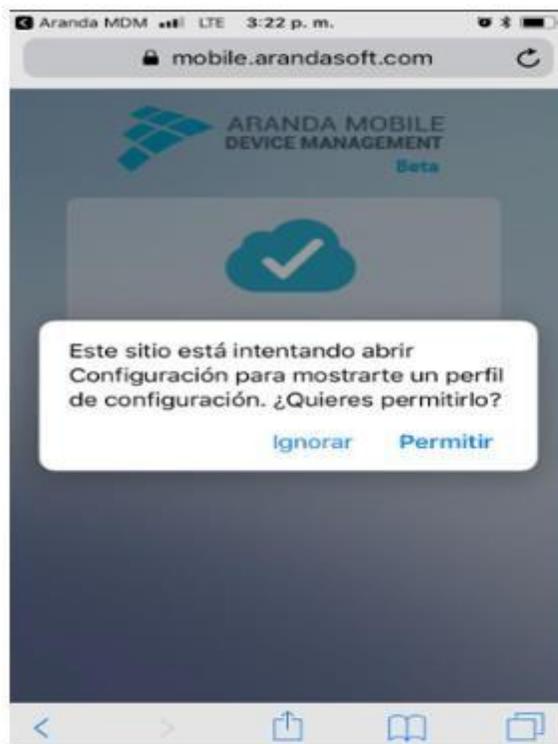
El siguiente paso es para descargar e instalar el certificado. Por favor de clic en **Descargar CA**



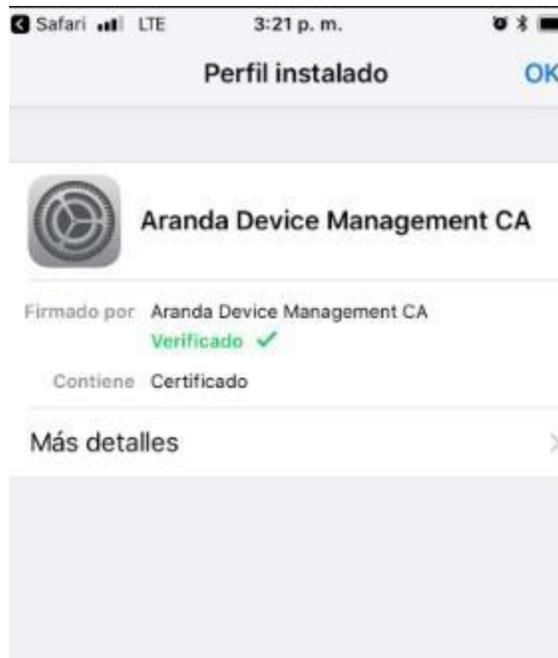
Después de esto usted será direccionado al sitio seguro **mobile.arandasoft.com** para instalar el certificado.



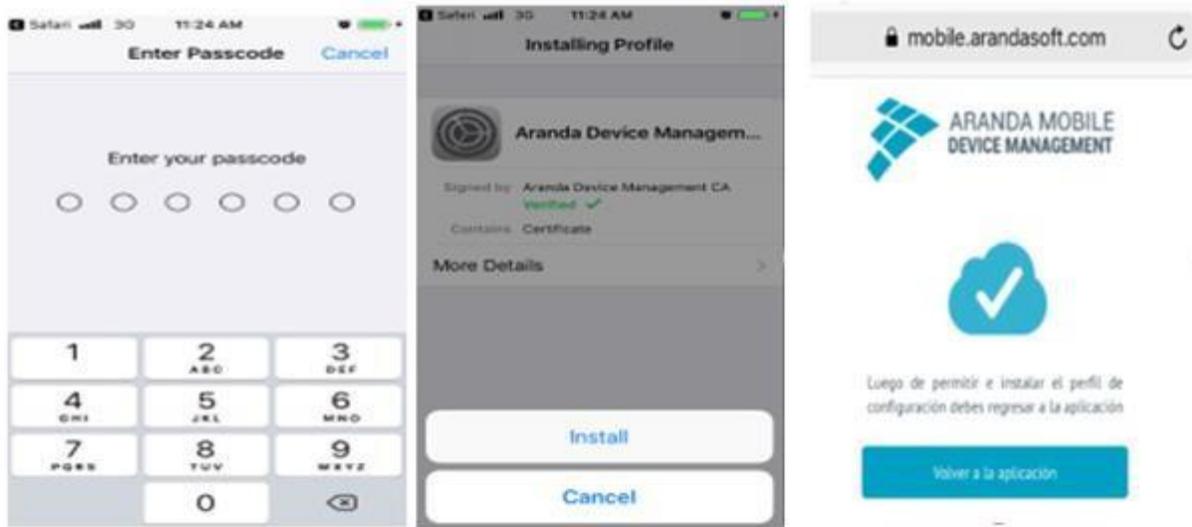
Por favor complete los siguientes pasos para continuar:



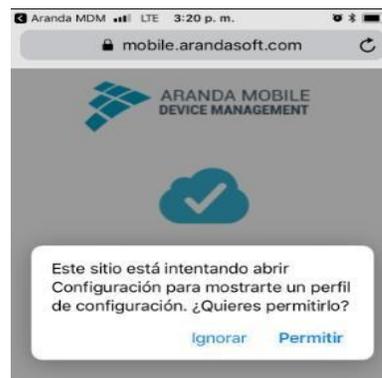
Por favor de clic en OK



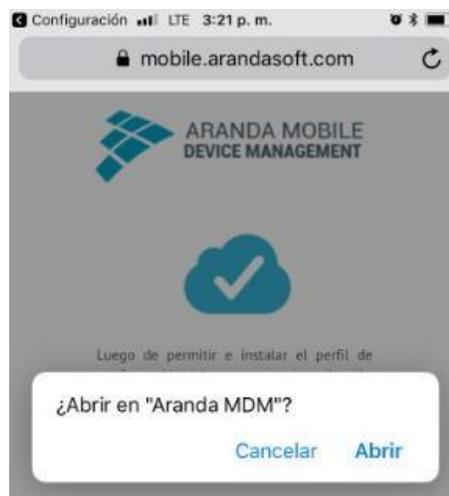
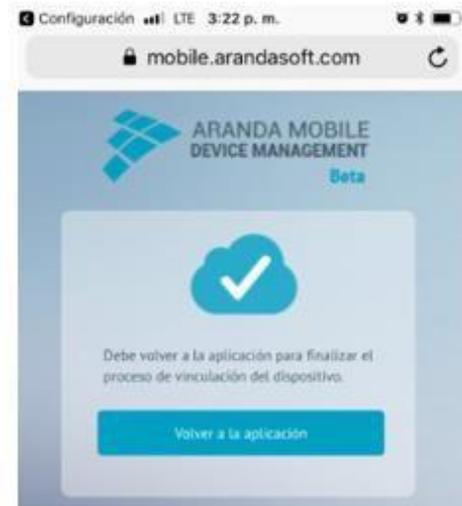
Si su dispositivo tiene contraseña, por favor digítela y luego de clic en **Instalar**



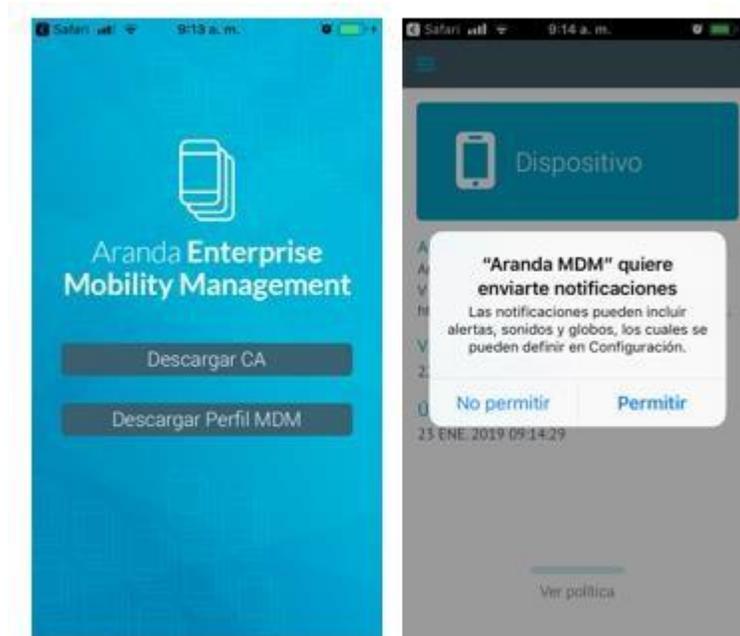
De clic en **permitir**



Después de esto, por favor seguir los siguientes pasos para instalar el perfil Por favor complete los siguientes pasos y culmínelos dando clic en **abrir**



La siguiente imagen es presentada para descargar e instalar un perfil de iOS que le permite a estos dispositivos ser vinculados. De clic en **Descargar Perfil EMM** y luego de clic en **permitir**.



Finalmente, cuando usted observa la siguiente imagen, su perfil ha sido instalado y su dispositivo vinculado exitosamente y podrá ser controlado desde la consola web



5.4. Windows

En AEMM es posible realizar vinculación de dispositivos con sistema operativo Windows 10 Pro y Windows 10 Mobile.

Estos dispositivos ya cuentan con un mecanismo propio de gestión MDM ofrecido por Microsoft Windows y sobre el cual AEMM trabaja.

5.4.1. Vinculación Windows 10 Pro

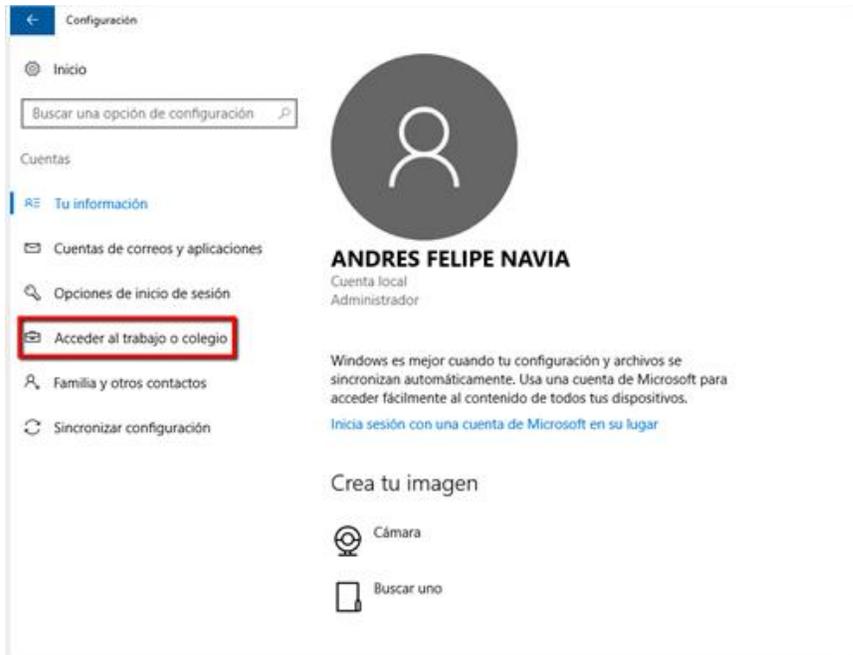
5.4.1.1. Vinculación al MDM Nativo de Microsoft Windows

La vinculación nativa de Windows se realiza usando herramientas propias del sistema operativo. Una vez terminada el dispositivo es dado de alta en el Servidor ya se puede iniciar la gestión del mismo.

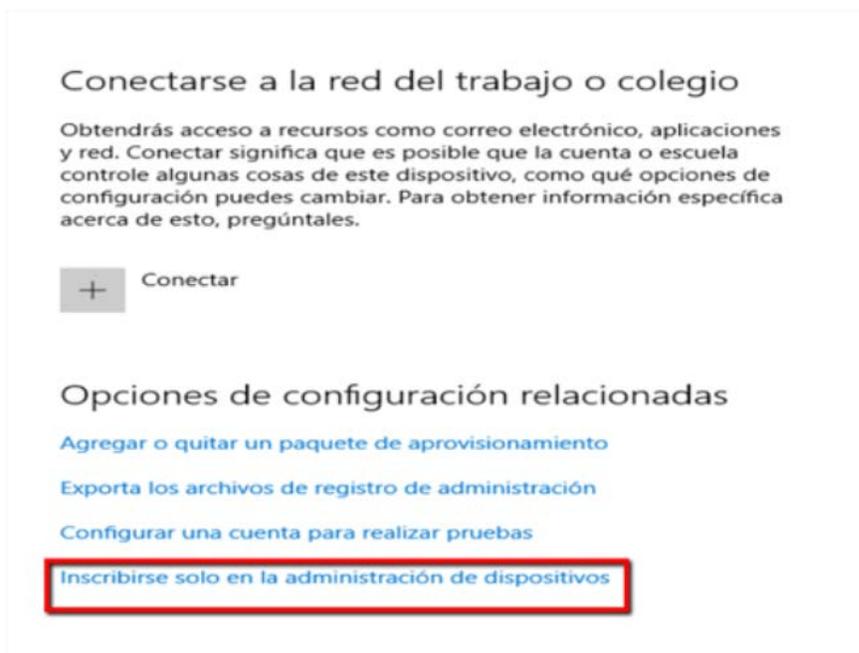
Ingresa al módulo de Configuración de Windows y selecciona la opción Cuentas



Después de seleccionar la opción cuentas, se debe seleccionar la opción “acceder al trabajo o colegio “



En la siguiente pantalla se debe seleccionar la opción: “Inscribirse solo en la administración de dispositivos”



En la siguiente pantalla digitar el usuario de la cuenta con la cual se va a vincular el dispositivo.

Configurar una cuenta laboral o educativa

Obtendrás acceso a recursos como el correo electrónico, las aplicaciones y la red. Al conectarte, la cuenta laboral o educativa controlará varias cosas del dispositivo, como las opciones de configuración que puedes cambiar. Si quieres obtener más detalles sobre este tema, solo tienes que pedirla.

Siguiente

En la siguiente pantalla se debe registrar la url de vinculación Windows, la cual consiste en la url completa del servidor MDM más la ruta interna "ws/mobile/W10EnrollmentHandler.ashx":

Configurar una cuenta de trabajo o escuela

Obtendrás acceso a recursos como correo electrónico, aplicaciones y red. Conectar significa que es posible que la cuenta o escuela controle algunas cosas de este dispositivo, como qué opciones de configuración puedes cambiar. Para obtener información específica acerca de esto, pregúntales.

andres.navia@arandasoft.com

/AMDMWS/ws/mobil/W10EnrollmentHandler.ashx

No pudimos detectar automáticamente un extremo de administración que coincida con el nombre de usuario escrito. Comprueba tu nombre de usuario y vuelve a intentarlo. Si conoces la dirección URL para el extremo de administración, escríbela.

Siguiente

Si los datos solicitados se registraron correctamente al dar clic sobre el botón siguiente, se desplegará la siguiente pantalla, donde es necesario registrar el usuario y la contraseña de la cuenta correspondiente al directorio activo.

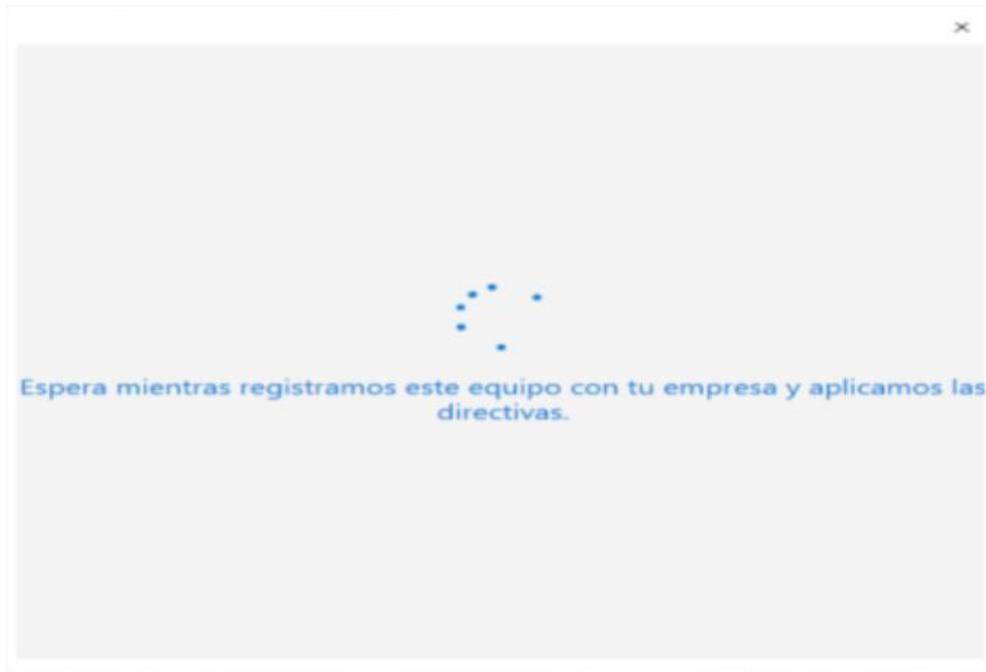
Configurar una cuenta de trabajo o escuela

Obtendrás acceso a recursos como correo electrónico, aplicaciones y red. Conectar significa que es posible que la cuenta o escuela controle algunas cosas de este dispositivo, como qué opciones de configuración puedes cambiar. Para obtener información específica acerca de esto, pregúntales.

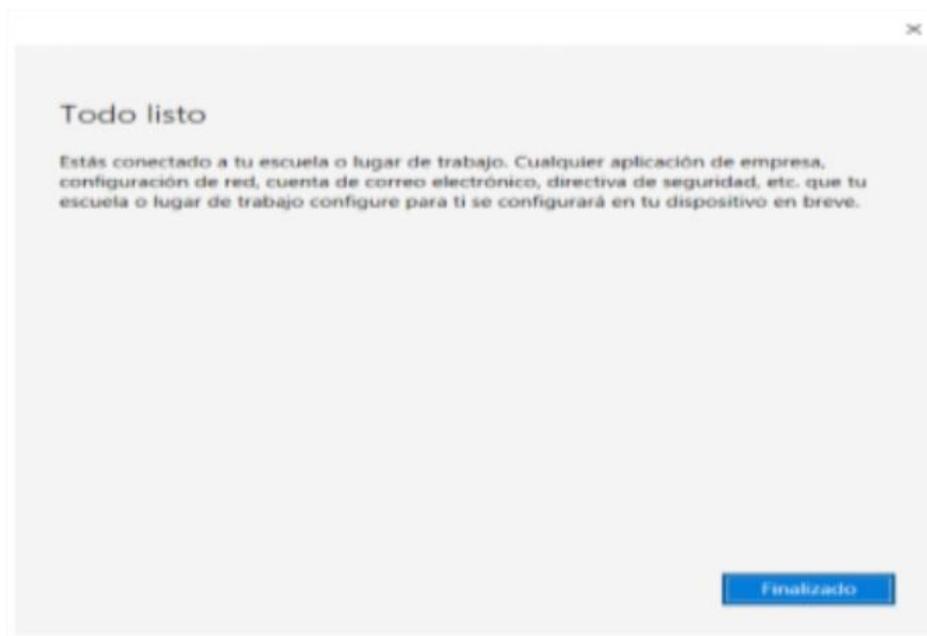
INTERSEQ\ANDRES.NAVIA

Siguiente

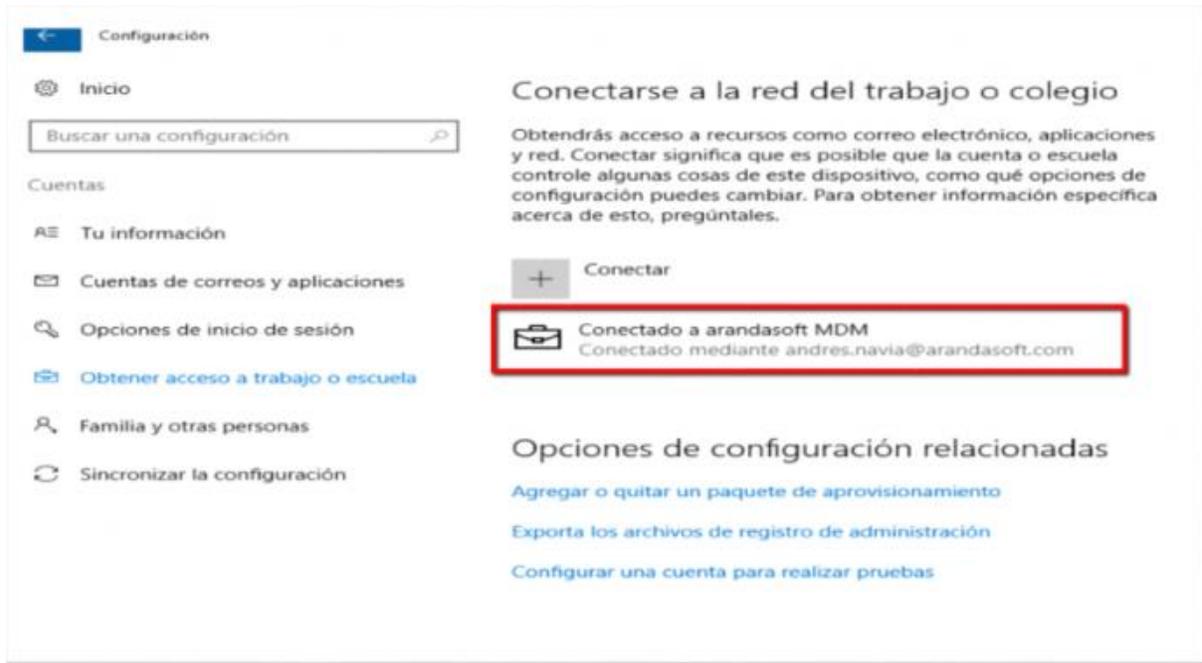
Al dar clic sobre el botón siguiente, el sistema registrara el dispositivo en cuestión.



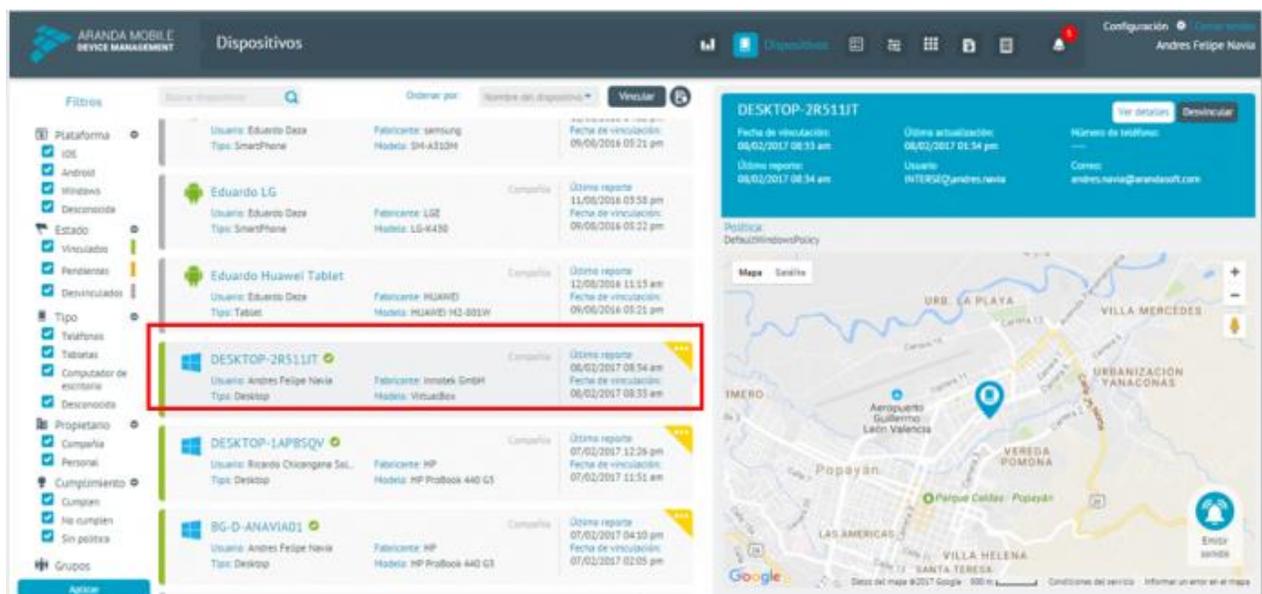
Y finalmente se despliega la pantalla de confirmación indicando que el proceso terminó satisfactoriamente.



Automáticamente el sistema lleva al usuario al módulo de configuración de Windows, donde se debe visualizar el dispositivo conectado la consola de Aranda AEMM.



Para verificar lo anteriormente mencionado, ingresar en la consola de AMDM / a la sección de Dispositivos donde se podrá visualizar el nombre del dispositivo vinculado:

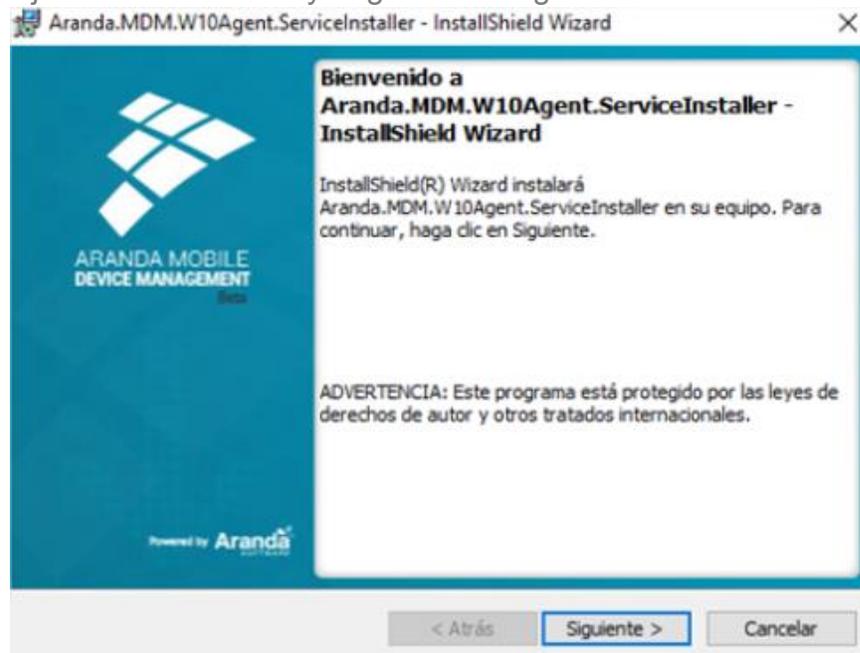


5.4.1.2. Vinculación del Agente Aranda AEMM para Windows

Una vez terminada la vinculación nativa se debe realizar la instalación del agente para alcanzar mayor capacidad de gestión sobre el dispositivo. Para ello se requiere la última versión del siguiente paquete:

Aranda.MDM.W10Agent.Service.Installer.exe

Ejecute el instalador y haga clic en siguiente:



Confirmar la instalación registrando correctamente los datos que a continuación se describen:

- **SERVER_URL:** corresponde a la dirección url del servidor donde se están desplegando los servicios web de la consola, sin incluir rutas internas.
- **USER_DOMAIN:** corresponde al tipo de autenticación del usuario en el dominio, ya sea ARANDA (usuarios locales) o el nombre del directorio activo
- **USER_NAME:** nombre del usuario existente en el dominio respectivo.
- **USER_PWD:** contraseña del usuario

NOTA: actualmente no se está realizando la validación en cuanto a la calidad de los datos ingresados, por lo tanto, es vital que este proceso se haga cuidadosamente, para no requerir una corrección manual o la reinstalación del servicio

Aranda.MDM.W10Agent.ServiceInstaller - InstallShield Wizard

Datos para Vinculación
Ingrese los datos solicitados

SERVER_URL

USER_DOMAIN

USER_NAME

USER_PWD

InstallShield

< Atrás Siguiete > Cancelar

Al dar clic sobre el botón Siguiete, se realizará la instalación y debemos esperar que el proceso termine.

Aranda.MDM.W10Agent.ServiceInstaller - InstallShield Wizard

Preparado para instalar el programa
El Asistente está preparado para comenzar la instalación.

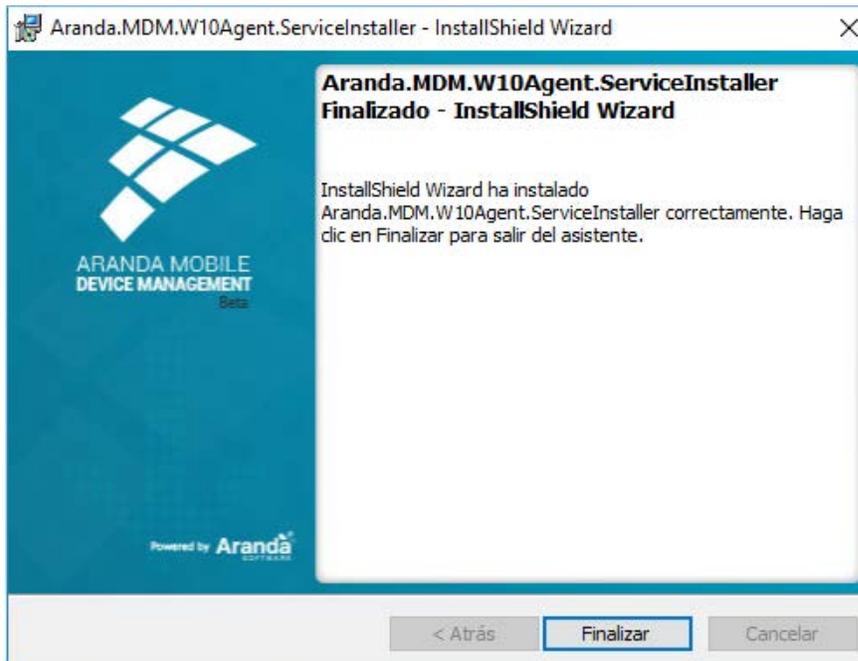
Haga clic en Instalar para comenzar la instalación.

Si desea revisar la configuración de la instalación o realizar algún cambio, haga clic en Atrás. Haga clic en Cancelar para salir del Asistente.

InstallShield

< Atrás Instalar Cancelar

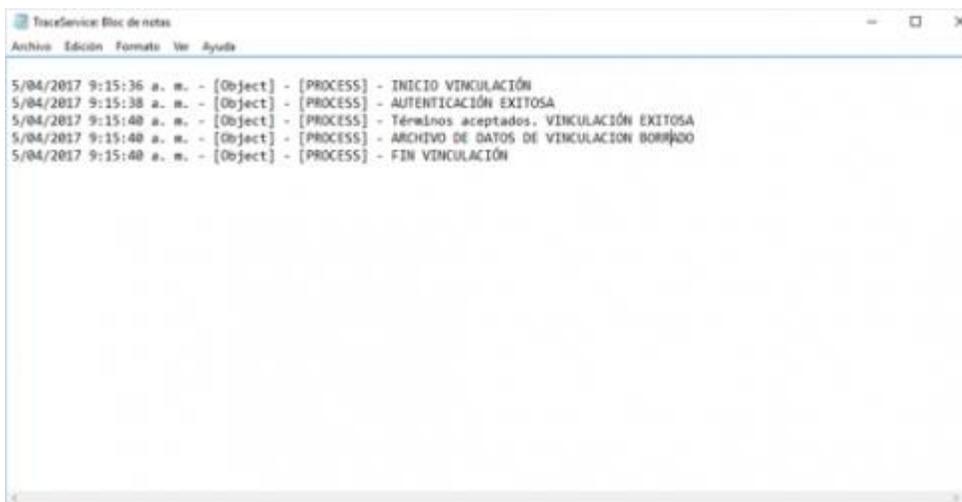
Una vez terminada la copia de archivos, librerías y paquetes necesarios damos clic en finalizar.



Después de instalado el agente, para corroborar que la instalación fue satisfactoria, debemos buscar el archivo TraceService.log en la siguiente ruta:

C:\Program Files (x86)\Aranda\MDM Agent\Logos

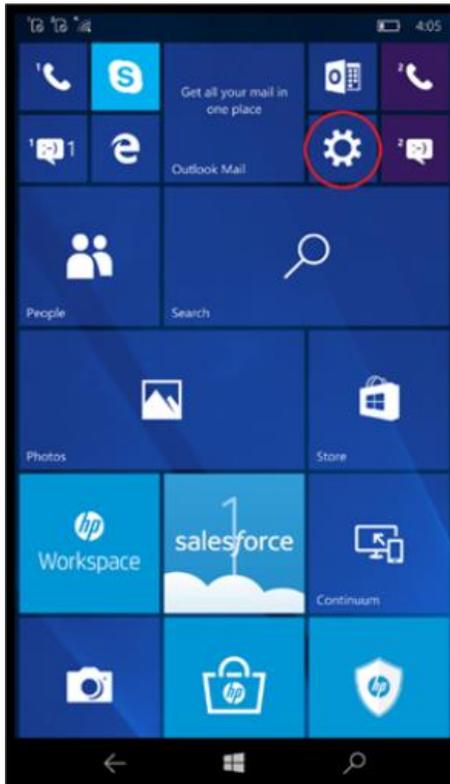
Al abrir dicho archivo se debe visualizar el siguiente contenido, con lo cual es posible validar que el proceso fue exitoso-



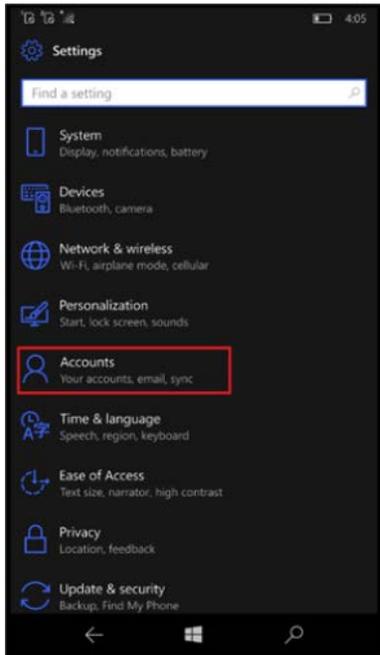
5.4.2. Vinculación Windows 10 Mobile

En Windows 10 Mobile solo está disponible la vinculación nativa, la cual se realiza usando herramientas propias del sistema operativo; para ello siga los siguientes pasos:

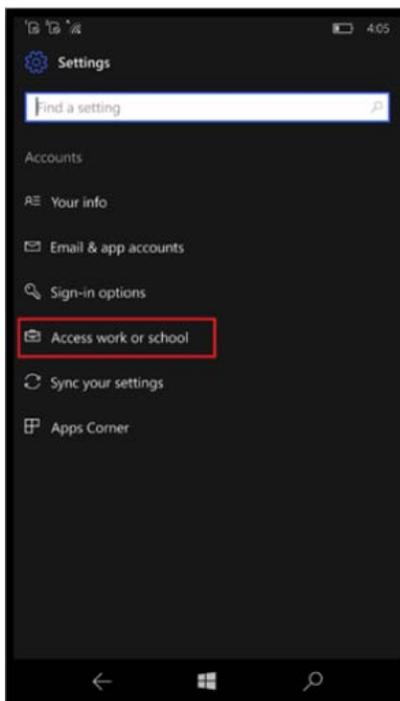
Buscar e Ingresar a la configuración del dispositivo



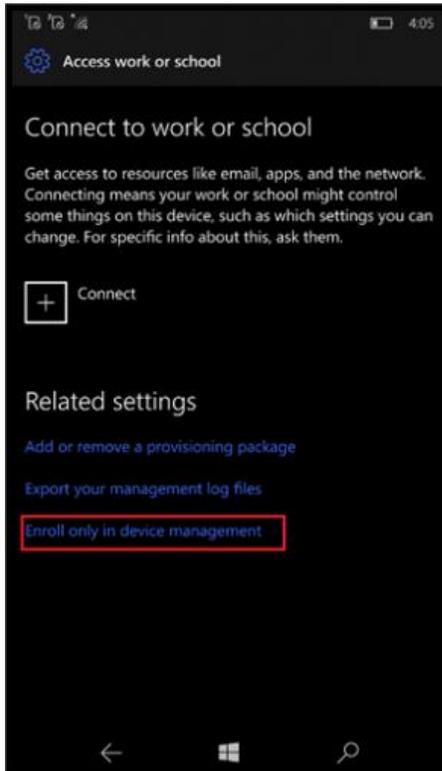
Acto seguido buscar e ingresar a la opción Accounts (cuentas)



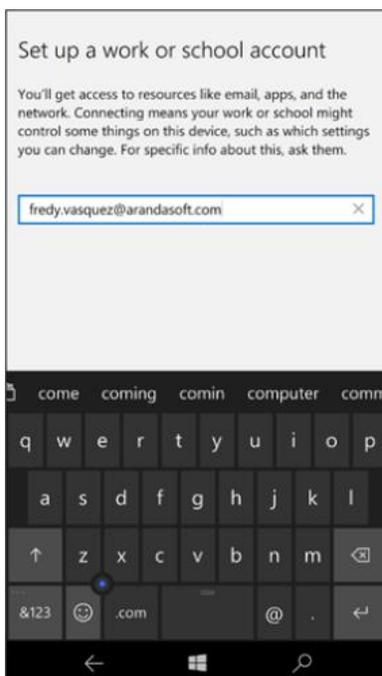
Después de seleccionar la opción cuentas, es necesario buscar e ingresar a la opción “Acceder al Trabajo o Colegio “ (Access work or school).



Posteriormente se debe seleccionar la opción Inscribirse solo en la administración de dispositivos:



Una vez hayamos ingresado al administrador de dispositivos, el paso a seguir es digitar correctamente la cuenta de correo.



Aparece una pantalla donde informa que no encuentra el endpoint de auto descubrimiento, por lo que se debe ingresar la URL del servidor, el site que contiene los servicios y la ruta al handler de enrolamiento. https:

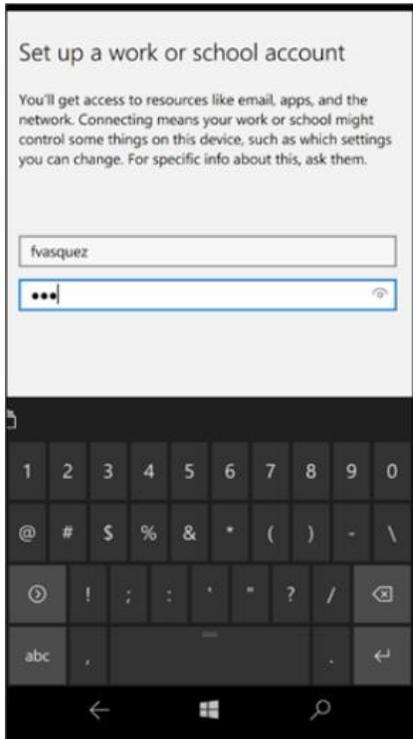
://{server}/{servicios}/WS/Mobile/W10EnrollmentHandler.ashx



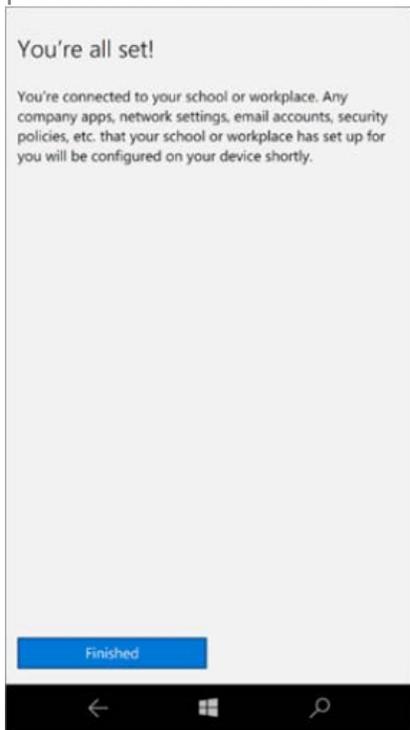
Si la ruta se escribió correctamente, el siguiente paso es Ingresar un usuario de Aranda o del dominio y el password.



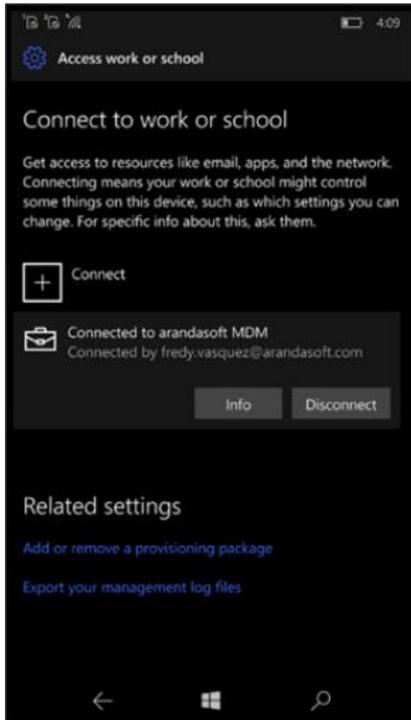
Al hacer tap en “Siguiente”, se envían los datos al servidor y se realiza el proceso de vinculación.



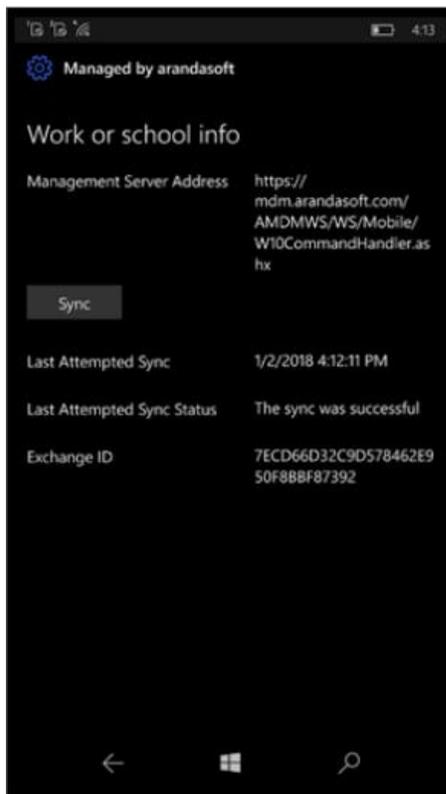
La siguiente pantalla en el dispositivo móvil indicará que se finalizó correctamente el proceso de vinculación



Para validar que la vinculación se realizó con éxito, se debe mostrarse la información de la conexión al servidor de Aranda AEMM.



Se puede hacer tap en los detalles de la conexión y ver más información del proceso y llevar a cabo el proceso de sincronización con el servidor.



5.5. Desvinculación

La desvinculación de un dispositivo se puede hacer desde la consola web o desde el dispositivo.

5.5.1. Desde la consola Web

Cuando un dispositivo se encuentra vinculado, este se puede identificar desde la consola web mediante una marca de color verde ubicada en la parte izquierda de la lista de dispositivos.

The screenshot shows the 'Dispositivos' (Devices) section of the Aranda Enterprise Mobility Management web console. On the left, there are filters for Platform (IOS, Android, Windows, Desconocida), Status (Vinculados, Pendientes, Desvinculados), Lost Mode (Activo, Inactivo), and Type (Teléfonos, Tablets, Computador de). The main area displays a list of devices, with the 'Motorola Luis Arbesu' device highlighted in a red box. To the right, a detailed view of this device is shown, including its status (Vinculados), last report, and a map of its location. The 'Desvincular' button is visible in the top right corner of the detailed view.

Para desvincular un dispositivo, selecciónelo de la lista de dispositivos, y de clic en **Desvincular** ubicado en el panel del lado derecho de la consola web. El sistema le preguntará que confirme si desea desvincular el dispositivo.

This screenshot is identical to the one above, but with the 'Desvincular' button in the detailed view of the 'Motorola Luis Arbesu' device highlighted with a red box to indicate the action to be taken.

Si la desvinculación se hace por este procedimiento se debe esperar unos minutos para que el dispositivo reciba la notificación de que fue desvinculado.

5.5.2. Desde el dispositivo

Para desvincular un dispositivo desde la aplicación móvil, despliegue el menú de opciones lateral y seleccione **Configuración**.



En la vista de **Configuración**, seleccione la opción **Desvincular dispositivo**, la aplicación despliega la pantalla donde está la opción para desvincular, si da clic en el botón **Desvincular**, la aplicación mostrará un mensaje de alerta para confirmar el proceso que se va a hacer.



Si el usuario confirma la desvinculación, la aplicación muestra un mensaje informativo y deja a la aplicación en la ventana inicial del proceso de enrolamiento.

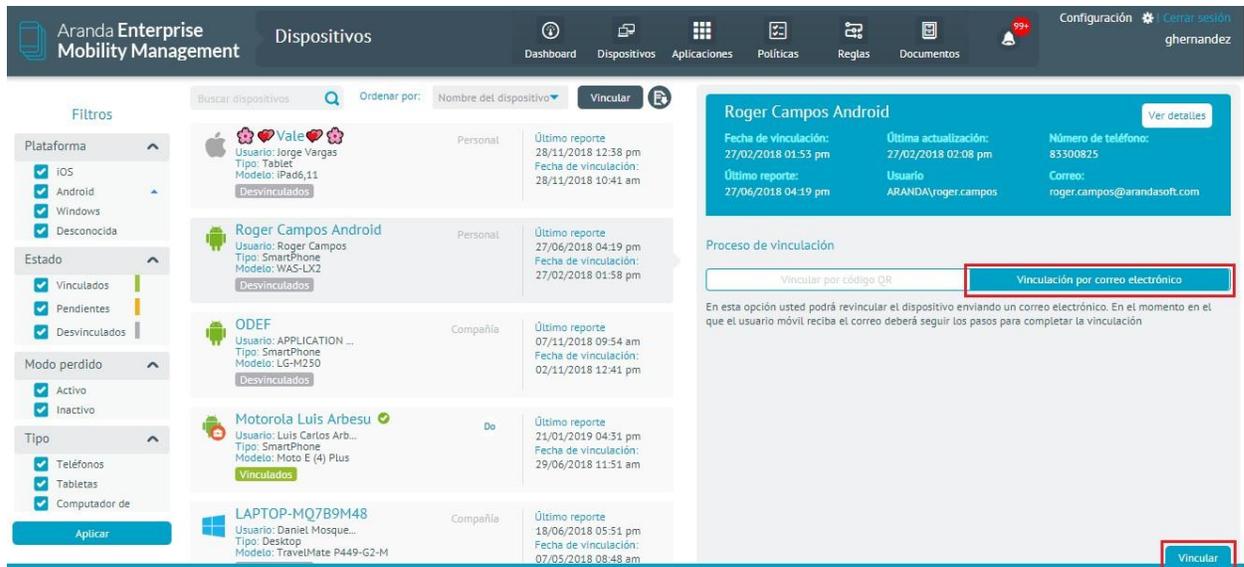


5.6. Re-vinculación de dispositivos

Para volver a vincular un dispositivo lo puede hacer desde la consola escaneando el código QR generado para cada dispositivo el cual contiene la información del usuario.

Dispositivo	Usuario	Tipo	Modelo	Estado	Último reporte	Fecha de vinculación
Vale	Jorge Vargas	Tablet	iPad6,11	Desvinculados	28/11/2018 12:38 pm	28/11/2018 10:41 am
Roger Campos Android	Roger Campos	SmartPhone	WAS-LX2	Desvinculados	27/06/2018 04:19 pm	27/02/2018 01:58 pm
ODEF	APPLICATION ...	SmartPhone	LG-M250	Desvinculados	07/11/2018 09:54 am	02/11/2018 12:41 pm
Motorola Luis Arbesu	Luis Carlos Arb...	SmartPhone	Moto E (4) Plus	Vinculados	21/01/2019 04:31 pm	29/06/2018 11:51 am
LAPTOP-MQ7B9M48	Daniel Mosque...	Desktop	TravelMate P449-G2-M		19/06/2018 05:51 pm	02/06/2018 08:16 am

También puede volver a vincular un dispositivo enviando un correo electrónico escogiendo la opción Vinculación por correo electrónico del selector y dando clic en Vincular.



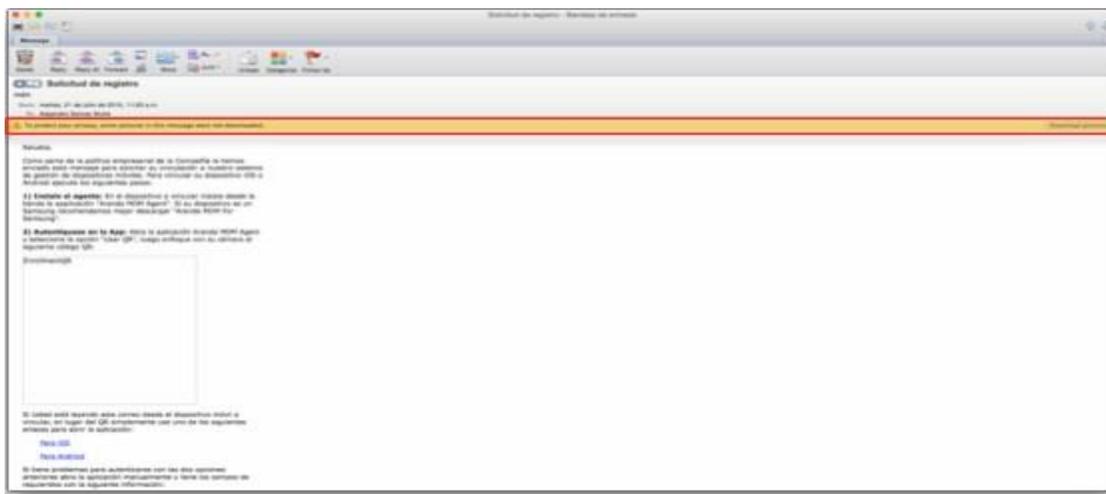
5.7. Problemas comunes de vinculación

El correo no llega

En ocasiones puede ocurrir que el correo se demore unos minutos en llegar debido a que este debe pasar por un servidor saliente y otro entrante, lo que se traduce en dos procesos cuya velocidad depende de las peticiones que se hagan sobre los servidores y de la velocidad de la conexión a internet.

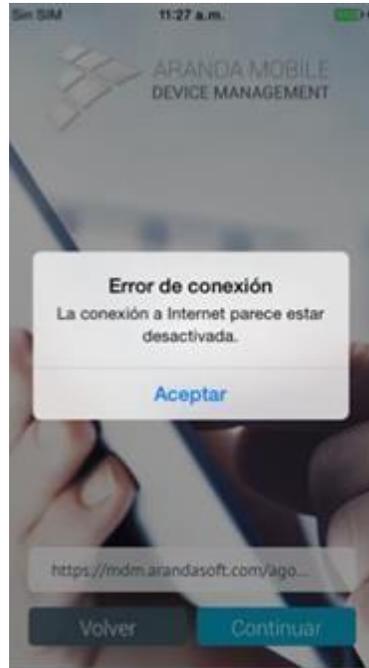
Cuando abro el correo, la imagen con el código QR no aparece

Esto puede presentarse por dos razones: porque el servidor de correos bloquea las imágenes de correos entrantes, en este caso se debe realizar la autorización para descargar las imágenes adjuntas al correo.



O porque la imagen aún no ha cargado, en este caso se debe esperar un momento más para que la imagen cargue o refrescar el correo.

La aplicación presenta un mensaje de error de conexión



Esto se debe a que el dispositivo no está conectado a ninguna red o su conexión es muy débil, debe tratar de buscar una conexión más estable o desactivar y volver a activar la conexión existente.

El despachador web no redirige el dispositivo para instalar el perfil (aplica solo para dispositivos iOS)

Dependiendo de la velocidad de la descarga del perfil desde el despachador, este re direccionamiento puede demorarse unos segundos, se puede verificar si la descarga se está realizando con el indicador de actividad del dispositivo ubicado en la parte superior.



La aplicación presenta un mensaje de error para descargar el perfil (aplica solo para dispositivos iOS).

Este mensaje se puede presentar porque el perfil aún no ha sido descargado o porque ya se descargó, pero aún no hay una respuesta de confirmación del servidor. Para verificar si el perfil ya fue instalado, de clic en **Ajustes > General > Perfil**, si el perfil se encuentra instalado y el mensaje continúa apareciendo, se debe esperar un momento mientras el servidor procesa la información.

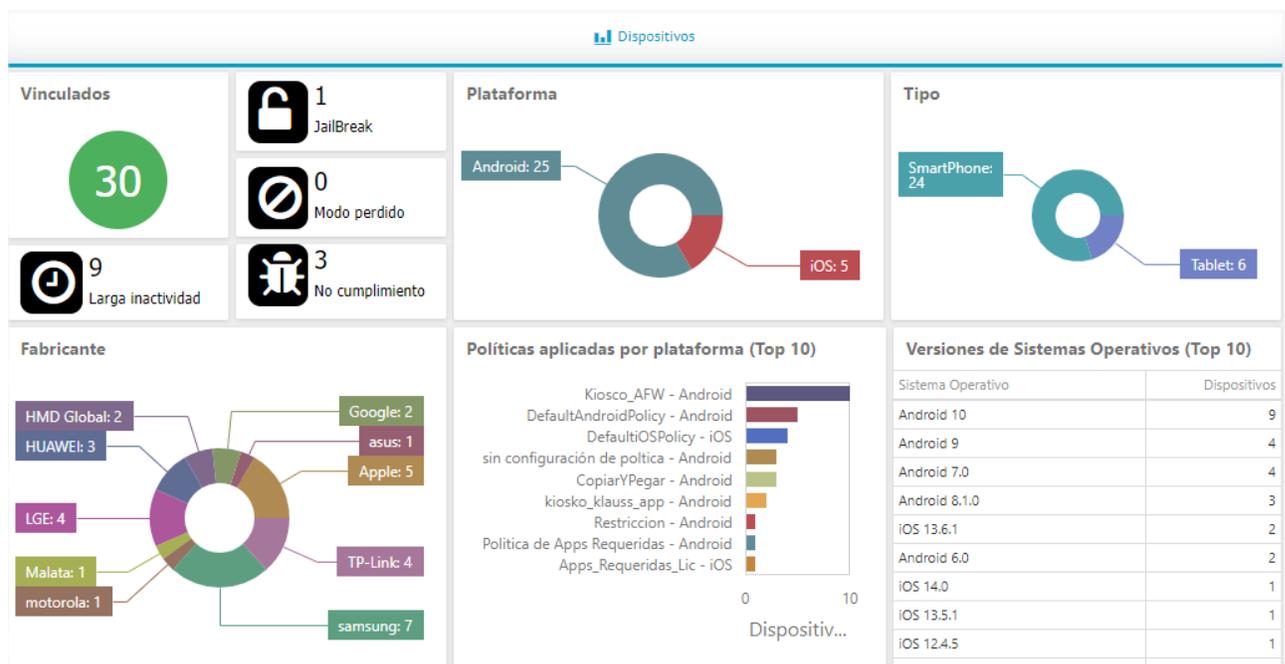


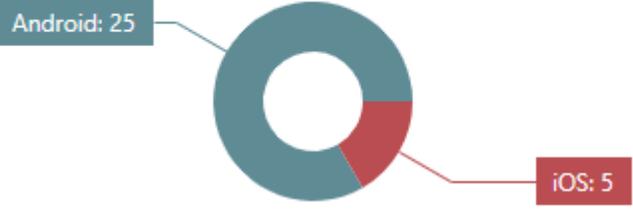
6. DASHBOARDS

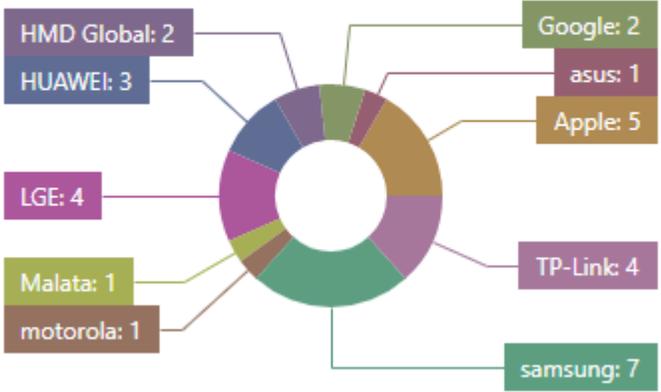
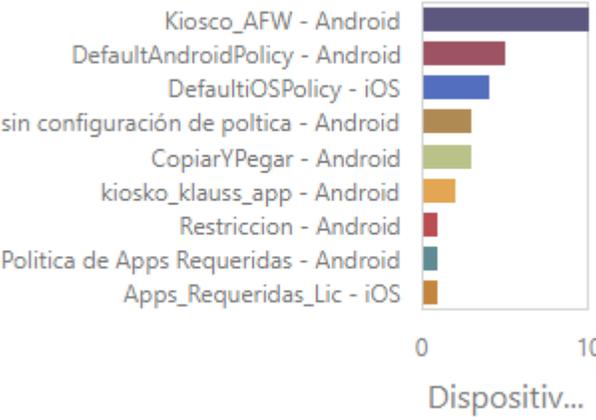
La sección de inicio de la plataforma, por defecto es la sección de Dashboard, es decir, apenas se inicia sesión en la plataforma para un usuario que tiene permisos de acceso a Dashboard es redirigido a esta sección. Dentro de la sección de Dashboard se puede consultar información estadística de forma rápida que nos muestra un pequeño resumen de las tendencias respecto a los datos de los dispositivos que se administran desde la consola. Cada uno de los tableros y sus respectivos gráficos son configurables desde la base de datos y se actualizan a partir de la lógica de negocio de la aplicación. Es posible acceder a Dashboard en cualquier momento desde la opción del menú principal de la consola de administración.

6.1. Dashboard de Dispositivos

El Dashboard de dispositivos presenta información estadística y de conteo para los dispositivos actualmente vinculados al servidor AEMM.



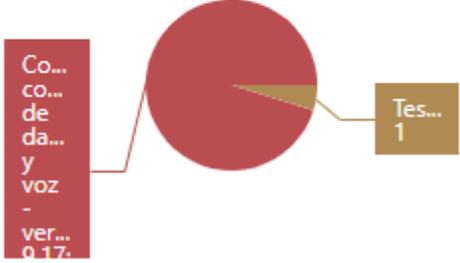
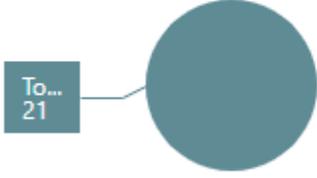
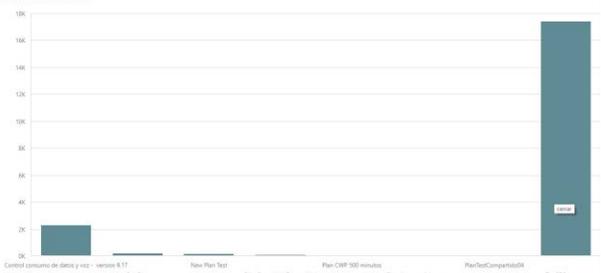
Indicador	Descripción						
<p>Vinculados</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>30</p> </div> <div style="border: 1px solid #ccc; padding: 5px; width: 150px;">  1 JailBreak </div> <div style="border: 1px solid #ccc; padding: 5px; width: 150px;">  0 Modo perdido </div> <div style="border: 1px solid #ccc; padding: 5px; width: 150px;">  9 Larga inactividad </div> <div style="border: 1px solid #ccc; padding: 5px; width: 150px;">  3 No cumplimiento </div> </div>	<ul style="list-style-type: none"> • Cantidad de dispositivos vinculados actualmente. • Cantidad de dispositivos con seguridad quebrantada (root y jailbreak). • Cantidad de dispositivos en modo perdido • Cantidad de dispositivos con larga inactividad • Cantidad de dispositivos que incumplen la política asignada. 						
<p>Plataforma</p>  <table border="1" style="margin-top: 10px;"> <thead> <tr> <th>Plataforma</th> <th>Cantidad</th> </tr> </thead> <tbody> <tr> <td>Android</td> <td>25</td> </tr> <tr> <td>iOS</td> <td>5</td> </tr> </tbody> </table>	Plataforma	Cantidad	Android	25	iOS	5	<ul style="list-style-type: none"> • Cantidad de dispositivos vinculados por plataforma
Plataforma	Cantidad						
Android	25						
iOS	5						
<p>Tipo</p>  <table border="1" style="margin-top: 10px;"> <thead> <tr> <th>Tipo</th> <th>Cantidad</th> </tr> </thead> <tbody> <tr> <td>SmartPhone</td> <td>24</td> </tr> <tr> <td>Tablet</td> <td>6</td> </tr> </tbody> </table>	Tipo	Cantidad	SmartPhone	24	Tablet	6	<ul style="list-style-type: none"> • Cantidad de dispositivos por tipo
Tipo	Cantidad						
SmartPhone	24						
Tablet	6						

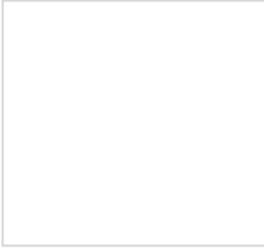
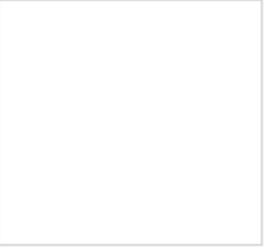
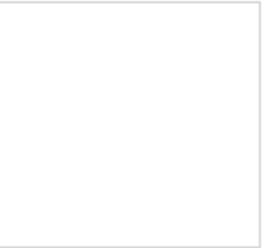
<p>Fabricante</p>  <p> HMD Global: 2 HUAWEI: 3 LGE: 4 Malata: 1 motorola: 1 Google: 2 asus: 1 Apple: 5 TP-Link: 4 samsung: 7 </p>	<ul style="list-style-type: none"> Cantidad de dispositivos por fabricante 																				
<p>Políticas aplicadas por plataforma (Top 10)</p>  <p> Kiosco_AFW - Android DefaultAndroidPolicy - Android DefaultiOSPolicy - iOS sin configuración de política - Android CopiarYPegar - Android kiosko_klauss_app - Android Restriccion - Android Política de Apps Requeridas - Android Apps_Requeridas_Lic - iOS </p> <p>0 10 Dispositiv...</p>	<ul style="list-style-type: none"> Cantidad de dispositivos por política 																				
<p>Versiones de Sistemas Operativos (Top 10)</p> <table border="1" data-bbox="186 1323 803 1785"> <thead> <tr> <th>Sistema Operativo</th> <th>Dispositivos</th> </tr> </thead> <tbody> <tr><td>Android 10</td><td>9</td></tr> <tr><td>Android 9</td><td>4</td></tr> <tr><td>Android 7.0</td><td>4</td></tr> <tr><td>Android 8.1.0</td><td>3</td></tr> <tr><td>iOS 13.6.1</td><td>2</td></tr> <tr><td>Android 6.0</td><td>2</td></tr> <tr><td>iOS 14.0</td><td>1</td></tr> <tr><td>iOS 13.5.1</td><td>1</td></tr> <tr><td>iOS 12.4.5</td><td>1</td></tr> </tbody> </table>	Sistema Operativo	Dispositivos	Android 10	9	Android 9	4	Android 7.0	4	Android 8.1.0	3	iOS 13.6.1	2	Android 6.0	2	iOS 14.0	1	iOS 13.5.1	1	iOS 12.4.5	1	<ul style="list-style-type: none"> Cantidad de dispositivos por versión de sistema operativo
Sistema Operativo	Dispositivos																				
Android 10	9																				
Android 9	4																				
Android 7.0	4																				
Android 8.1.0	3																				
iOS 13.6.1	2																				
Android 6.0	2																				
iOS 14.0	1																				
iOS 13.5.1	1																				
iOS 12.4.5	1																				

6.2. Dashboard de Consumos



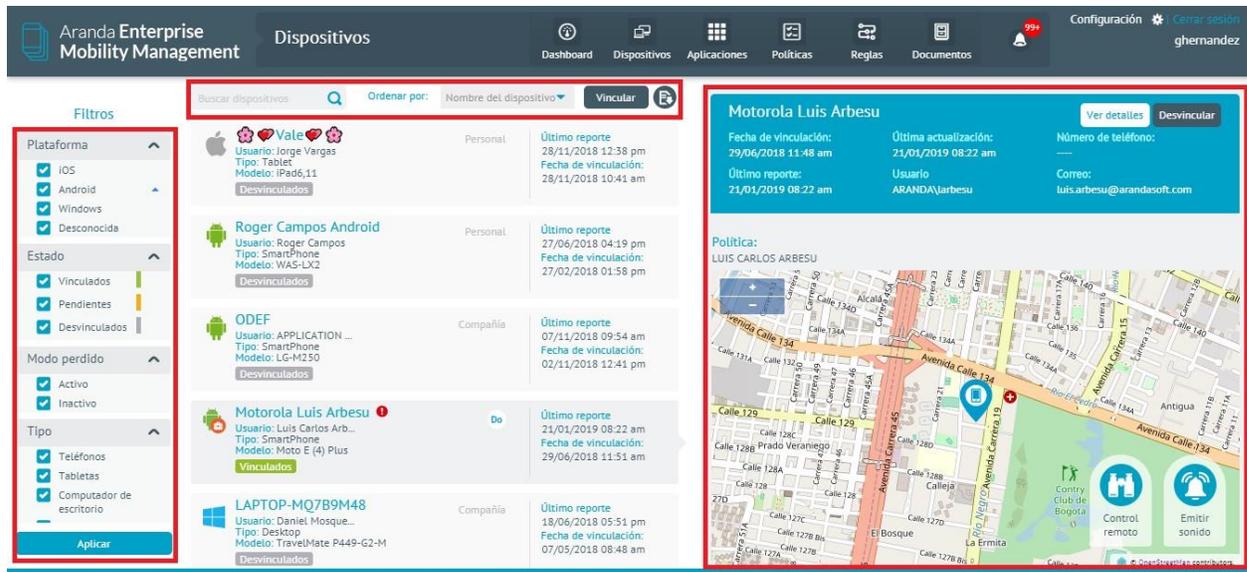
Indicador	Descripción
<p>Dispositivos con plan asignado</p> 	<ul style="list-style-type: none"> Cantidad de dispositivos con plan de consumo asignado

<h3>Dispositivos por plan</h3> 		<ul style="list-style-type: none"> • Cantidad de dispositivos por plan de consumo 								
<h3>Dispositivos por operador</h3> 		<ul style="list-style-type: none"> • Cantidad de dispositivos por Operador 								
<table border="1"> <tr> <td></td> <td>1 Excedidos en datos locales</td> </tr> <tr> <td></td> <td>0 Excedidos en voz local</td> </tr> <tr> <td></td> <td>0 Excedidos en datos de roaming</td> </tr> <tr> <td></td> <td>0 Excedidos en voz de roaming</td> </tr> </table>		1 Excedidos en datos locales		0 Excedidos en voz local		0 Excedidos en datos de roaming		0 Excedidos en voz de roaming		<p>Cantidad de dispositivos con consumos excedidos en:</p> <ul style="list-style-type: none"> • Datos Locales • Voz Local • Datos en Roaming • Voz en Roaming
	1 Excedidos en datos locales									
	0 Excedidos en voz local									
	0 Excedidos en datos de roaming									
	0 Excedidos en voz de roaming									
<p>Datos locales últimos 30 días</p> 		<ul style="list-style-type: none"> • Consumos de Datos locales por plan en los últimos 30 días 								

<p>Datos de roaming últimos 30 días</p>  <p>Control consumo de datos y voz - version Test27Consumr</p>		<ul style="list-style-type: none">• Consumos de datos en roaming por plan en los últimos 30 días
<p>Voz local últimos 30 días</p>  <p>Control consumo de datos y voz - version Test27Consumr</p>		<ul style="list-style-type: none">• Consumo de voz local por plan en los últimos 30 días
<p>Voz de roaming últimos 30 días</p>  <p>Control consumo de datos y voz - version Test27Consumr</p>		<ul style="list-style-type: none">• Consumo de voz en roaming por plan en los últimos 30 días

7. MÓDULO DISPOSITIVOS

Una vez se completa el proceso de vinculación un dispositivo podrá ser consultado y gestionado desde la consola de administración. En el menú principal dar clic en la opción "Dispositivos" para entrar al listado. Se muestra una lista que permite filtros por tipo (Smartphone, Tablet), propiedad (del usuario, de la compañía), estado (vinculado, desvinculado, pendiente), plataforma (iOS, Android) y cumplimiento (de acuerdo o no con la política aplicada). Al seleccionar un ítem de la lista se muestra en la parte derecha una pre visualización que contiene información básica y localización en mapa.



The screenshot displays the 'Dispositivos' (Devices) section of the Aranda Enterprise Mobility Management console. On the left, there is a 'Filtros' (Filters) sidebar with categories like 'Plataforma' (Platform), 'Estado' (Status), 'Modo perdido' (Lost Mode), and 'Tipo' (Type). The main area shows a list of devices, including 'Motorola Luis Arbesu'. A detailed view of this device is shown on the right, featuring a map of its location in Bogotá, Colombia, and various control buttons like 'Control remoto' (Remote Control) and 'Emitir sonido' (Ringtone).

Detalle de dispositivos (general, actividad, aplicación, ubicación)

Desde la lista de dispositivos, seleccione un ítem en estado vinculado y luego de clic en "Detalles" para ir a la hoja de vida del dispositivo. Se muestra del lado izquierdo una sección con información básica y un conjunto de controles para envío de comandos al dispositivo. En la parte hay un control de tabulado que muestra de manera separada información detallada del móvil.

7.1. Dispositivos

7.1.1. General

Permite ver información de hardware (Fabricante, modelo, IMEI, espacio disponible, etc.), software (Sistema operativo, versión de agente, versión del SO, etc.), red (ICCID o identificador de SIM card, MAC de wifi, MAC de bluetooth, roaming habilitado, operador de la SIM card, etc.) y estado (nivel de batería, almacenamiento disponible, etc.). La cantidad de información desplegada en cada una de estas secciones varía de acuerdo a la plataforma y el fabricante del dispositivo.

Hardware

- INEL/MEID: 35 92506 692529 5
- UDID: 61ef27cd6759706c712364f4de4c81335767982
- Tecnología: I
- Modelo: iPhone
- Fabricante: Apple
- Nombre del producto: iPhone7,2
- ID del Modelo: MG472LL
- Almacenamiento interno: 11,9GB
- Está liberado: NO

Red

- ICCID: 8957 7521 1114 4373 3082
- Operador de SIM: TIGO
- En roaming: false
- Dirección MAC Wi-Fi: 9c:f0:01:06:58:6d
- Dirección MAC Bluetooth: 9c:f0:01:06:58:6e
- MCC actual: 732
- MNC actual: 103
- Datos por roaming habilitados: true

Software

- Sistema operativo: iOS
- Versión de compilado: 12H143
- Firmware: 2.41.00
- Versión SO: 8.4
- Versión del agente MDM: 1.2.0.1

Estado

- Nivel de batería: 92%
- Almacenamiento disponible: 6,5GB

7.1.2. Actividad

Permite ver un listado de todos los eventos ocurridos en el móvil, ordenados por fecha de ocurrencia. Este listado de actividad muestra el ciclo de vida de los comandos (envío, recepción en el móvil y ejecución), así como los eventos registrados (envío de localización, salida o entrada de zonas, desvinculación, etc.)

General | **Actividad** | Aplicaciones | Ubicación | Consumo | CI

Registro de actividad | Comandos pendientes | Sesiones de control remoto

Buscar [] Actualizar Exportar registro

Fecha y hora	Tipo de evento	Evento	Usuario
28/09/2020 03:20:20 pm	Evento del móvil	Nueva ubicación reportada (No se detectó movimiento)	-----
28/09/2020 02:59:15 pm	Evento del móvil	Nueva ubicación reportada (No se detectó movimiento)	-----
28/09/2020 02:41:19 pm	Comando recibido	Comando recibido en el dispositivo. Tipo: Acción. Nombre: InstallApplication: com.arandasoft.amdm.content	-----
28/09/2020 02:40:15 pm	Evento del móvil	Nueva ubicación reportada (No se detectó movimiento)	-----
28/09/2020 02:31:18 pm	Comando enviado	Comando enviado. Tipo: Política. Nombre: Kiosco_AFW	-----
28/09/2020 02:26:35 pm	Comando enviado	Comando enviado. Tipo: Acción. Nombre: InstallApplication: com.arandasoft.amdm.content	-----
28/09/2020 02:26:22 pm	Evento del móvil	Instalación de aplicación en dispositivo : com.arandasoft.dialer	-----
28/09/2020 02:26:21 pm	Evento del móvil	Instalación de aplicación en dispositivo : com.google.android.gm	-----
28/09/2020 02:26:21 pm	Evento del móvil	Instalación de aplicación en dispositivo : duff24.com.duff24	-----

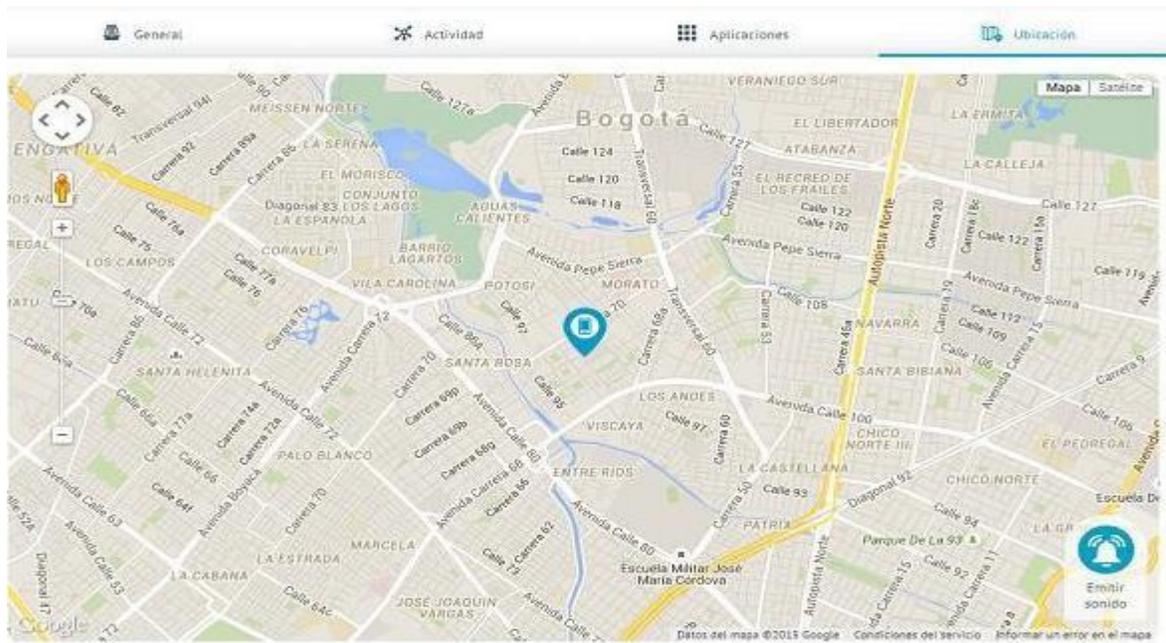
7.1.3. Aplicaciones

Permite ver el listado de aplicaciones instaladas en el móvil de acuerdo al último reporte recibido. Cada aplicación permite seleccionarse en esta lista para mostrar información detallada (descripción, categoría, etc.). En esta pantalla se puede solicitar la desinstalación de la aplicación, lo cual generará el envío del comando respectivo al móvil. En Android genérico la desinstalación se realiza con la aprobación del usuario, en Samsung se desinstalan de manera silenciosa, en iOS la desinstalación ocurre de manera silenciosa pero solo para aplicaciones instaladas desde el EMM. Desde aquí también se pueden instalar aplicaciones en el móvil. Cuando el comando de instalación se ejecuta en el móvil iOS o en Android genérico se pide automáticamente una confirmación al usuario. En móviles Samsung se muestra primero una notificación simple al usuario por algunos segundos y luego se instala sin requerir confirmación.



7.1.4. Ubicación

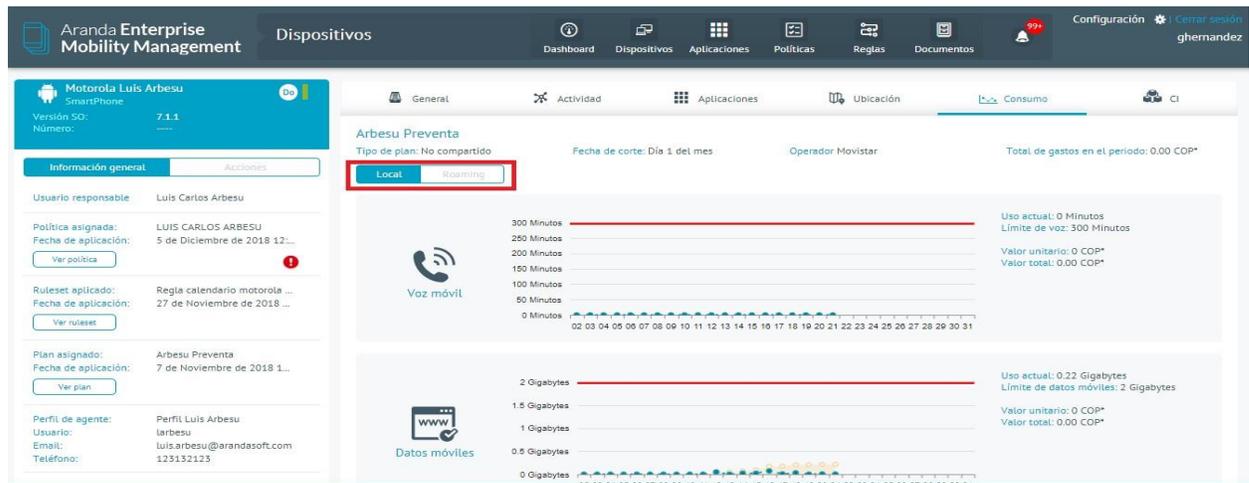
Permite ver la localización del dispositivo en un mapa de manera clara y con todas las opciones de navegación necesarias. Desde esta pantalla se puede enviar un comando de alerta sonora para ubicar el dispositivo dentro de una oficina o algún otro espacio cerrado.



7.1.5. Consumo

Esta opción nos permite ver una gráfica detallada del consumo del plan telefónico tanto de voz como de datos, está también nos permite observar el plan al cual está asignado el dispositivo y ver lo consumido localmente como en roaming en caso de tener este servicio activado.

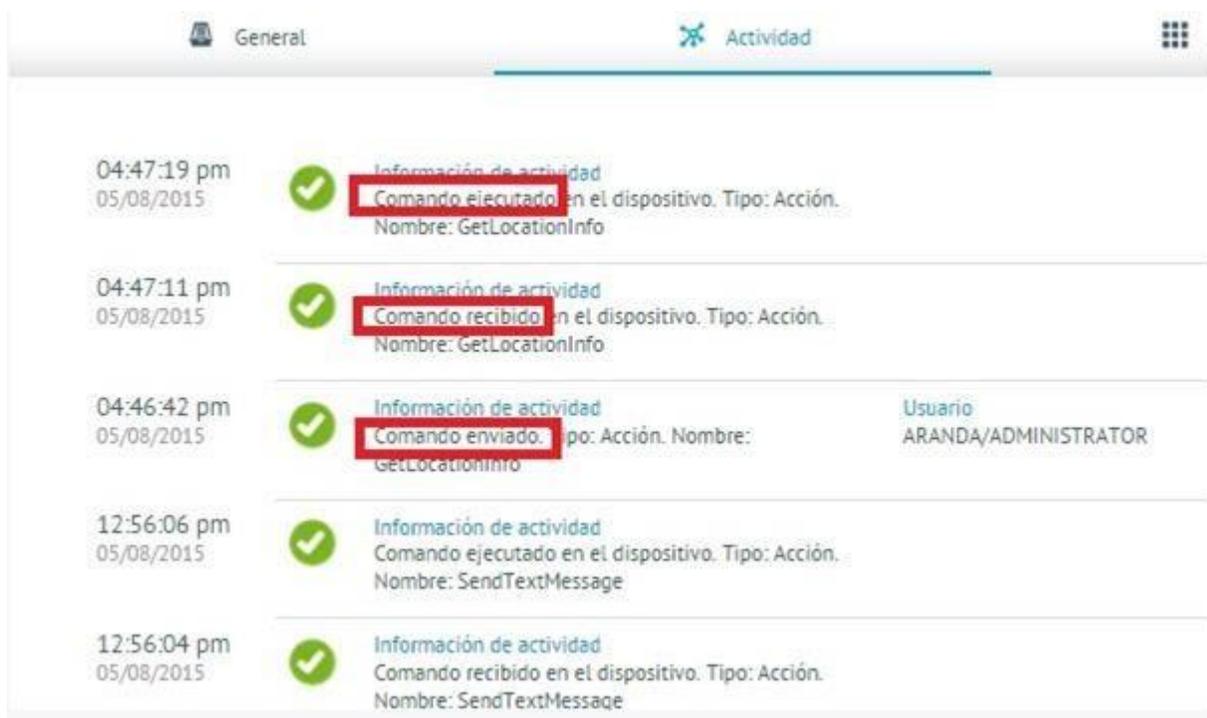
El consumo de voz móvil es visualizado en segundos y el plan de voz en Gigabytes.



Comandos

Un comando es una orden enviada al dispositivo a través del aire. Para la correcta ejecución de un comando el móvil debe tener conexión a Internet y debe poder comunicarse con el servidor EMM. Normalmente los comandos tardan segundos en

ejecutarse, sin embargo, dependiendo de las condiciones de conectividad pueden tardar minutos y hasta horas para completarse. El ciclo de vida de un comando se puede apreciar en la línea de tiempo del dispositivo (pestaña de actividad). Por cada comando se muestra en la línea de tiempo un mensaje de "Enviado" indicando que se solicitó, uno de "Recibido" indicando que ya el móvil lo obtuvo y se encuentra procesándolo y otro de "Ejecutado" que indica que el móvil ya respondió al servidor con el resultado del comando.



Los comandos en AEMM se clasifican en: **acciones, políticas y reglas**. Un comando de acción se usa para realizar un cambio o tener un efecto inmediato en el móvil sin requerir algún tipo de configuración previa.

Se pueden evidenciar los siguientes tipos de comando de **acción**:

- **Inventario:** Solicita un inventario completo del móvil (red, hardware, software, estado).
- **Localización:** Solicita únicamente los datos de ubicación del móvil
- **Mensaje:** Despliega una notificación en el móvil, invitando al usuario a dar clic para abrir la aplicación agente. La aplicación agente muestra todos los mensajes recibidos en un listado, diferenciando los que ya fueron leídos.
- **Alerta sonora:** Al igual que el comando de mensaje despliega una notificación en el móvil, pero ésta es acompañada de un sonido fuerte que permite localizarlo dentro de un espacio cerrado.

- **Cambio de contraseña (Android únicamente):** Cambia la contraseña del móvil por la que indique el administrador.
- **Bloqueo:** Realiza un bloqueo de pantalla, forzando el ingreso del password si está configurado para volver a desbloquearlo.
- **Limpiar contraseña:** Elimina la contraseña que tenga asignada el móvil, permitiendo que cualquier usuario pueda ingresar sin restricciones.
- **Restauración:** Reinicia el móvil a su configuración de fábrica. La restauración no elimina el rooteo o el jailbreak de un dispositivo.

Los comandos de tipo **política** por su parte permiten aprovisionar el dispositivo y establecer restricciones en su uso. Con un comando de política, el móvil puede obtener toda la configuración que requiere para trabajar en la Compañía: Email, wi-fi, política de contraseñas, web clips, restricciones y aplicaciones.

Para enviar una política esta debe configurarse con los valores apropiados, luego debe ser aprobada. Siempre que se envíe un comando de política se instalará la última versión aprobada (y no la última versión guardada).

Los comandos de tipo **regla** envían un conjunto de reglas a un dispositivo, con el fin de dar manejo a los eventos que sobre él ocurren. Por medio de un conjunto de reglas podemos definir las acciones a ejecutar bajo la ocurrencia de ciertos eventos como: desvinculación, salida o entrada de zonas, detección de jailbreak, incumplimiento de política, etc... Las acciones pueden incluir la desvinculación del móvil, el envío de mensajes o alertas, el cambio de política, envío de emails, etc.

Problemas comunes en manejo de dispositivos El comando no llega al dispositivo

Los dispositivos deben tener conexión a Internet para poder recibir los comandos. El tiempo de recepción depende mucho de la velocidad de la red en el móvil y en el canal del servidor. Si un comando no ha llegado es posible que el móvil esté apagado, o que la conexión esté lenta. En ambos casos el comando llegará cuando las condiciones cambien. Algunos comandos son procesados directamente por la aplicación agente. Si el agente fue suspendido manualmente no recibirá comandos, será necesario en este caso abrir la aplicación en el móvil para retomar la comunicación. Este problema se evidencia cuando en la línea de tiempo solo se muestra el mensaje de envío de comando.



Se envían muchos comandos y solo llega uno

Cuando se envía un comando a un móvil, el sistema automáticamente bloquea el envío de más comandos del mismo tipo, hasta que el primero termine su ciclo de vida. Se recomienda simplemente esperar a que el primero termine.

El comando de localización retorna un error

En la línea de tiempo se puede observar un error en el comando de localización cuando en el móvil el usuario decide deshabilitar la localización para la app. Esta situación escapa del control del EMM, ya que el usuario siempre es libre de decidir si quiere o no que lo ubiquen a través de su móvil.



El comando no se puede ejecutar en el momento

En la línea de tiempo se puede observar una advertencia en el comando de política cuando el dispositivo iOS no está disponible para procesar peticiones del EMM. Normalmente esto sucede cuando el dispositivo está bloqueado. Si esto sucede se recomienda esperar a que el dispositivo esté disponible y vaya automáticamente a recibir el comando. Normalmente el dispositivo queda disponible cuando el usuario enciende la pantalla.



En iOS la política llega, pero no se ve la descripción en el móvil

La descripción de la política aplicada es manejada exclusivamente por la aplicación agente. En iOS las políticas se despachan directamente al sistema operativo con un protocolo diferente. Puede que la comunicación con la aplicación agente sea más lenta en algunos casos. Cuando esto sucede se recomienda simplemente esperar. En cualquier caso, si el usuario abre la aplicación agente la descripción llegará.

El comando de sonido se percibe en el móvil como un comando de mensaje

Si el dispositivo tiene deshabilitado el sonido el comando de alerta sonora solo se verá como un mensaje. El EMM no tiene forma de forzar la habilitación del sonido cuando el usuario lo ha impedido a propósito.

7.2. Proyectos de Gestión

Esta función permite crear grupos (Proyectos) de dispositivos y realizar envío de configuraciones a estos de manera unificada o masiva. Esto se realiza a través de la creación de un archivo .CSV con el Imei de los equipos a los cuales se les enviará la configuración.

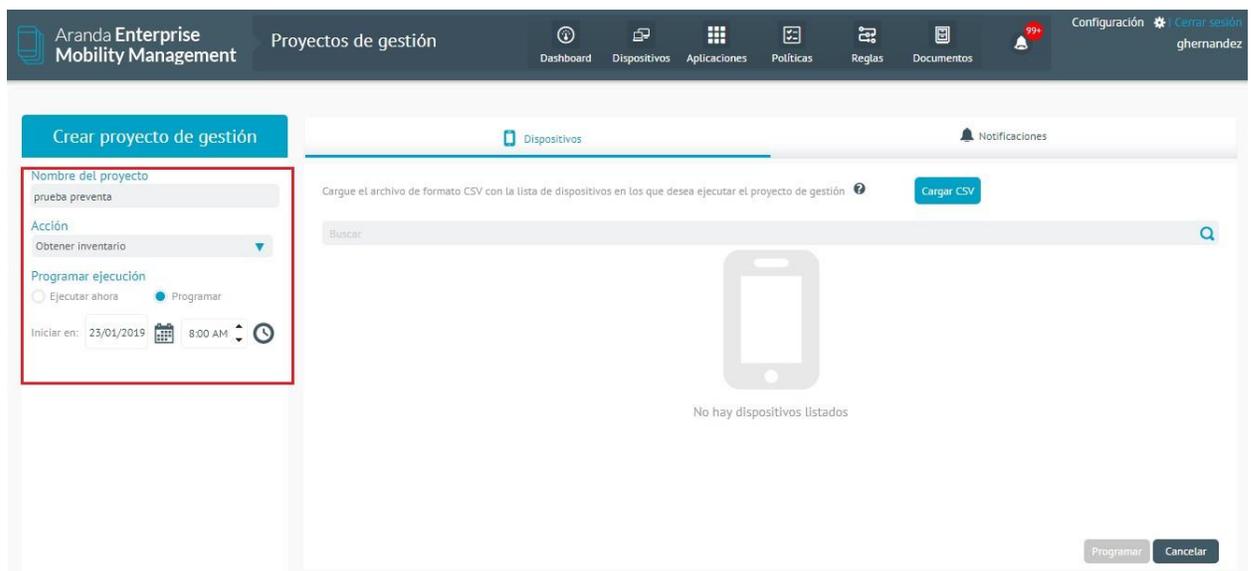
De clic en la pestaña Dispositivos y seleccione Proyectos de Gestión.



Luego de clic en la opción **Nuevo proyecto**.

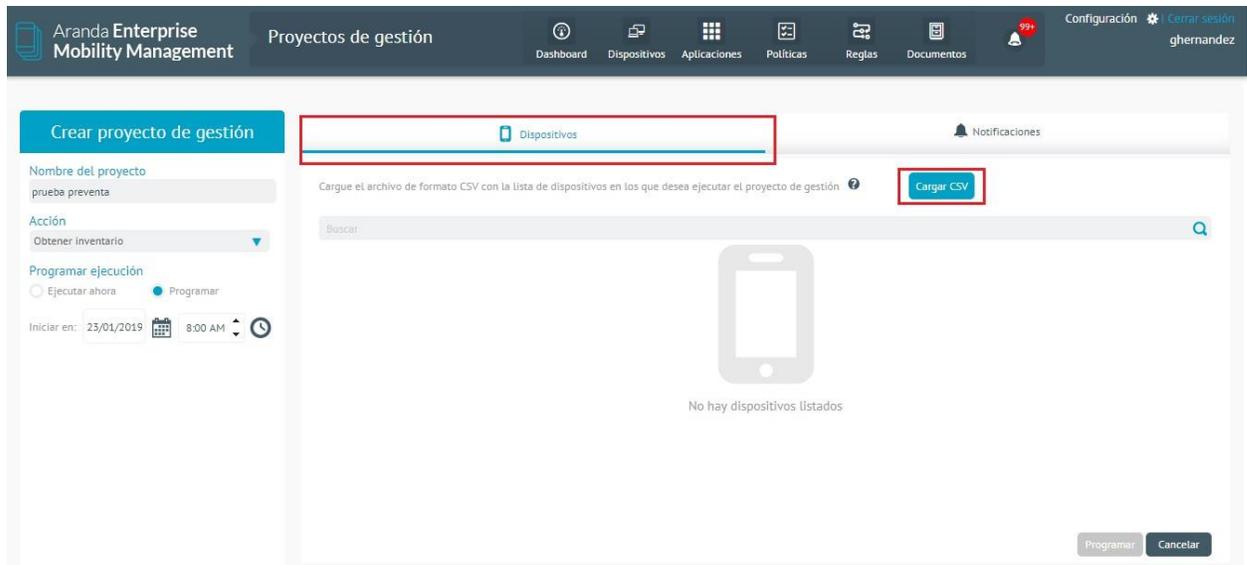


En el costado derecho, diligencie los datos del proyecto y la acción a tomar para este grupo (Dispositivos). Esta opción también le permite programar la ejecución ya sea de manera inmediata o alguna fecha y hora específica.

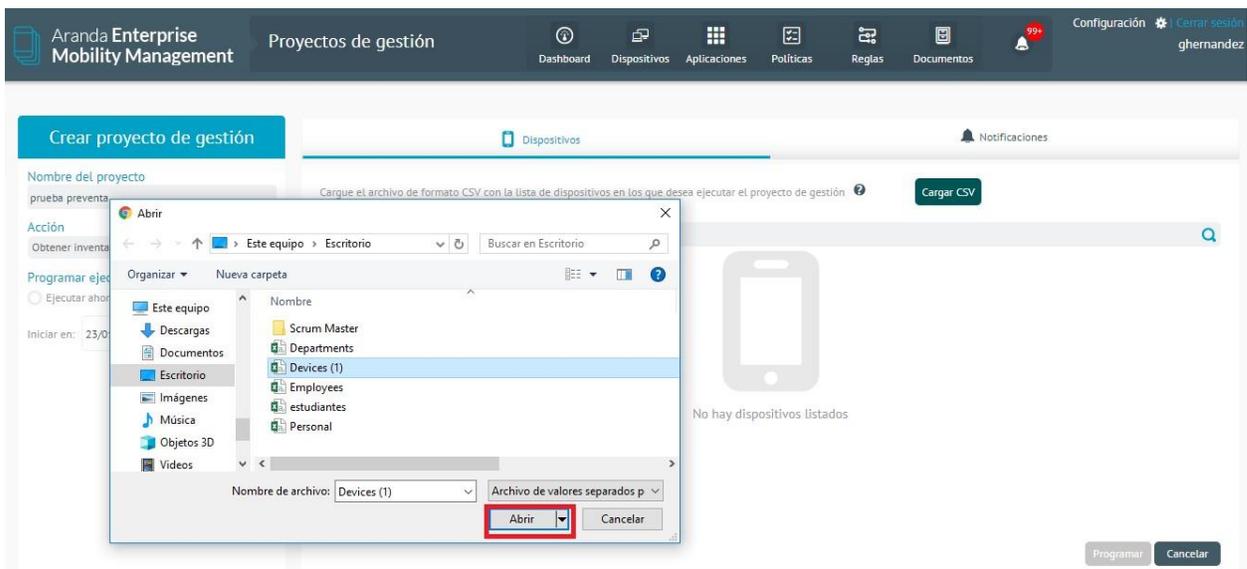


Dispositivos

Cree el listado un archivo de Excel con los números de Imei de los dispositivos y guardarlo como archivo .csv, luego de clic en la opción Cargar CSV y cargue el archivo.



Exporte el archivo CSV en la ruta en la cual lo tenga almacenado y de clic en **Abrir**.



Luego de clic en **Guardar**

Archivo CSV X

Resumen

Dispositivos encontrados

0

Dispositivos no encontrados

2

Dispositivos sin vincular

1

Tenga en cuenta que en el proyecto de gestión, se listarán únicamente los dispositivos encontrados en la base de datos y que estén vinculados al sistema.

Dispositivos con conflictos
 Los siguientes dispositivos no serán listados en el proyecto de gestión, debe revisar su archivo CSV, podría presentar datos incorrectos que no permiten detectar los dispositivos en la base de datos del sistema.

Dispositivos no encontrados	Dispositivos sin vincular
ID	Nombre del dispositivo
IMEI	
35 799305 514678 6	

Guardar
Cancelar

Notificaciones

En esta opción, configure los usuarios a los que desea enviarle notificación cuando inicie la ejecución del proyecto al igual que cuando esta culmine.

Aranda Enterprise Mobility Management
Configuración ghernandez

Crear proyecto de gestión

Nombre del proyecto: prueba prueba

Acción: Obtener inventario

Programar ejecución: Ejecutar ahora Programar

Fecha en: 23/01/2019 8:00 AM

Dispositivos
Notificaciones

Notificaciones
 Edite las notificaciones que se enviarán al iniciar y finalizar la ejecución del proyecto de gestión.

Notificación al iniciar ejecución

Para: German Hernandez (ARANDA)ghernandez

Título: prueba

Mensaje: prueba

Notificación al finalizar ejecución

Para: German Hernandez (ARANDA)ghernandez

Título: prueba

Mensaje: prueba

Programar
Cancelar

Luego de clic en **Programar**.

7.3. Gestión de Consumos

Esta opción se debe configurar si se desea realizar un seguimiento al consumo de voz y/o datos de un dispositivo móvil y para hacer uso del conjunto de reglas de gastos. A continuación:

Ingrese a pestaña Dispositivos y seleccione la opción **Gestión de Consumos** dentro del menú EMM y de clic en **Nuevo Plan**.

The screenshot shows the 'Gestión de consumos' interface. On the left, there is a list of plans with filters for 'Tipo' (Compartido, No compartido) and an 'Aplicar' button. The main area displays a list of plans, with the 'Arbesu Preventa' plan selected. On the right, a detailed view of the 'Arbesu Preventa' plan is shown, including its creation date, total devices, and current consumption statistics for local and roaming services.

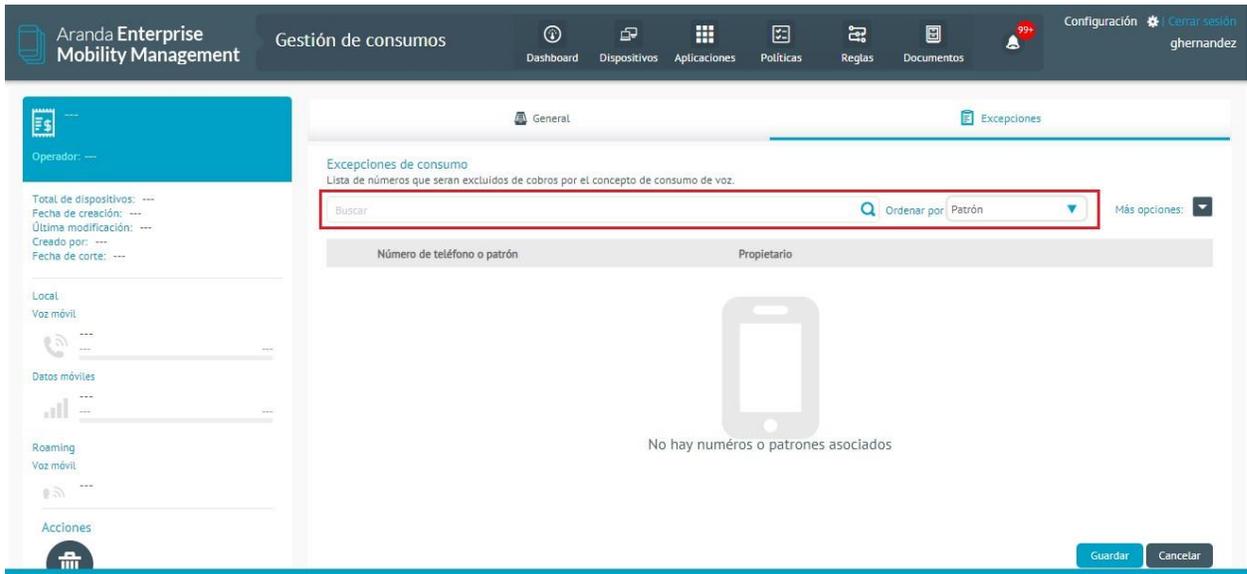
Ingrese los datos solicitados y de clic en **Guardar**.

This screenshot shows the configuration form for a new plan. The 'Información básica' section includes fields for 'Nombre' and 'Operador'. The 'Facturación' section includes 'Tipo de moneda' (set to Colombian Peso), 'Fecha de corte del plan' (set to Día 28), and 'Factor de corrección para el consumo' (set to 1.0). The 'Límites y costos' section is divided into 'Local' and 'Roaming' categories, each with fields for 'Paquete de voz' and 'Paquete de datos' with their respective costs. The 'Guardar' button is highlighted in red.

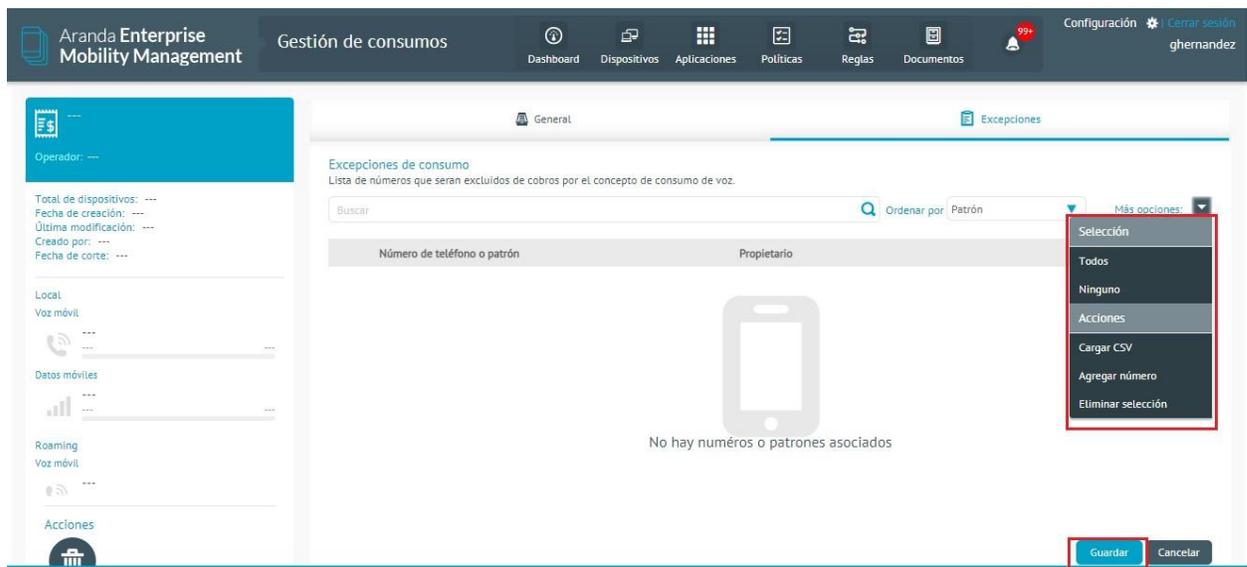
7.3.1. Excepciones

Para crear una excepción de consumo, esta se puede llevar a cabo de varias formas:

- Realizando búsqueda del número del dispositivo a través de la opción Buscar, ordenando a la vez por patrón o propietario



- La otra opción es, seleccionar un grupo de números o dispositivos cargando un archivo CSV con el listado de dispositivos a los cuales desea realizar la excepción y luego de clic en el botón **Guardar**.



8. APLICACIONES

En esta sección se podrán visualizar todas las aplicaciones que se han encontrado a través de los inventarios de los dispositivos y como resultado de la importación de aplicaciones desde cada una de las tiendas (google play y app store). +

La sección de aplicaciones funciona a manera de catálogo donde se podrán realizar diversas acciones sobre cada una de las aplicaciones y de esta manera administrar cada una de las apps con la posibilidad de realizar acciones masivas sobre los dispositivos que tienen o que no tienen instalada una aplicación específica.

Catálogo de apps

La pantalla se divide en tres columnas principales:

The screenshot shows the 'Aplicaciones' section of the Aranda Enterprise Mobility Management system. The interface includes a top navigation bar with options like Dashboard, Dispositivos, Aplicaciones, Políticas, Reglas, and Documentos. Below this, there's a search bar and a list of applications. The left sidebar has filters for 'Plataforma' (iOS, Android, Windows) and 'Origen' (Corporativo, Tienda). The main area shows a list of apps with details such as 'Dispositivos', 'Tipo', 'Fabricante', 'Versión', and 'Última actualización'. The right sidebar shows the details of the selected app, 'Lollapalooza', including its description and device information.

Filtros

En esta columna se visualizarán dos tipos de filtro uno por tipo de plataforma y otra por origen de la aplicación.

Listado

Esta parte de la pantalla comienza con un campo de búsqueda de aplicaciones donde se podrá buscar por nombre de las aplicaciones y un campo adicional para ordenar la búsqueda que se haya realizado. Un botón para importar una aplicación y otra para subir un APK empresarial. Existe otro botón en el extremo derecho de la columna en donde se puede exportar el listado logrado luego de la búsqueda realizada. El archivo exportado después de ejecutar la acción es un archivo de Excel.

Cada una de las tarjetas de resultados tiene el nombre de la aplicación, plataforma, cantidad de dispositivos que la tienen instalada, tipo de aplicaciones, desarrollador de la aplicación, versión de la aplicación y versión de la misma.

El listado es navegable con teclado para facilitar al usuario su navegación y poder ver uno a uno el detalle de cada ítem.

Detalle de la aplicación

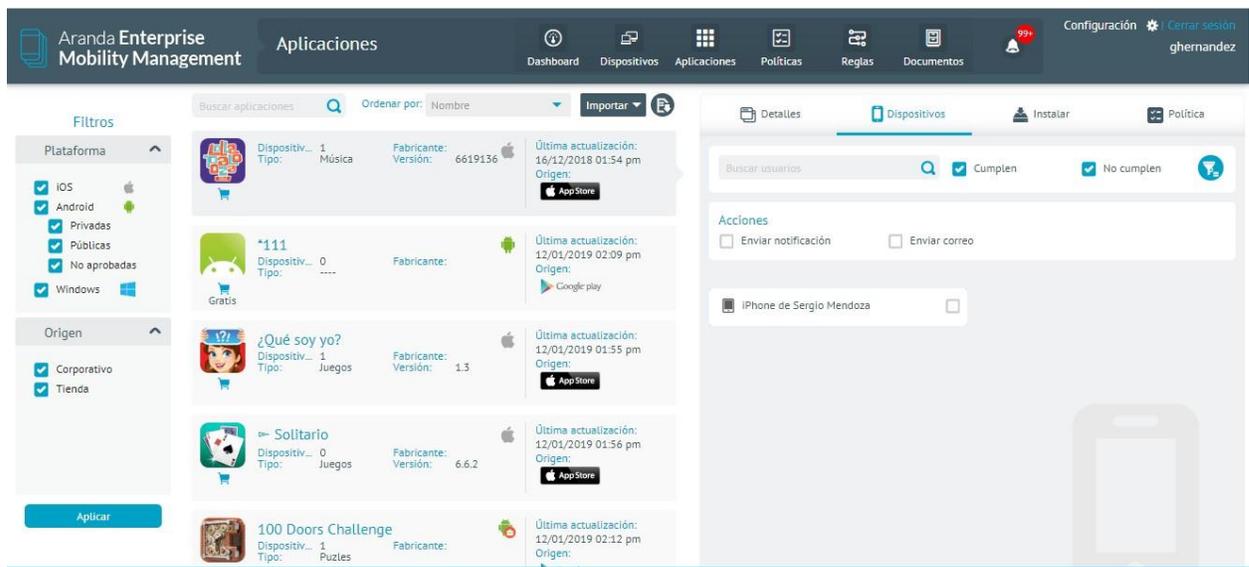
En la parte derecha de la pantalla se encuentra el detalle del ítem del listado. Esta zona tiene 4 pestañas que dividen la información de la aplicación en; detalle, dispositivos, instalar y política. En la primera pestaña de este detalle se encuentra la descripción general de la app con la siguiente información:

- Icono de la aplicación. – Tipo de aplicación. – Cantidad de dispositivos que tiene la aplicación. – Última actualización. – Versión de la aplicación.

En la parte inferior de esta pestaña se encuentra la calificación de la aplicación dada por los usuarios en cada una de las tiendas de donde provienen.

Por último, se muestra la descripción de la aplicación dada por el desarrollador de la misma.

En la segunda pestaña (**Dispositivos**) se encuentran los dispositivos que ya tienen instalada la aplicación y a los cuales se le pueden realizar tres acciones dependiendo del tipo de dispositivo:



Desinstalar

Esta acción solo está disponible para dispositivos Android Knox. En caso de que el dispositivo tenga esta condición se podrán realizar desinstalaciones de app que se hallan instalado a través del EMM.

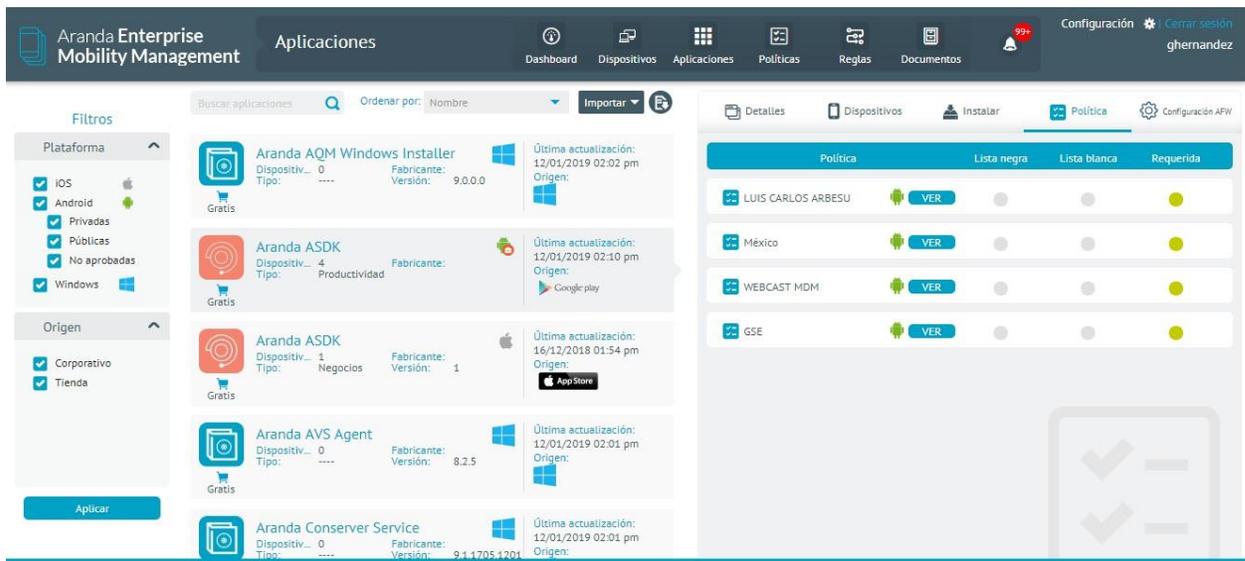
Enviar notificación

Esta acción se puede realizar a cualquier tipo de dispositivo (Android o iOS) y se utiliza al dar clic en la casilla y se activan dos campos. Uno de asunto que tiene por defecto el nombre de la aplicación con la cual se relacionará el mensaje. Y un segundo campo donde podrá escribir el cuerpo del mensaje.

Esta acción tiene la posibilidad de seleccionar a cuáles dispositivos desea enviarle la notificación, para esto se cuenta con un campo de búsqueda donde se podrá ingresar el criterio de nombre de dispositivo. Adicional a esta herramienta se podrá filtrar el listado por los dispositivos que cumplen o incumplen la política que tenga relacionada la aplicación. Para realizar esta acción cada vez que se escoja uno de estos filtros se debe dar clic en el botón de filtrar para realizar el refinamiento.

La tercera pestaña (**Instalar**) se utiliza para buscar, agregar e instalar la aplicación en los dispositivos que se agregaron.

En la cuarta pestaña (**política**) se muestra la(s) política(s) en las cuales se incluyó la aplicación y en qué tipo de lista (negra, blanca o requeridas). También se encuentra un botón para poder ir a ver la política a la que se hace referencia.



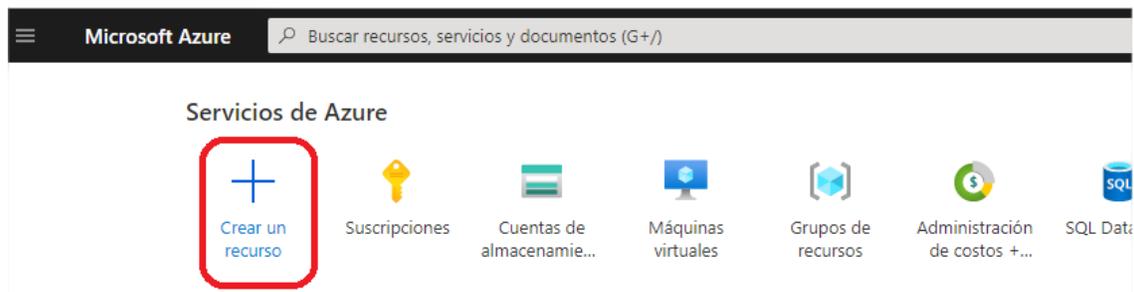
8.1. Instalación de aplicaciones usando una URI externa

Precondiciones:

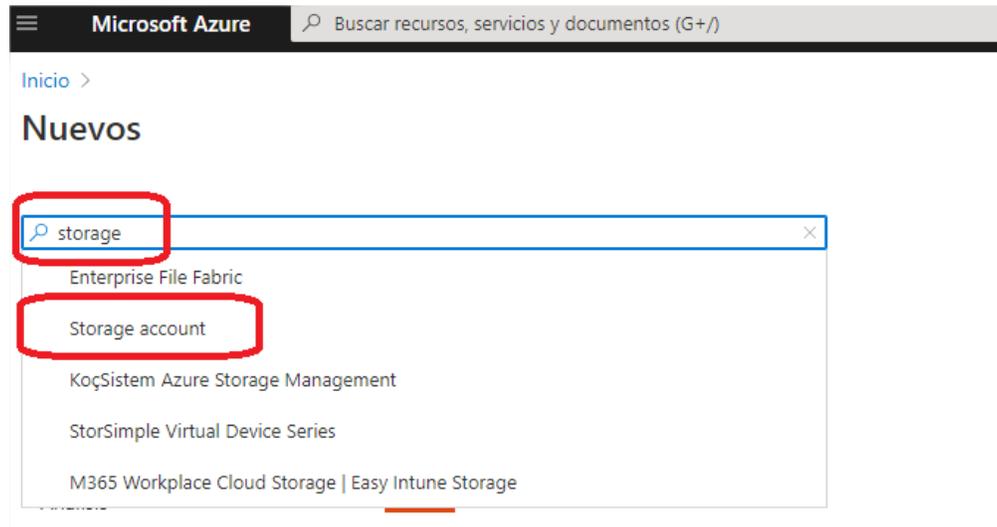
- Una cuenta activa y con saldo disponible en Microsoft Azure
- Archivo APK/IPA de la aplicación en cuestión
- Nombre del paquete de la aplicación

8.1.1. Proceso De Carga Y Publicación De Archivo En Microsoft Azure

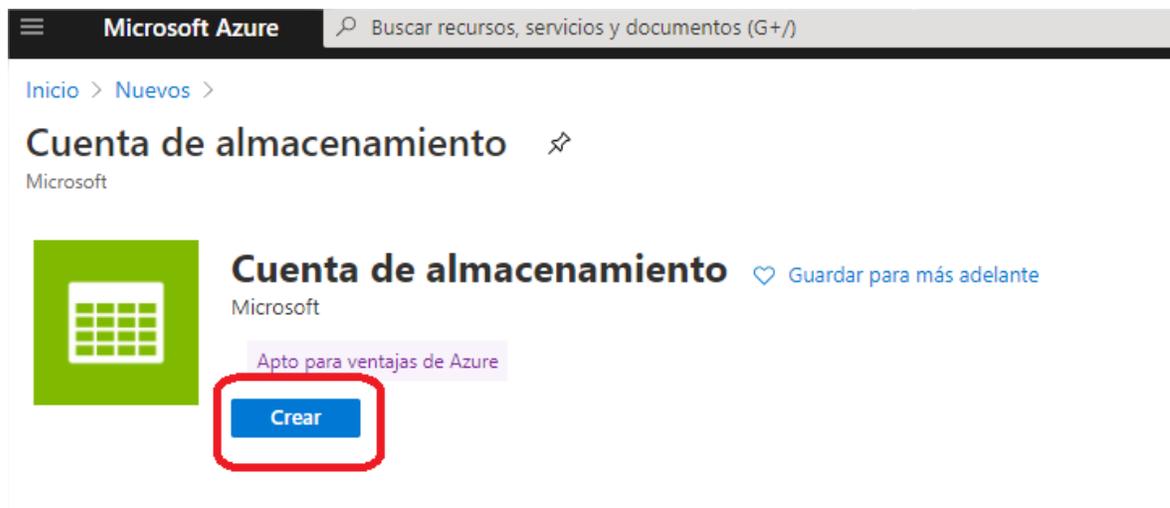
- Ingresa a Microsoft Azure (<https://portal.azure.com/#home>)
- Clic en la opción crear un recurso



- c. Escriba en la barra de búsqueda de recursos la palabra “storage” y luego clic en “Storage Account” o en español “Cuenta de almacenamiento”



- d. Clic en “Crear”



- e. Escoja la suscripción y escoja o cree un grupo de recursos

organizar y administrar todos los recursos.

Suscripción *

Grupo de recursos *

Detalles de instancia

El modelo de implementación predeterminado es el de Resource Manager, que admite las últimas características de Azure. Como alternativa, puede elegir el modelo de implementación clásica.

Nombre de la cuenta de almacenamiento *

Ubicación *

Un grupo de recursos es un contenedor que tiene los recursos relacionados de una solución de Azure.

Nombre *

- f. Escriba el nombre de la cuenta de almacenamiento, escoja la ubicación o simplemente déjela en la predeterminada, en el tipo de cuenta escoja “BlobStorage”, y por ultimo escoja la replicación con redundancia local (opción más económica), o escoja el tipo de replicación a su conveniencia.

Detalles de instancia

El modelo de implementación predeterminado es el de Resource Manager, que admite las últimas características de Azure. Como alternativa, puede elegir el modelo de implementación clásica. [Elegir el modelo de implementación clásica](#)

Nombre de la cuenta de almacenamiento *

Ubicación *

Rendimiento Estándar Premium

Tipo de cuenta

Replicación

Las cuentas con el tipo de replicación y rendimiento seleccionados solo admiten blobs en bloques y anexos. No estarán disponibles los blobs en páginas, recursos compartidos de archivos, tablas ni colas.

- g. Haga clic en “Revisar y crear”

Rendimiento ⓘ Estándar Premium

Tipo de cuenta ⓘ

Replicación ⓘ

i Las cuentas con el tipo de replicación y rendimiento seleccionados solo blobs en bloques y anexos. No estarán disponibles los blobs en páginas, compartidos de archivos, tablas ni colas.

Revisar y crear < Anterior Siguiente: Redes >

g. Haga clic en “Crear”

Crear cuenta de almacenamiento

✓ Validación superada

Datos básicos Redes Protección de datos Opciones avanzadas Etiquetas Revisar y crear

Datos básicos

Suscripción	Ricardo Chicangana Solano – MPN
Grupo de recursos	(Nuevo) StorageAccountGroup
Ubicación	Oeste de EE. UU.
Nombre de la cuenta de almacenamiento	storageaccntttest
Modelo de implementación	Resource Manager
Tipo de cuenta	BlobStorage
Replicación	Almacenamiento con redundancia local (LRS)
Rendimiento	Estándar

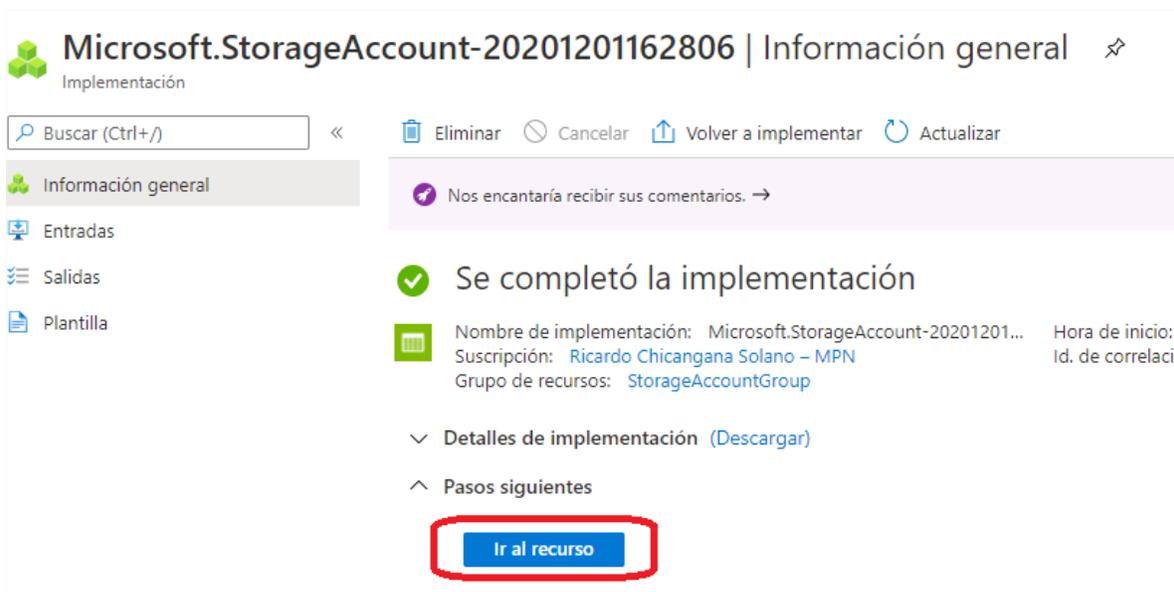
Redes

Crear < Anterior Siguiente > [Descargar una plantilla para la automatización](#)

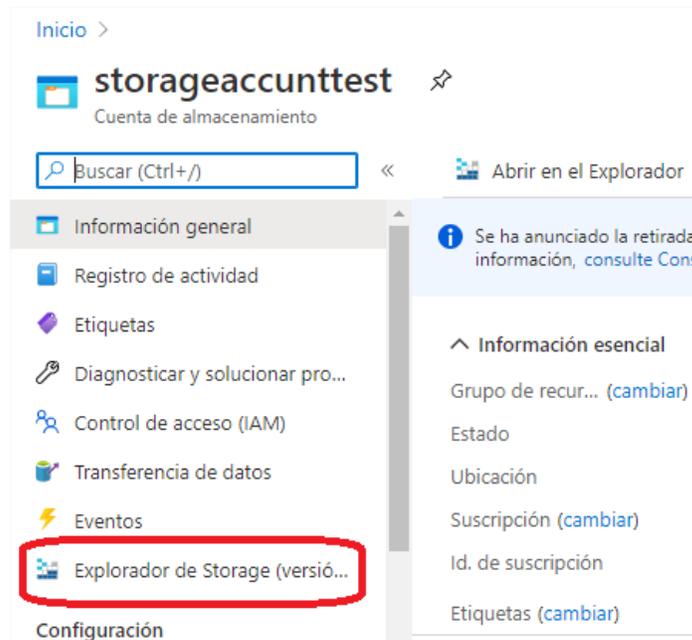
h. Espere a que el recurso sea creado



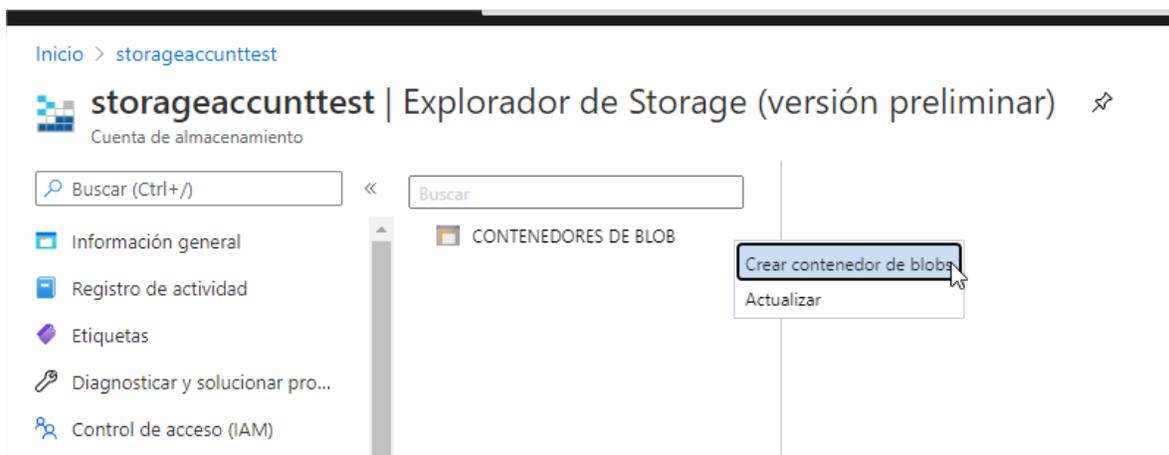
i. Una vez creado el recurso haga clic en “Ir al recurso”



j. En la interfaz del recurso haga clic en “Explorador de Storage”



k. Ya en el explorador, haga clic derecho sobre “CONTENEDORES DE BLOB”, luego en el menú emergente haga clic sobre “Crear contenedor de blobs”



a. Ingrese el nombre del nuevo contenedor y luego haga clic en “Crear”

Nuevo contenedor ×

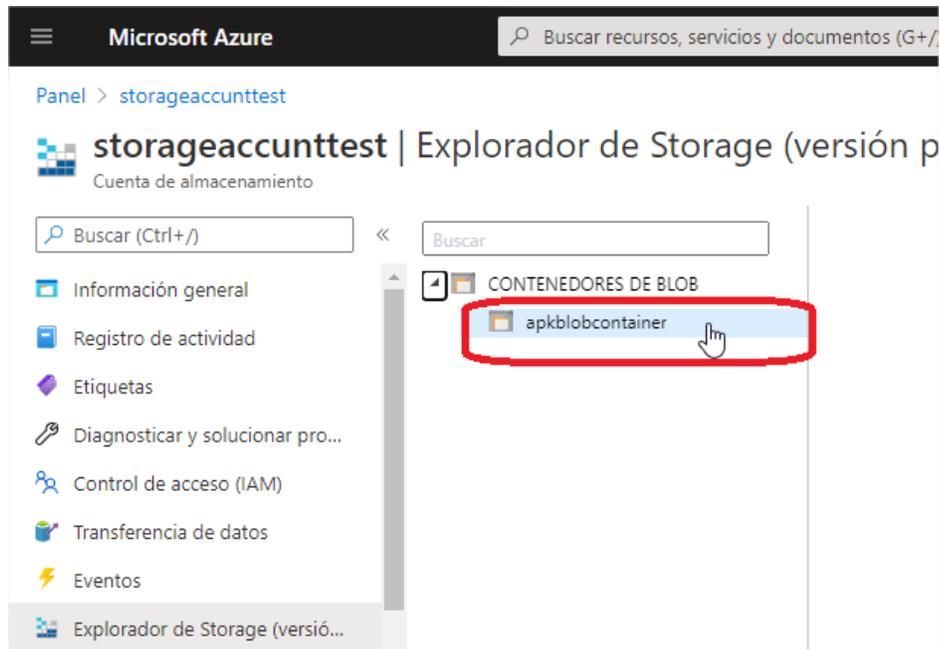
Nombre *
apkblobcontainer ✓

Nivel de acceso público ⓘ
Privada (sin acceso anónimo) ▼

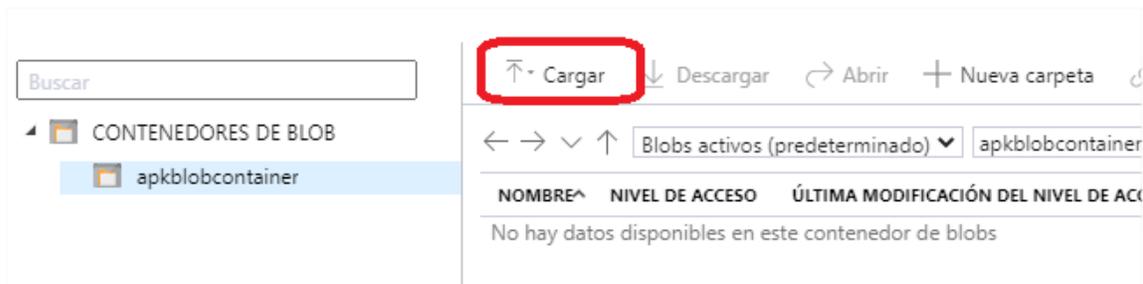
▼ Avanzado

Crear Descartar

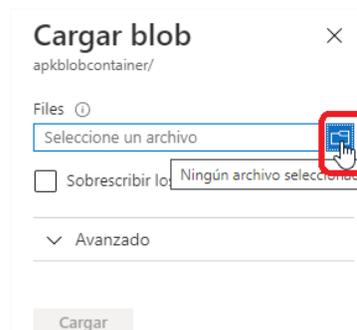
- I. De ser necesario refresque la página para que aparezca el nuevo contenedor creado. Luego expanda el árbol de contenedores y haga clic sobre el que se acaba de crear.



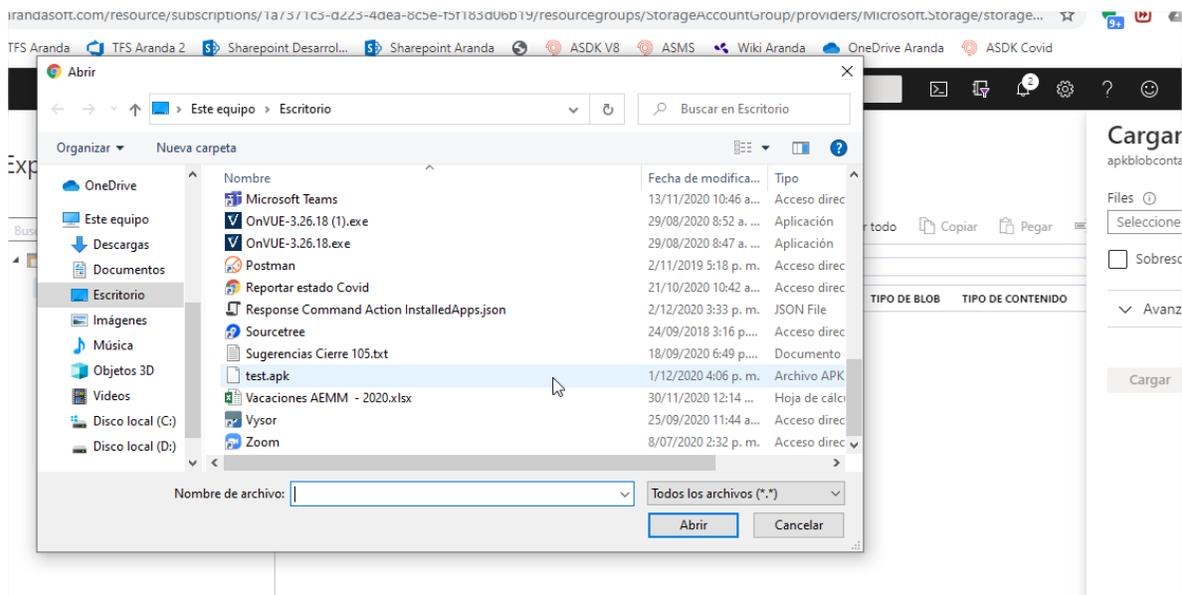
m. Haga clic en “Cargar”



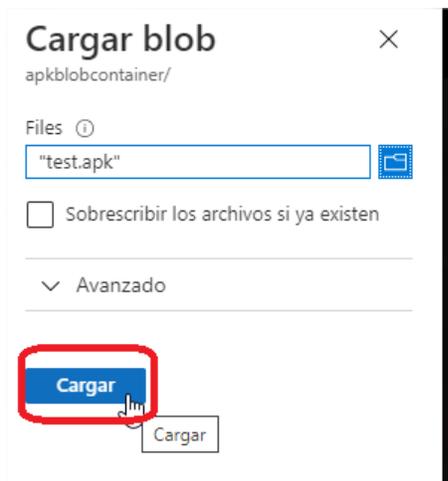
n. Haga clic en el ícono de archivo



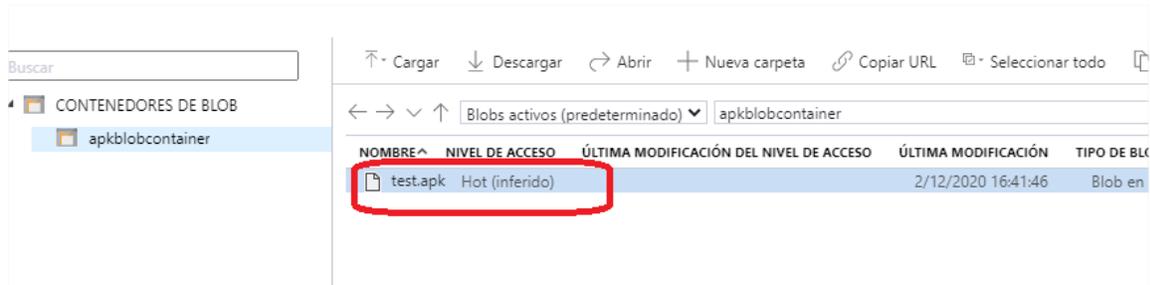
o. Ubique y escoja el archivo APK o IPA específico



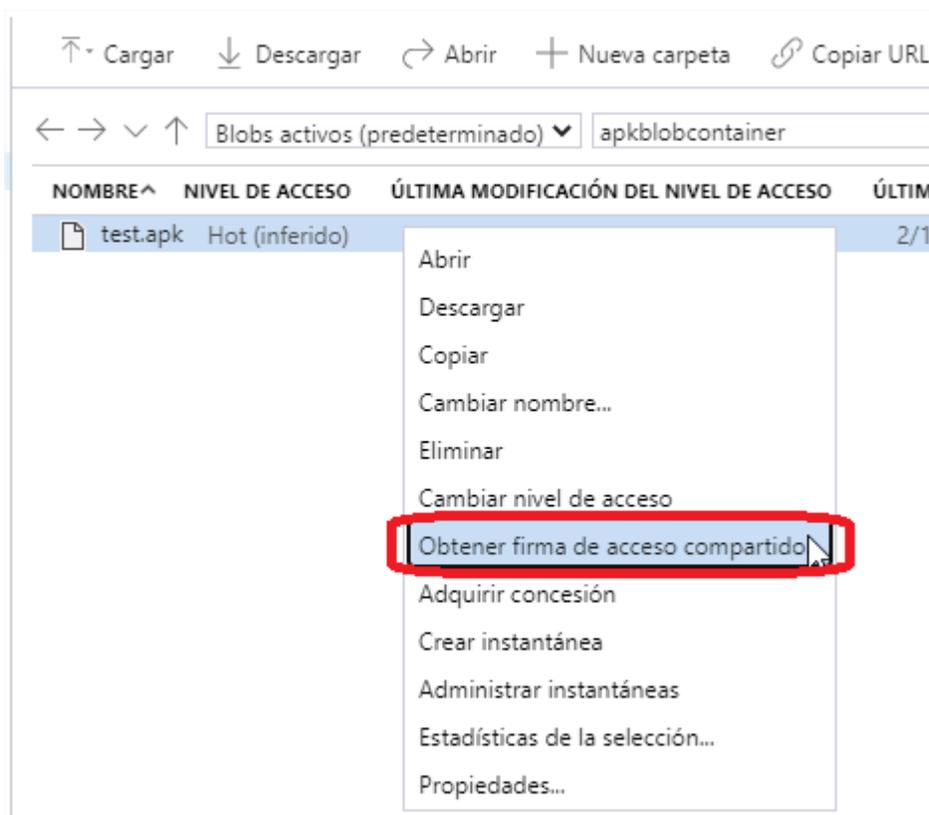
p. Haga clic en "Cargar"



q. Una vez completada la carga del archivo aparecerá en el explorador



r. Haga clic derecho sobre el archivo cargado y luego clic en “Obtener firma de acceso compartido”



- s. Haga clic en “Crear”, teniendo en cuenta la caducidad del enlace, dado que cuando dicho enlace caduque será necesario la creación de un nuevo enlace.

Firma de acceso compartido



Directiva de acceso: (ninguno) ▼

Hora de inicio: 02/12/2020 04:29 p. m. 🗑️

Hora de caducidad: 03/12/2020 04:29 p. m. 🗑️

Zona horaria:
 Local
 UTC

Permisos:
 Leer
 Agregar
 Crear
 Escribir
 Eliminar

Generar URI de firma de acceso compartido de nivel de contenedor



- t. Haga clic en copiar de la sección URI

Firma de acceso compartido

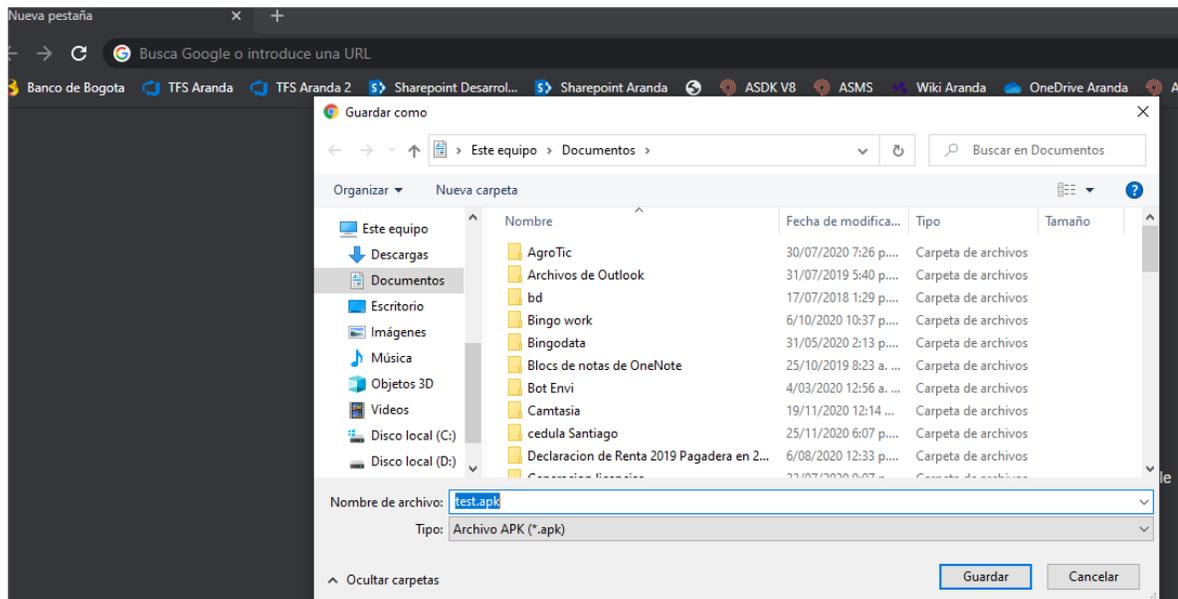
✕

Blob:
test.apk

URI:
<https://storageaccounttest.blob.core.windows.net/apkblobcontainer/test.apk?sp=> Copiar

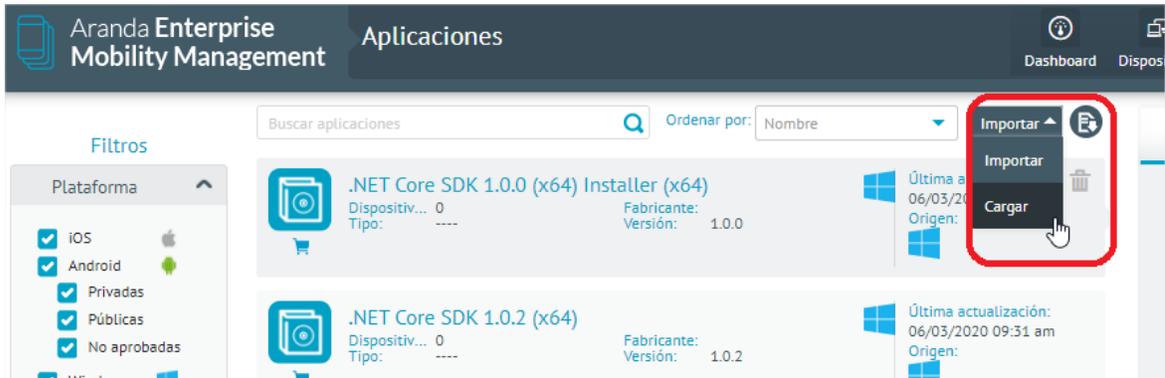
Cadena de consulta:
[?sp=rl&st=2020-12-02T21:29:43Z&se=2020-12-03T21:29:43Z&sv=2019-12-128](https://storageaccounttest.blob.core.windows.net/apkblobcontainer/test.apk?sp=rl&st=2020-12-02T21:29:43Z&se=2020-12-03T21:29:43Z&sv=2019-12-128) Copiar

- u. Abra un navegador y pegue la URI copiada en la parte de direcciones y compruebe que la descarga del archivo se hace correctamente

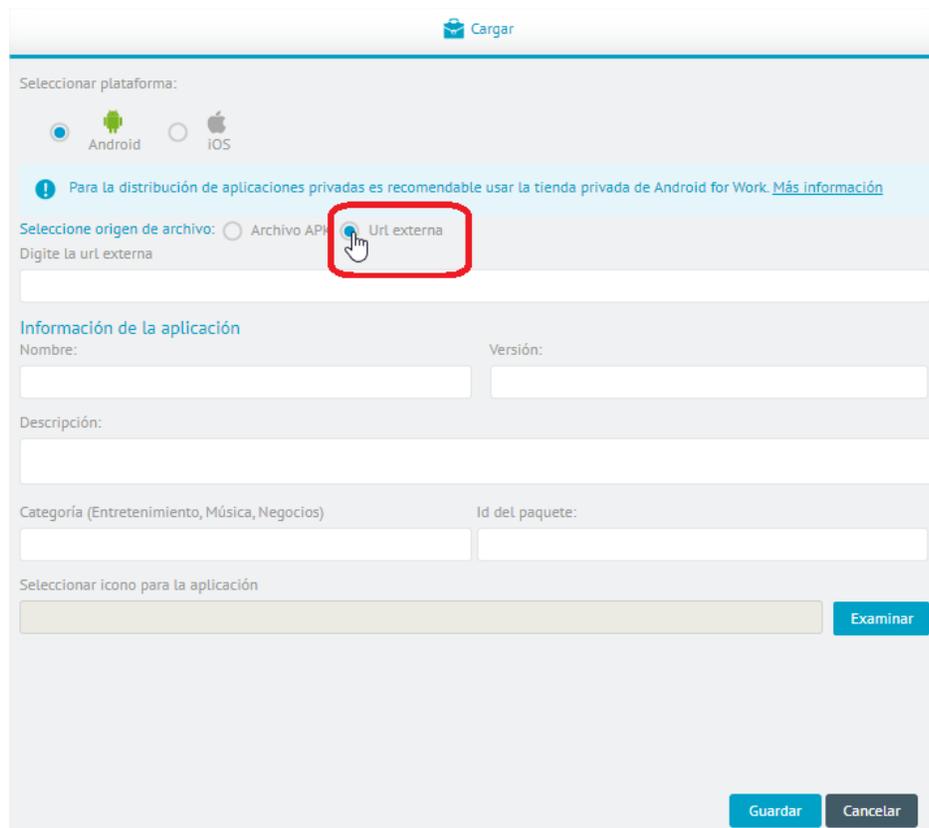


8.2. Utilización De La Uri Creada En Microsoft Azure Como Url Externa De Aplicación En Aemm

- a. Ingrese a la consola AEMM y vaya a la sección aplicaciones, luego haga clic en la opción “Cargar” del menú “Importar”



- b. Una vez en la sección de detalles escoja el origen del archivo como “Url Externa”



- c. Posteriormente pegue la URI obtenida en Azure en la caja de texto para la url externa, luego llene el nombre de la aplicación, la versión, la descripción, categoría, Id del paquete e ícono de la aplicación. Tenga especial cuidado y atención con el **id del paquete** ya que si se digita de manera incorrecta la instalación en el dispositivo no se realizará. Adicionalmente verifique que la URI externa copiada no tenga espacios de más al inicio, en medio o al final.

 Cargar

Seleccionar plataforma:

Android iOS

 Para la distribución de aplicaciones privadas es recomendable usar la tienda privada de Android for Work. [Más información](#)

Seleccione origen de archivo: Archivo APK Url externa

Digite la url externa

`https://storageaccounttest.blob.core.windows.net/apkblobcontainer/test.apk?sp=rl&st=2020-12-02T21:32:51Z&se=2020-12-03T21:32:51`

Información de la aplicación

Nombre: Versión:

Descripción:

Categoría (Entretenimiento, Música, Negocios) Id del paquete:

Seleccionar icono para la aplicación

d. Luego haga clic en “Guardar” para persistir los datos en la consola

Cargar

Seleccionar plataforma:

Android iOS

Para la distribución de aplicaciones privadas es recomendable usar la tienda privada de Android for Work. [Más información](#)

Seleccione origen de archivo: Archivo APK Url externa

Digite la url externa

`https://storageaccounttest.blob.core.windows.net/apkblobcontainer/test.apk?sp=rl&st=2020-12-02T21:32:51Z&se=2020-12-03T21:32:51`

Información de la aplicación

Nombre: Versión:

Descripción:

Categoría (Entretenimiento, Música, Negocios) Id del paquete:

Seleccionar icono para la aplicación

Aranda Enterprise Mobility Management Aplicaciones

Dashboard Dispositivos Aplicaciones Políticas Reglas Reportes Documentos Configuración Ricardo Chacangana

Filtros

Plataforma: iOS Android Privadas Públicas No aprobadas Windows

Origen: Corporativo Tienda

Nombre	Fabricante	Versión	Última actualización
.NET Core SDK 1.0.0 (x64) Installer (x64)	---	1.0.0	06/03/2020 09:31 am
.NET Core SDK 1.0.2 (x64)	---	1.0.2	06/03/2020 09:31 am
.NET Core SDK 1.0.2 (x64)	4.0.37725	---	06/03/2020 09:31 am
.NET Core SDK 1.0.3 (x64)	4.0.54117	---	06/03/2020 09:31 am
.NET Core SDK 1.0.3 (x64)	---	1.0.3	06/03/2020 09:31 am
.NET Core SDK 1.1.0 (x64)	---	1.1.0	06/03/2020 09:31 am

Las aplicaciones seleccionadas se importaron con éxito

Detalles

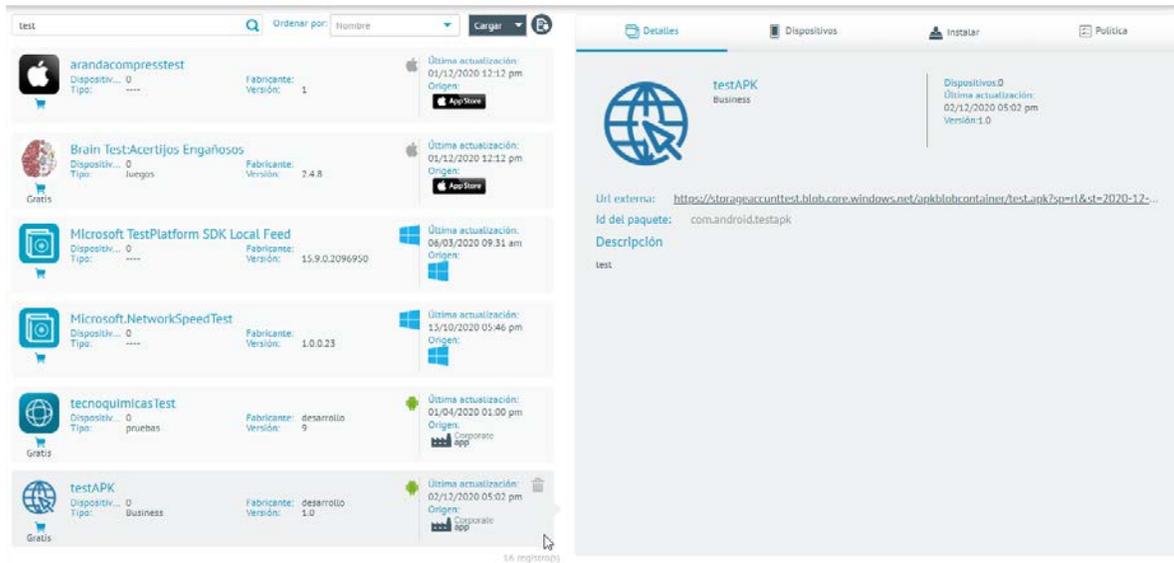
Dispositivos 0 Último actualización: 06/03/2020 09:31 am Versión: 1.0.0

Instalar Política Ejecutables

Id del paquete: 000085c9613813a2590a44e2907fabd8766c0000f1f

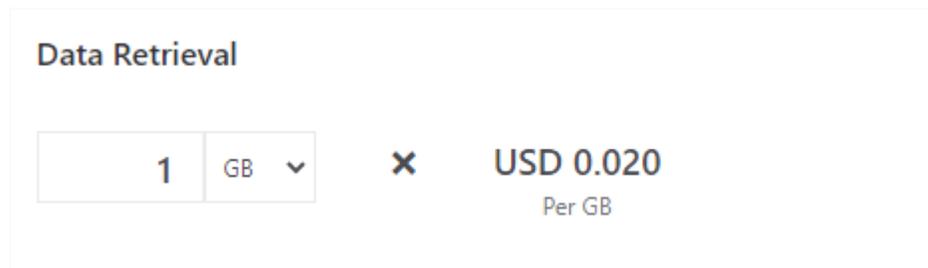
Descripción

- e. Luego de hecho este proceso se puede encontrar la aplicación creada e iniciar su instalación en la misma sección de aplicaciones o ser agregada como aplicación requerida en una política.

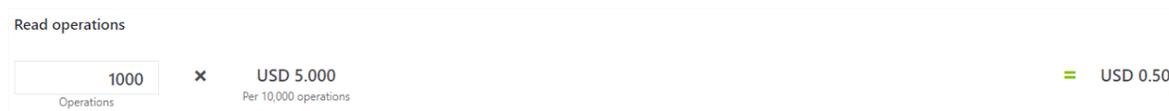


8.3. Costos

Tomando como referencia la calculadora de precios de Microsoft Azure (<https://azure.microsoft.com/es-mx/pricing/calculator>) los costos aproximados por cada 1 GB de descargas acumuladas sobre el (los) archivo (s) es de US \$ 0.02



Adicional a lo anterior se calcula el costo aproximado por cada 1000 operaciones de lectura a US \$ 0.5



9. POLÍTICAS

Las políticas son parámetros que se asignan a los dispositivos móviles para su funcionamiento.

9.1. Cumplimiento en dispositivos

Si al dispositivo se le asigna una política y este cumple con la condición, se visualiza un Check de color verde. Esto se puede evidenciar en diferentes secciones de la consola:

- La pestaña de dispositivo

- Listado de dispositivos

- Hoja de vida del dispositivo

Listado y pre visualización

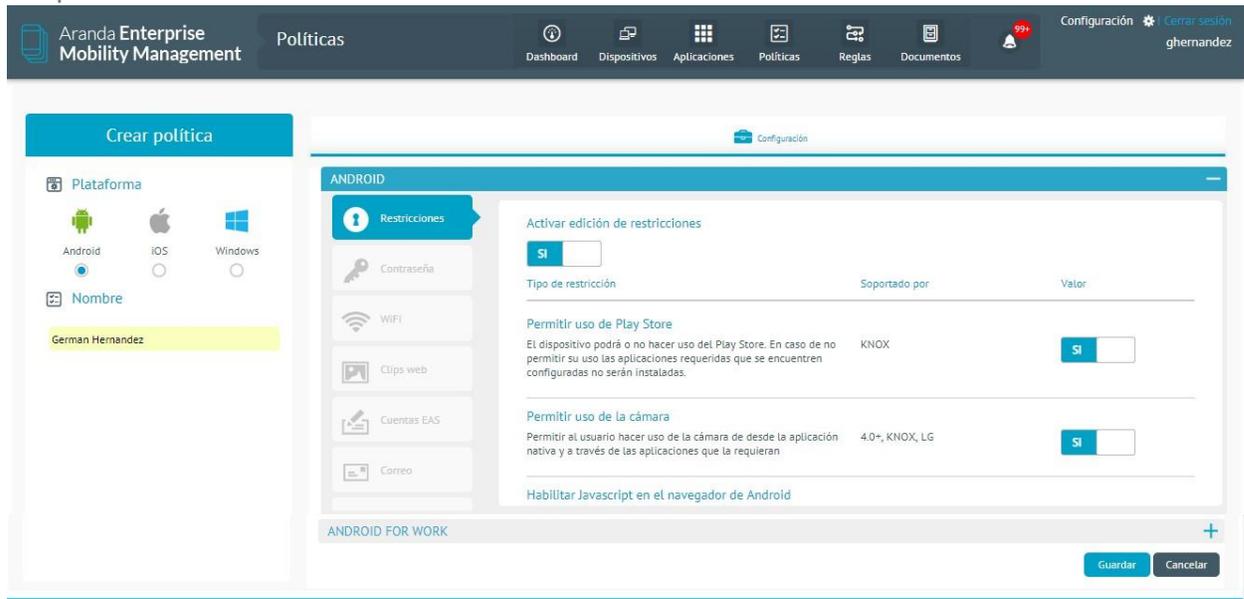
- Se visualiza el filtro para la información, esto se puede realizar por plataforma y/o estado.
- Es el resumen de política, donde se almacena el nombre, fecha de modificación y fecha de aprobación.
- Es la tarjeta donde se consigna fecha de creación, última modificación, última aprobación, dispositivos asociados y creado por.
- Son las gráficas que registran la cantidad de dispositivos asociados y su cumplimiento.

- Es el resumen de configuración por tipo de política.

9.2. Configuración de políticas

9.2.1. Restricciones Android

Son los parámetros que se restringen a dispositivos móviles Android, luego de aplicar una política.



Permitir uso de la cámara: Si esta opción no está seleccionada, el dispositivo no puede hacer uso de la cámara ni a través de aplicaciones que la requieran (Solo aplica para Android versión superior a 4.0 o Knox)

Permitir pop-ups en el navegador de Android: Si se habilita esta política el navegador del dispositivo no permite pop up. (Solo aplica para Android Knox).

Permitir backup en servicios de la nube: Si este parámetro está activo el dispositivo. (Solo aplica para Android Knox).

Cifrar dispositivo Android: Esta opción por defecto viene deshabilitada, pero si se decide aplicar al dispositivo este permite fusionar todos los datos con una contraseña o clave. (Solo aplica para Android Knox)

Permitir roaming: Si se habilita esta política el dispositivo no permite el servicio de roaming. (Solo aplica para Android Knox)

Permitir tethering USB: Si se aplica esta política el dispositivo no permite compartir la conexión con cualquier otro ordenador (Solo aplica para Android Knox).

Permitir Reproductor de Multimedia USB (Kies): Si esta opción no está seleccionada, el dispositivo Android no permite sincronizarse con Kies de Samsung (Solo aplica para Android Knox).

Permitir Bluetooth: Si este parámetro está activo no permite la conexión por medio de Bluetooth en el dispositivo móvil. (Solo aplica para Android Knox)

Habilitar Javascript en el navegador de Android: Si se habilita esta política el navegador de Android no habilita el JavaScript. (Solo aplica para Android Knox).

Permitir cookies en el navegador de Android: Este parámetro se activa y el móvil no habilita las cookies para el navegador. (Solo aplica para Android Knox)

Habilitar WiFi en un dispositivo Android: Esta restricción si se aplica al dispositivo Android no permite que este se conecte a la Wifi. (Solo aplica para Android Knox)

Permitir marcación por voz: Si este parámetro está activo no es posible realizar marcación por voz a través del dispositivo. (Solo aplica para Android Knox)

Permitir roaming de datos: Si se habilita esta política el dispositivo no permite el servicio de roaming de datos. (Solo aplica para Android Knox).

Permitir depuración USB: Si esta opción no está seleccionada no es posible realizar depuración USB con el dispositivo móvil (Solo aplica para Android Knox).

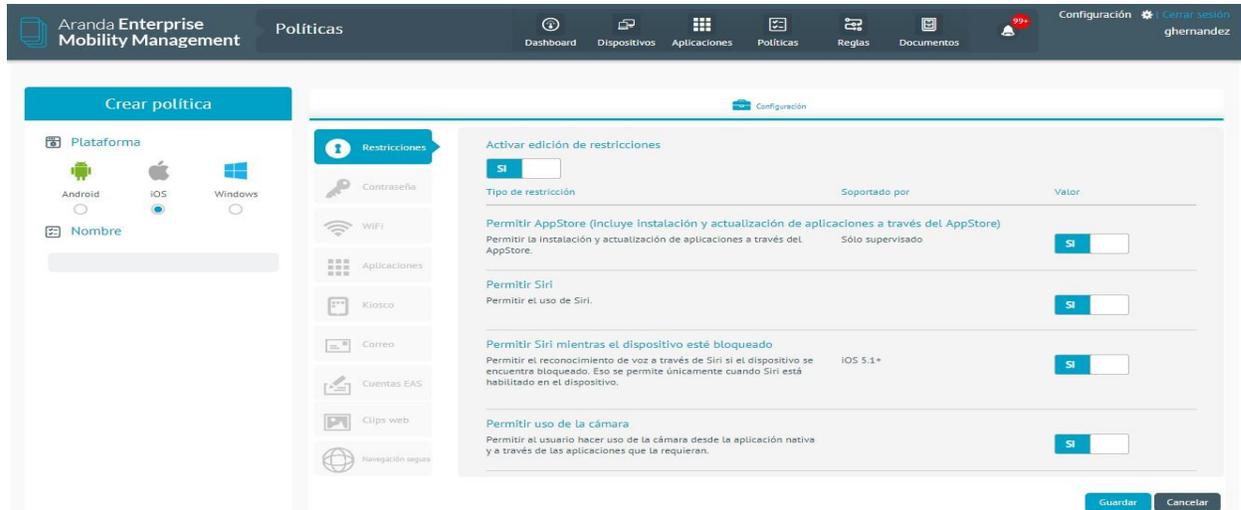
Permitir uso de SMS: Si esta política se aplica no es posible enviar o recibir SMS al móvil. (Solo aplica para Android Knox).

Permitir manipulación del GPS: Si este parámetro está activo no se tiene acceso al GPS (Solo aplica para Android Knox)

Permitir actualización de sistema operativo: Si esta opción esta inactiva no se permitirá descargar ni instalar actualizaciones de sistema operativo, tanto manualmente como automáticamente (Solo aplica para vinculaciones en AFW con agente samsung Knox)

9.2.2. Restricciones en iOS

Son los parámetros que se restringen a dispositivos móviles iOS, luego de aplicar una política.



The screenshot shows the 'Aranda Enterprise Mobility Management' interface. The main area is titled 'Configuración' and displays the 'Restricciones' (Restrictions) settings for iOS. The settings are as follows:

Tipo de restricción	Soportado por	Valor
Permitir AppStore (incluye instalación y actualización de aplicaciones a través del AppStore). Permitir la instalación y actualización de aplicaciones a través del AppStore.	Sólo supervisado	<input type="checkbox"/>
Permitir Siri Permitir el uso de Siri.		<input type="checkbox"/>
Permitir Siri mientras el dispositivo esté bloqueado Permitir el reconocimiento de voz a través de Siri si el dispositivo se encuentra bloqueado. Eso se permite únicamente cuando Siri está habilitado en el dispositivo.	iOS 5.1+	<input type="checkbox"/>
Permitir uso de la cámara Permitir al usuario hacer uso de la cámara desde la aplicación nativa y a través de las aplicaciones que la requieran.		<input type="checkbox"/>

Permitir App Store (incluye instalación y actualización de aplicaciones a través del App Store): Si se aplica esta configuración el dispositivo iOS no tendrá acceso al App Store.

Permitir Siri mientras el dispositivo esté bloqueado: Esta política no activa el reconocimiento de voz a través de SIRI si el dispositivo se encuentra bloqueado (Solo aplica para dispositivos iOS versión superior a 5.1).

Permitir informes automáticos de diagnóstico: Este parámetro activo deshabilita la opción de enviar informes automáticos de diagnóstico (Solo aplica para dispositivos iOS versión superior a 6.0)

Permitir Game Center: Si esta opción no es seleccionada el dispositivo no tiene acceso al Game Center. (Solo aplica para dispositivos iOS versión superior a 6.0)

Permitir uso del iTunes Store: Esta política no permite el acceso a la tienda en línea de contenido digital a través de iTunes Store.

Permitir Safari: Este parámetro activo no permite el acceso al navegador Safari.

Permitir backup en servicios de la nube: Si se aplica esta configuración no se le permite al dispositivo realizar backup en la nube de servicios de Apple (Solo aplica para dispositivos iOS versión superior a 5.0)

Permitir Photo Stream: Este parámetro no permite la sincronización de fotos a través del PhotoStream (Solo aplica para dispositivos iOS versión superior a 5.0)

Permitir Shared Photo Stream: Si se aplica esta política el dispositivo no puede compartir las fotos que tienen sincronizada. El shared Photo Stream se deshabilita (Solo aplica para dispositivos iOS versión superior a 6.0)

Permitir cookies en Safari: Esta política puede configurar las Cookies de safari para que se permitan nunca, siempre o solo de los sitios visitados.

Permitir Siri: Esta política no activa el reconocimiento de voz a través de SIRI.

Permitir uso de la cámara: Si esta opción no está seleccionada, el dispositivo no puede hacer uso de la cámara ni a través de aplicaciones que la requieran.

Permitir contenido explícito: Este parámetro no permite el acceso a contenido explícito.

Permitir capturas de pantalla: Cuando se aplica esta política en el dispositivo no es posible realizar capturas de pantalla en el dispositivo móvil.

Forzar ingreso de contraseña de iTunes para cada transacción: Si este parámetro está activo, siempre que se realice alguna transacción con el iTunes solicitará la clave de acceso (Solo aplica para dispositivos iOS versión superior a 5.0)

Advertir al usuario sobre certificados HTTPS no confiables en vez de rechazarlos automáticamente: Si esta política se aplica al móvil siempre se le advierte al usuario cuando el certificado HTTPS no es confiable (Solo aplica para dispositivos iOS versión superior a 5.0)

Permitir sincronización de documentos en iCloud: Esta política no permite el almacenamiento en cloud computing de Apple (Solo aplica para dispositivos iOS versión superior a 5.0).

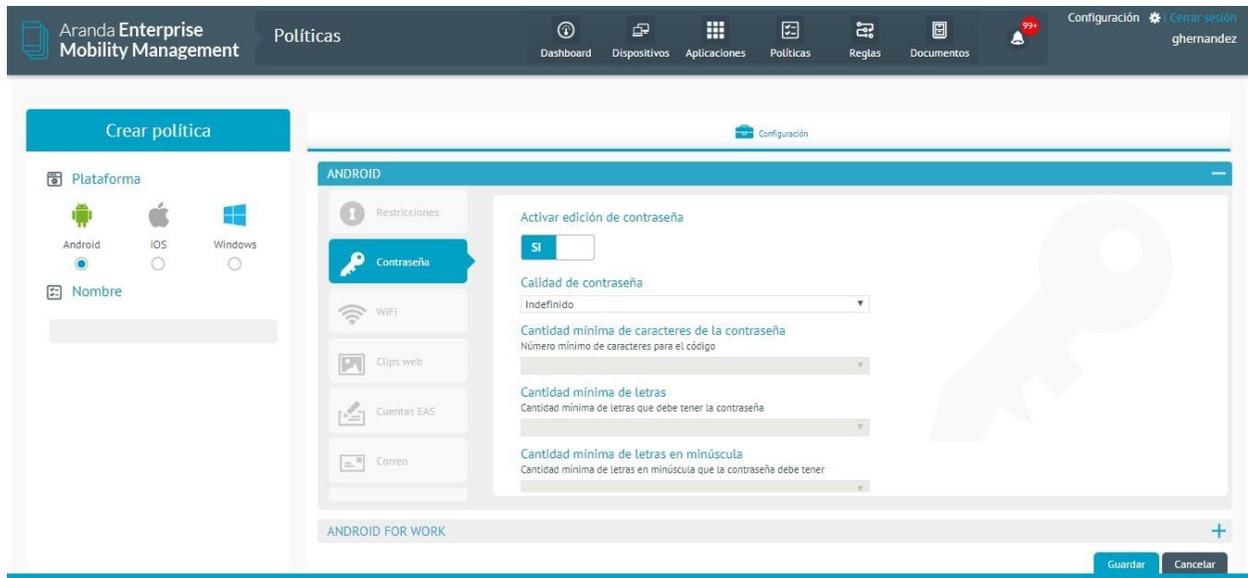
Permitir BookStore: Si se aplica esta política el dispositivo no tienen acceso al BookStore de Apple. (Solo aplica para dispositivos iOS versión superior a 6.0).

Permitir Javascript en Safari: Este parámetro no permite el uso de Javascript en safari.

9.2.3. Contraseña

9.2.3.1. Android

Son los parámetros que se aplican a un dispositivo Android para configurar en el móvil.



Calidad de contraseña: Existen 5 tipos de configuración de contraseña, estos son:

- **Indefinido:** Es necesario ingresar una contraseña con mínimo 4 caracteres
- **Alfabética:** La contraseña debe contener por lo menos 4 caracteres alfabéticos.
- **Alfanumérica:** La contraseña debe contener por lo menos 4 caracteres alfanuméricos.
- **Compleja:** La contraseña debe contener por lo menos 4 caracteres de los cuales mínimo uno es letra, una letra en minúscula, una letra en mayúscula, un carácter especial y un número.
- **Cualquiera:** La contraseña puede ser un patrón, un pin o una contraseña.

Longitud mínima del código: Es la cantidad de caracteres que mínimo debe tener la contraseña que va desde 4 hasta 16.

Cantidad mínima de letras: Es la cantidad de letras que mínimo debe tener la contraseña que va desde 1 hasta 16.

Cantidad mínima de letras en minúscula: Es la cantidad de letras minúsculas que mínimo debe tener la contraseña que va desde 1 hasta 16.

Cantidad mínima de letras en mayúscula: Es la cantidad de letras mayúsculas que mínimo debe tener la contraseña que va desde 1 hasta 16.

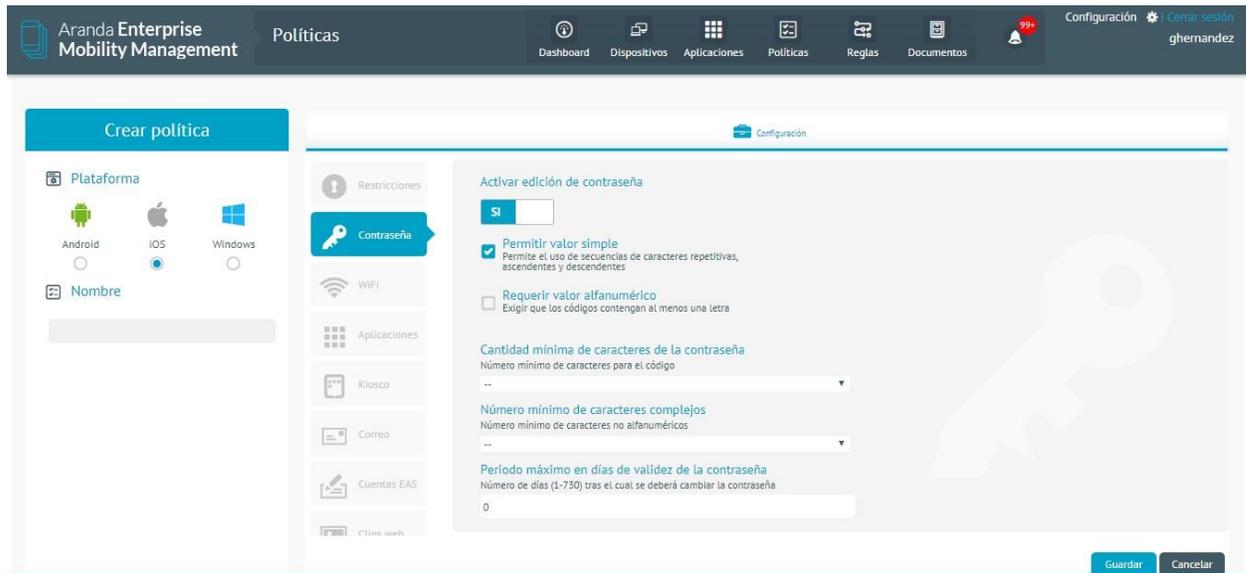
Cantidad mínima de caracteres que no sean letras: Es la cantidad de caracteres especiales que mínimo debe tener la contraseña que va desde 1 hasta 16.

Cantidad mínima de números: Es la cantidad de números que mínimo debe tener la contraseña que va desde 1 hasta 16.

Cantidad mínima de símbolos: Es la cantidad de símbolos que mínimo debe tener la contraseña que va desde 1 hasta 16.

9.2.3.2. iOS

Son los parámetros que se aplican a un dispositivo iOS para configurar en el móvil



Permitir valor simple: Permite el uso de secuencias de caracteres repetitivas, ascendentes y descendentes.

Requerir valor alfanumérico: Exige que los códigos contengan al menos una letra.
Longitud mínima del código: Es la cantidad mínima de caracteres que debe contener la contraseña que va desde 1 hasta 16.

Número mínimo de caracteres complejos: Es la cantidad mínima de caracteres complejos que debe contener la contraseña que va desde 1 hasta 4.

Periodo máximo de validez del código: Número de días (1-730) tras el cual se deberá cambiar la contraseña.

Bloqueo automático máximo: El dispositivo se bloquea tras el tiempo establecido se encuentra entre 1 a 15 minutos.

Historial de contraseñas: Número de contraseñas únicas (1-50) antes de poder repetir las.

Periodo de gracia máximo para el bloqueo de dispositivo: Cantidad máxima de tiempo que el dispositivo puede permanecer bloqueado sin solicitar el código de

desbloqueo. Las opciones son: De inmediato, 1 minuto, 5 minutos, 15 minutos, 1 hora o 4 horas.

Número máximo de intentos fallidos: Número máximo de intentos permitidos de introducir la contraseña antes de que se borren todos los datos del dispositivo o este se bloquee hasta que se conecte con el iTunes designado. Se encuentra entre 2 a 11.

9.2.4. Wifi

Es la política que configura la red WIFI en el dispositivo móvil.

9.2.4.1. Android

The screenshot displays the Aranda Enterprise Mobility Management interface. The top navigation bar includes 'Aranda Enterprise Mobility Management', 'Políticas', and a menu with 'Dashboard', 'Dispositivos', 'Aplicaciones', 'Políticas', 'Reglas', and 'Documentos'. A user profile 'ghernandez' is visible in the top right. The main content area is titled 'Crear política' and shows a sidebar with 'Plataforma' (Android, iOS, Windows) and 'Nombre'. The main panel is for 'Configuración' and is divided into 'ANDROID' and 'ANDROID FOR WORK' sections. The 'ANDROID' section includes a 'Restricciones' tab and a table of settings:

Tipo de restricción	Soportado por	Valor
Activar edición de restricciones		SI <input type="checkbox"/>
Permitir uso de Play Store	KNOX	SI <input type="checkbox"/>
Permitir uso de la cámara	4.0+, KNOX, LG	SI <input type="checkbox"/>
Habilitar Javascript en el navegador de Android		

Identificador de conjunto de servicios (SSID): Es el nombre de la red inalámbrica a la que se conectará.

Tipo de seguridad: Cifrado de la red inalámbrica que se utilizará para la conexión. Existe WEP, WPA/WPA2.

Contraseña: Es la contraseña para la autenticación en la red inalámbrica.

9.2.4.2. iOS

Aranda Enterprise Mobility Management | Políticas | Dashboard | Dispositivos | Aplicaciones | Políticas | Reglas | Documentos | Configuración | Cerrar sesión gherandez

Crear política

Plataforma: Android, iOS, Windows

Nombre

Restricciones

Contraseña

WIFI

Aplicaciones

Kiosco

Correo

Cuentas EAS

Flits web

Configuración

Activar edición de contraseña: SI

Permitir valor simple: Permite el uso de secuencias de caracteres repetitivos, ascendentes y descendentes

Requerir valor alfanumérico: Exigir que los códigos contengan al menos una letra

Cantidad mínima de caracteres de la contraseña: Número mínimo de caracteres para el código

Número mínimo de caracteres complejos: Número mínimo de caracteres no alfanuméricos

Período máximo en días de validez de la contraseña: Número de días (1-730) tras el cual se deberá cambiar la contraseña

Guardar | Cancelar

Identificador de conjunto de servicios (SSID): Nombre de la red inalámbrica a la que se conectará.

Conexión automática: Se selecciona si desea conectarse automáticamente a la red de destino.

Red oculta: Se selecciona si la red de destino está abierta o no.

Tipo de seguridad: Cifrado de la red inalámbrica que se utilizará para la conexión. Existe WEP o WPA/WPA2.

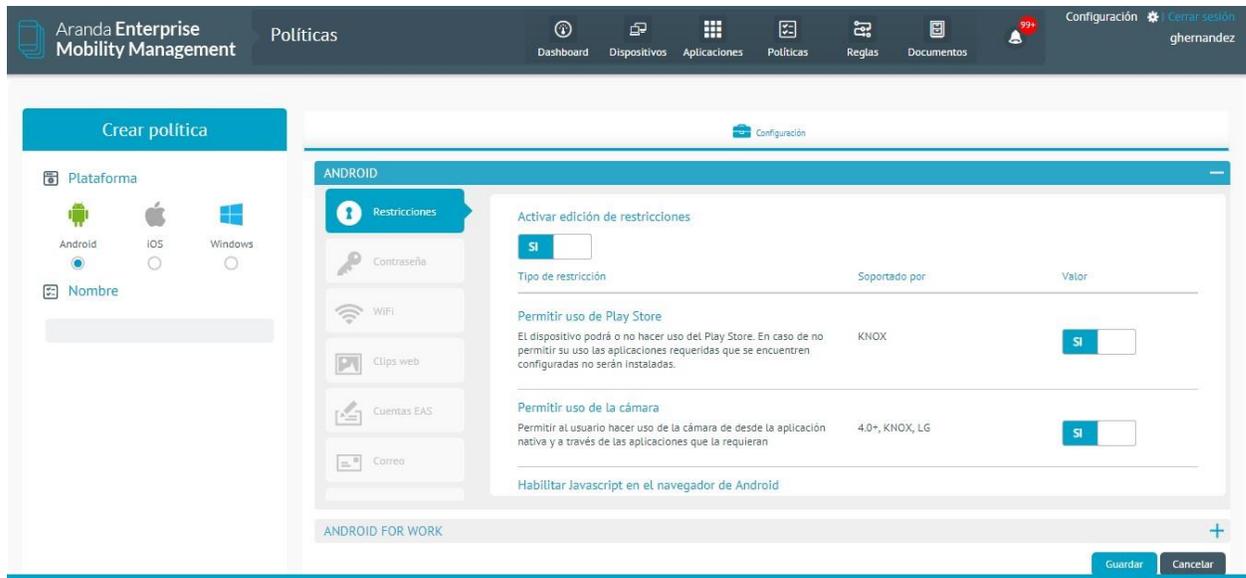
Contraseña: La contraseña para la autenticación en la red inalámbrica.

Proxy: Se seleccionada si el ajuste para la red inalámbrica del proxy es automático o manual.

9.2.5. Web clips

Esta política crea un acceso directo en el dispositivo móvil, el cual dirige a una URL.

9.2.5.1. Android

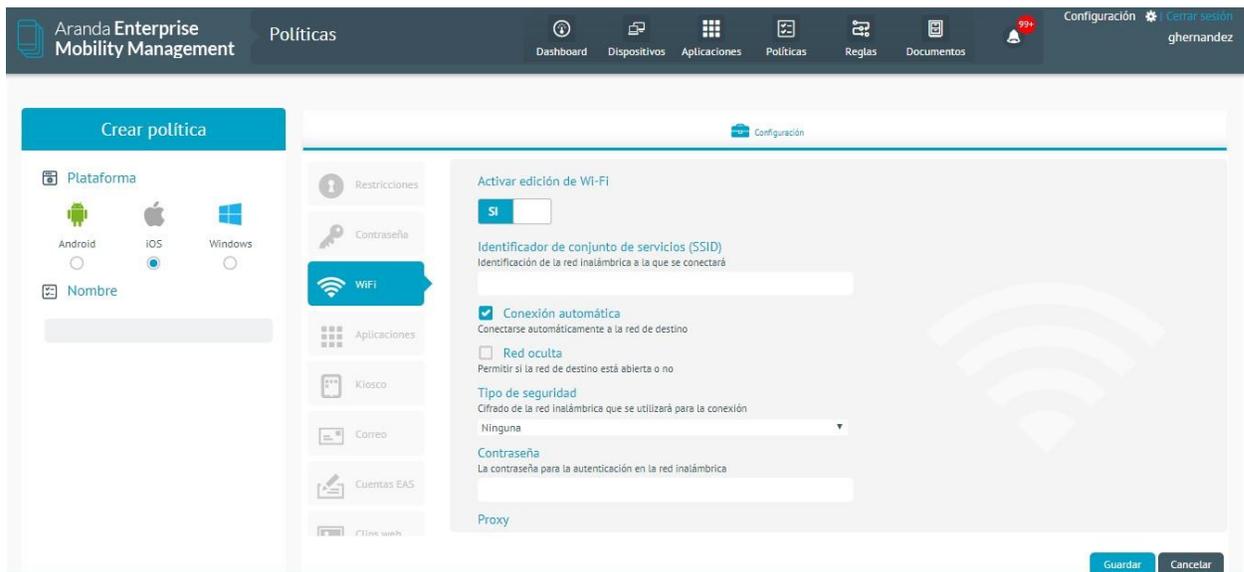


Etiqueta: Es el nombre que se asigna al clip web

URL: Dirección que dirige el Web Clip

Icono: Imagen que se va visualizar en el WebClip. Esta imagen debe tener un tamaño máximo de 200 pixeles de alto y 200 pixeles de ancho. Es posible adicionar más de un web clip con la opción "Crear un nuevo web clip".

9.2.5.2. iOS



Etiqueta: Es el nombre que se asigna al clip web.

URL: Dirección que dirige el Web Clip

Eliminable: Permitir eliminación del Clip Web.

Icono: Imagen que se va a visualizar en el Web Clip. Esta imagen debe tener un tamaño máximo de 200 píxeles de alto y 200 píxeles de ancho.

Icono pre compuesto: El icono se mostrará sin efectos visuales añadidos.

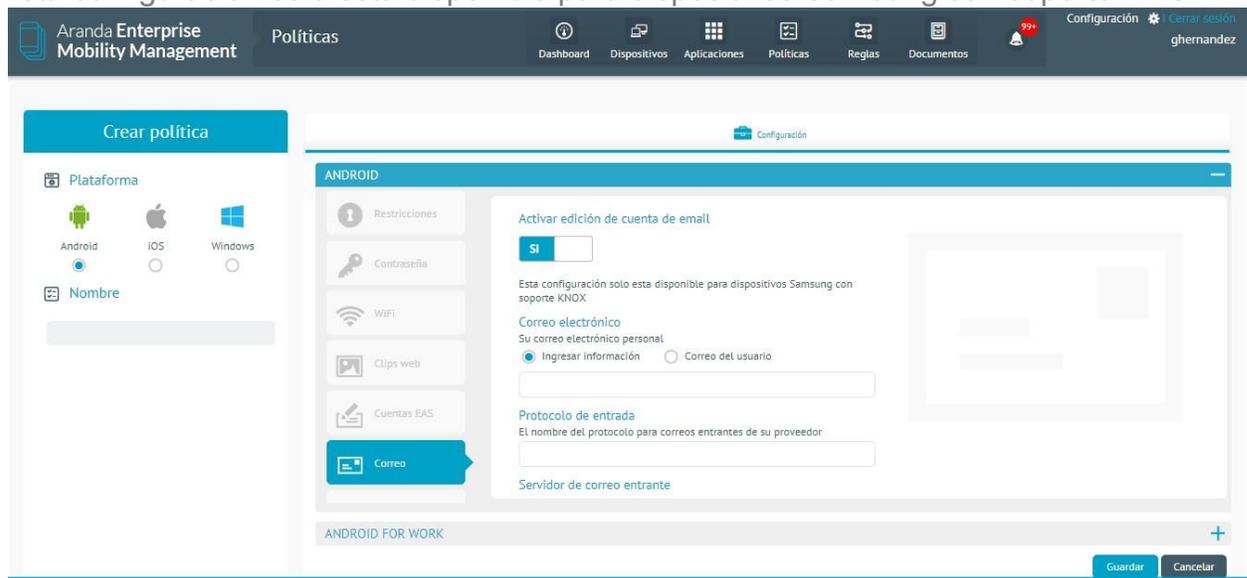
Pantalla completa: Presentar el clip web como una aplicación de pantalla completa. Es posible añadir más de un web clip con la opción “Crear un nuevo web clip”.

9.2.6. Email

Es la configuración de una cuenta de correo que se aplica a un dispositivo móvil.

9.2.6.1. Android

Esta configuración solo está disponible para dispositivos Samsung con soporte KNOX.



Correo electrónico: Es el correo electrónico que se va a configurar. El administrador tiene la opción de ingresarlo o el usuario del móvil.

Protocolo de entrada: El nombre del protocolo para correos entrantes de su proveedor.

Servidor de correo entrante: La dirección del servidor de correo entrante.

Puerto del servidor de correo entrante: El puerto utilizado por el servidor de correo entrante.

Login del servidor de correo entrante: Login utilizado en el servidor de correo entrante. El administrador tiene la posibilidad de ingresar el usuario o solicitarle al usuario el ingreso del Nombre de usuario o Correo.

Contraseña del servidor de correo entrante: Contraseña utilizada en el servidor de correo entrante. Este campo solo se habilita si se ingresa la información de la casilla anterior.

Protocolo de salida: El nombre del protocolo para correos salientes de su Proveedor.

Servidor de correo saliente: La dirección del servidor de correo saliente

Puerto del servidor de correo saliente: El puerto utilizado por el servidor de correo saliente

Login del servidor de correo saliente: Login utilizado en el servidor de correo saliente. El administrador tiene la posibilidad de ingresar al usuario o solicitarle al mismo el ingreso de Nombre de usuario o correo.

Contraseña del servidor de correo saliente: Contraseña utilizada en el servidor de correo saliente. Este campo solo se habilita si se ingresa la información de la casilla anterior.

9.2.6.2. iOS

Aranda Enterprise Mobility Management Políticas

Dashboard Dispositivos Aplicaciones Políticas Reglas Documentos Configuración Cerrar sesión ghernandez

Crear política

Plataforma

Android iOS Windows

Nombre

Restricciones

Contraseña

WIFI

Aplicaciones

Kiosco

Correo

Cuentas EAS

Flows work

Configuración

Activar edición de cuenta de email

SI

Descripción de la cuenta

Nombre visible de la cuenta (ej. 'Cuenta de la empresa')

Tipo

Protocolo de acceso a la cuenta

POP

Nombre visible de usuario

El nombre del usuario (ej. 'Alvaro Gómez')

Ingresar información Nombre del usuario Correo del usuario

Dirección de correo electrónico

La dirección de la cuenta (ej. 'agamez@empresa.com')

Ingresar información Correo del usuario

Guardar Cancelar

Descripción de la cuenta: Nombre visible de la cuenta.

Tipo: Protocolo de acceso a la cuenta. Existen dos protocolos:

- **Pop:** Se utiliza en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto.
- **Imap:** Con este protocolo se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.

Nombre visible de usuario: Es el nombre del usuario. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.

Dirección de correo electrónico: La dirección de la cuenta. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Correo.

Servidor (Correo entrante): Url del servidor o IP.

Puerto (Correo entrante): Número del puerto para conexión.

Nombre de usuario (Correo entrante): El nombre usado para conectarse al servidor de correo entrante. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.

Tipo de autenticación (correo entrante): El método de autenticación del servidor de correo entrante.

Contraseña (Correo entrante): La contraseña del servidor de correo entrante.

Usar SSL (correo entrante): Recuperar correo entrante a través de SSL.

Servidor (Correo saliente): Url del servidor o IP.

Puerto (Correo saliente): Número del puerto para conexión.

Nombre de usuario (Correo saliente): El nombre usado para conectarse al servidor de correo saliente. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.

Tipo de autenticación (correo saliente): El método de autenticación del servidor de correo saliente.

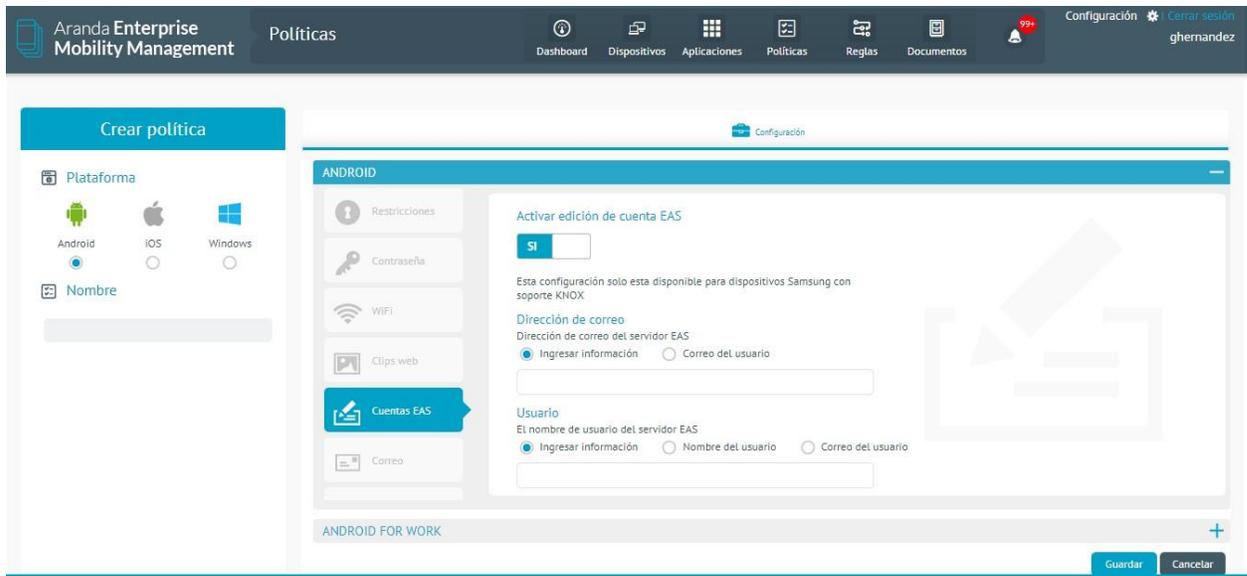
Contraseña (Correo saliente): La contraseña del servidor de correo saliente.

9.2.7. Exchange Active Sync

Es la configuración de una cuenta de correo que se aplica a un dispositivo móvil.

9.2.7.1. Android

Esta configuración solo está disponible para dispositivos Samsung con soporte KNOX



Correo electrónico: Su correo electrónico personal. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Correo.

Protocolo de entrada: El nombre del protocolo para correos entrantes de su proveedor.

Servidor de correo entrante: La dirección del servidor de correo entrante

Puerto del servidor de correo entrante: El puerto utilizado por el servidor de correo entrante.

Login del servidor de correo entrante: Login utilizado en el servidor de correo entrante. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.

Contraseña del servidor de correo entrante: Contraseña utilizada en el servidor de correo entrante.

Protocolo de salida: El nombre del protocolo para correos salientes de su proveedor.

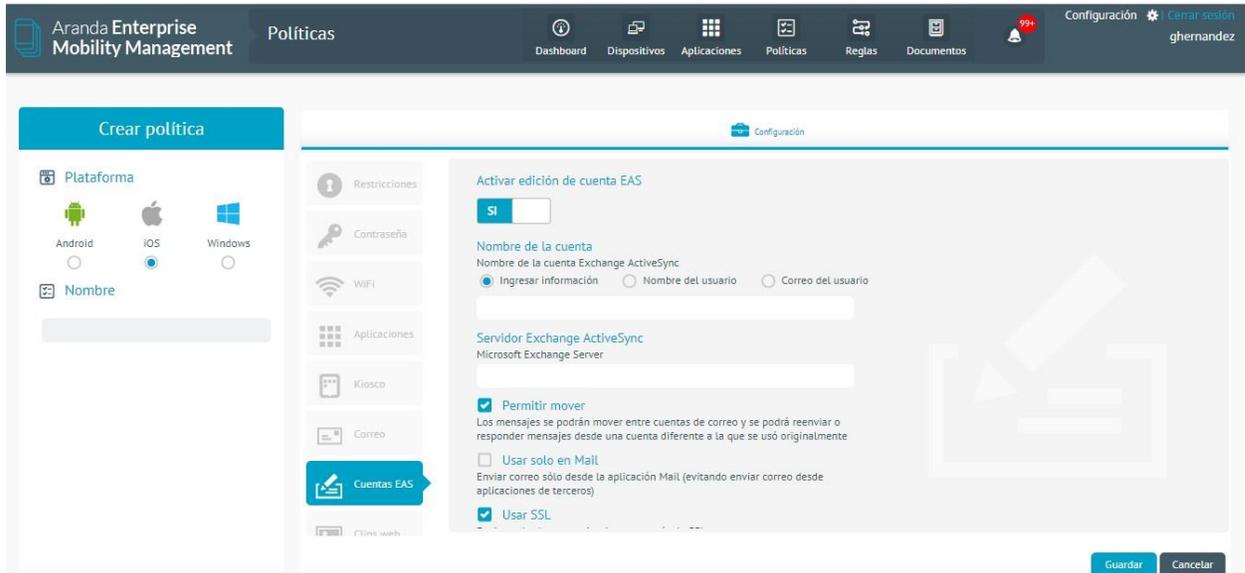
Servidor de correo saliente: La dirección del servidor de correo saliente.

Puerto del servidor de correo saliente: El puerto utilizado por el servidor de correo saliente.

Login del servidor de correo saliente: Login utilizado en el servidor de correo saliente. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.

Contraseña del servidor de correo saliente: Contraseña utilizada en el servidor de correo saliente.

9.2.7.2. iOS



Nombre de la cuenta Exchange ActiveSync: Nombre de la cuenta Exchange ActiveSync. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.

Microsoft Exchange Server: Microsoft Exchange Server.

Permitir mover: Los mensajes se podrán mover entre cuentas de correo y se podrá reenviar o responder mensajes desde una cuenta diferente a la que se usó originalmente.

Usar solo en Mail: Enviar correo sólo desde la aplicación Mail (evitando enviar correo desde aplicaciones de terceros).

Usar SSL: Enviar todas las comunicaciones a través de SSL.

Dominio: Dominio de la cuenta (si deja este campo vacío el dispositivo se lo solicitará al usuario). El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Correo.

Usuario: Usuario de la cuenta (si deja este campo vacío el dispositivo se lo solicitará al usuario). El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.

Dirección de correo electrónico: La dirección de la cuenta. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Correo.

Contraseña: La contraseña de la cuenta.

Días pasados de correo incluidos en la sincronización: El número de días pasados de correo que se incluirán en la sincronización. Tiene la opción de seleccionar: Sin límite, un día, tres días, una semana, dos semanas o un mes.

9.2.8. Aplicaciones

Es una política que se aplica a los dispositivos móviles, para auditar las aplicaciones que tienen instaladas. Existen tres tipos de listas que clasifican el estado que deben tener las aplicaciones.

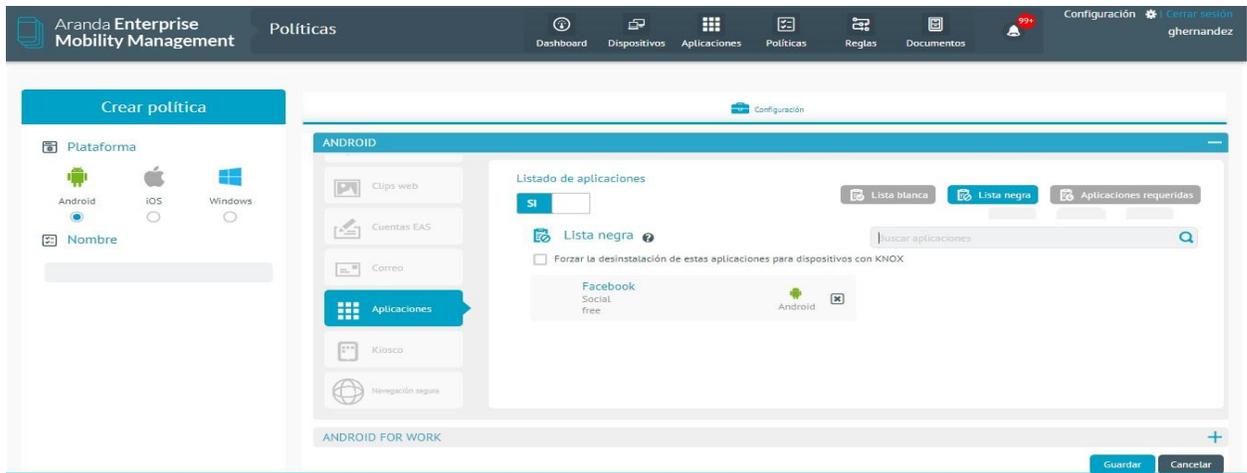
9.2.8.1. Lista Blanca

Listado de aplicaciones que tendrá permitido instalar el dispositivo asociado a esta política. Para dispositivos KNOX es posible desinstalar las aplicaciones que no se encuentran en la lista.

The screenshot displays the 'Aranda Enterprise Mobility Management' interface. The top navigation bar includes 'Políticas', 'Dashboard', 'Dispositivos', 'Aplicaciones', 'Políticas', 'Reglas', 'Documentos', 'Configuración', and 'Cerrar sesión ghernandez'. The main content area is titled 'Crear política' and shows a sidebar with options for 'Plataforma' (Android, iOS, Windows), 'Nombre', and 'Aplicaciones'. The 'Aplicaciones' section is active, showing a list of application categories: 'Clips web', 'Cuentas EAS', 'Correo', 'Aplicaciones', 'Kiosco', and 'Navegación segura'. The 'Aplicaciones' category is selected, displaying the 'Listado de aplicaciones' for 'ANDROID'. The interface includes a search bar, a 'Lista blanca' button, and a checkbox for 'Forzar la desinstalación de aplicaciones que no se encuentran en la lista para dispositivos con KNOX'. The message 'No se han seleccionado aplicaciones a esta lista' is displayed. The bottom of the interface has 'Guardar' and 'Cancelar' buttons.

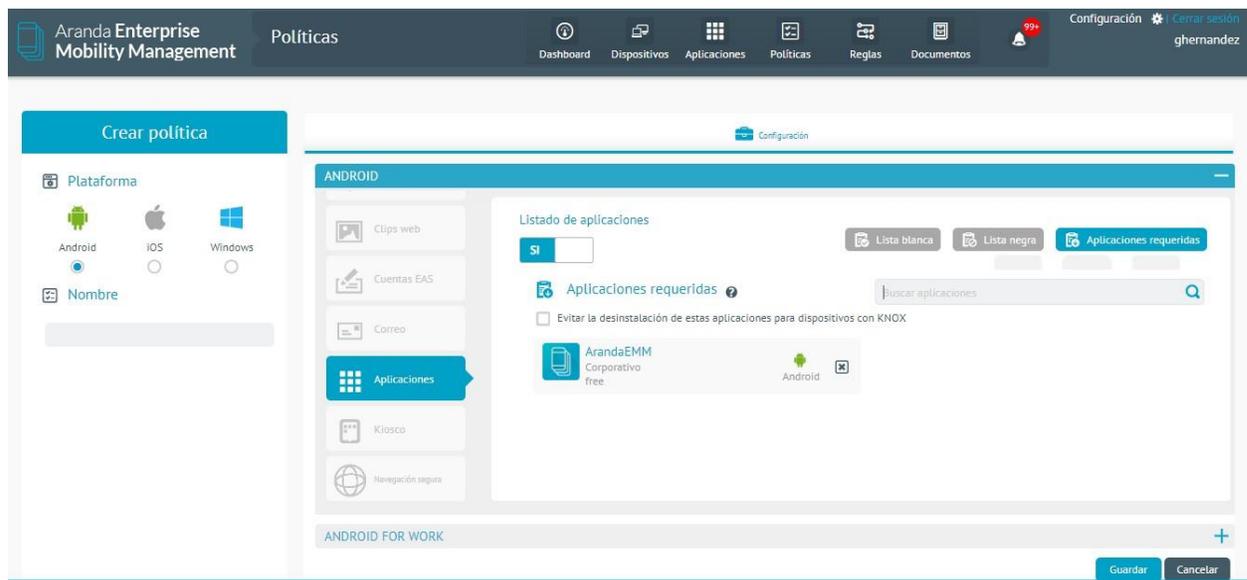
9.2.8.2. Lista Negra

Listado de aplicaciones que tendrá prohibido instalar en los dispositivos asociados a esta política. Para dispositivos Knox de Android se puede forzar la desinstalación de estas aplicaciones.



9.2.8.3. Aplicaciones requeridas

Listado de aplicaciones que deben tener instaladas obligatoriamente el dispositivo asociada a esta política. Para dispositivos Knox de Android se tiene la posibilidad de evitar la desinstalación de estas aplicaciones.



9.2.9. Kiosco

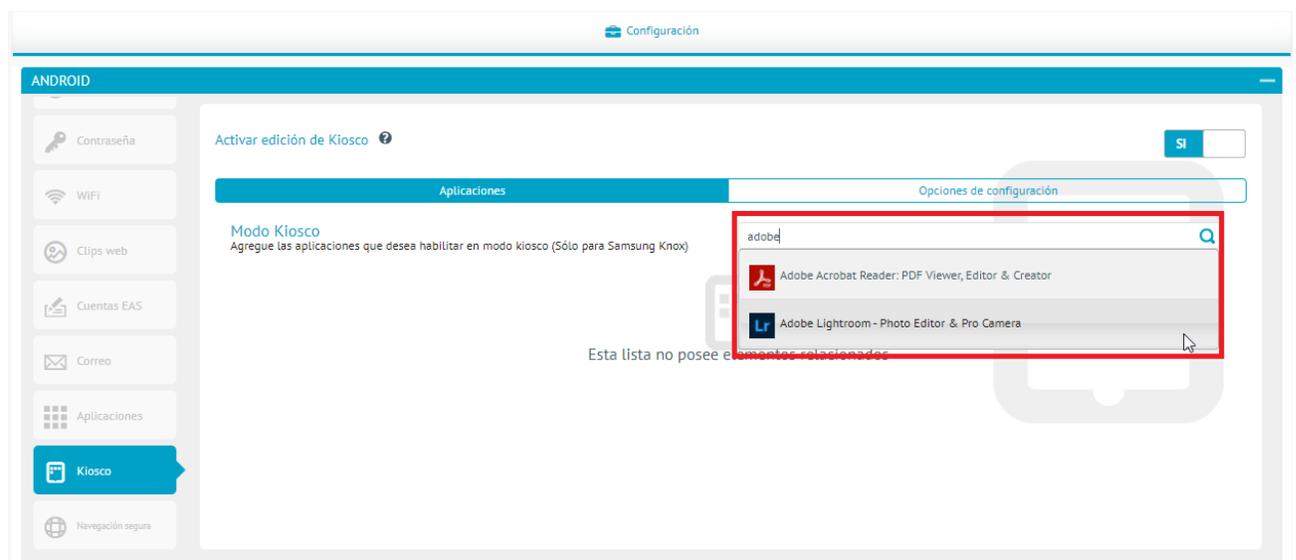
El módulo de Kiosco está destinado a que el dispositivo presente una interfaz por defecto con las aplicaciones y configuraciones aquí seleccionadas únicamente.

9.2.9.1. Android

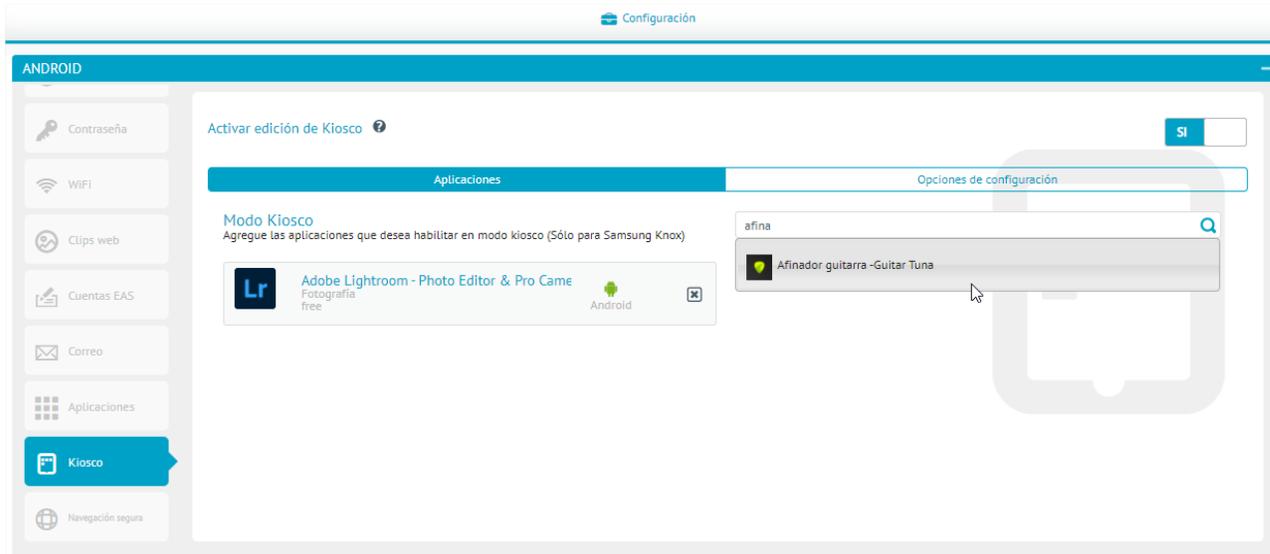
El modo Kiosco para Android genérico está disponible únicamente para vinculaciones con Agente Samsung Knox y Android superior a 4.0.

Para agregar aplicaciones al modo kiosco digite al menos 3 caracteres en la caja de texto para búsqueda y a continuación la consola presentará los resultados coincidentes en una lista desplegable tal y como se observa en la siguiente captura.

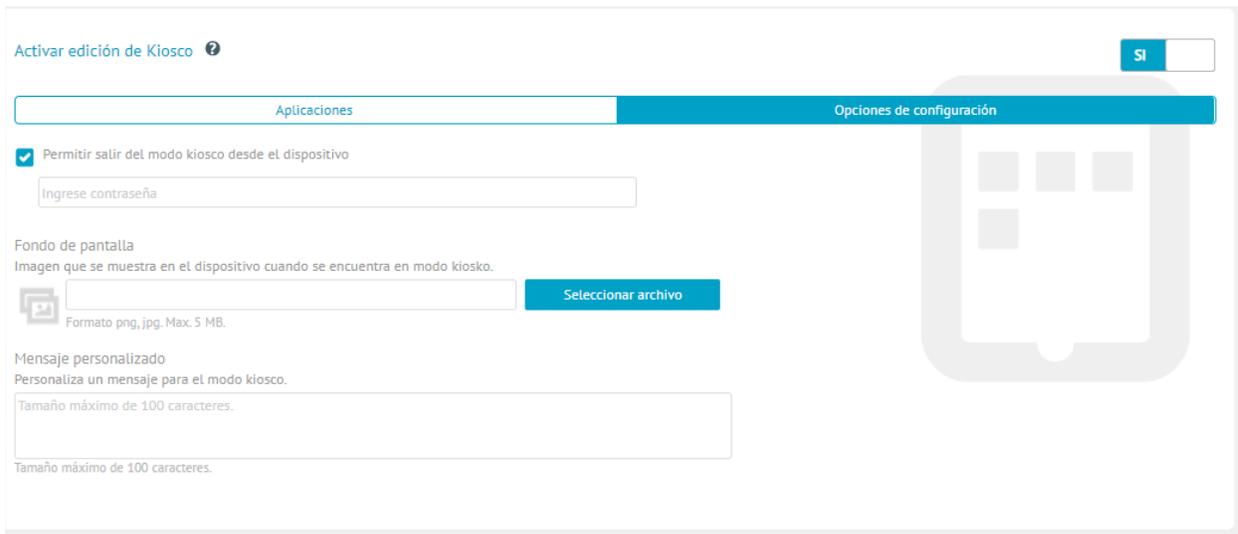
Luego haga clic en la aplicación para agregarla al listado.



Repita el proceso para cada aplicación



Para configurar opciones adicionales ingrese a la pestaña “opciones de configuración” y configure las opciones que se necesiten.



Las opciones de configuración disponibles son las siguientes:

- Contraseña de salida de kiosco: Al ingresar una contraseña, el usuario final del dispositivo tendrá la posibilidad de salir del modo kiosco, luego de ingresar dicha contraseña.
- Fondo de pantalla: El modo kiosco en el dispositivo mostrará la imagen que aquí de cargue. (5 Mb como máximo)
- Mensaje personalizado: La interfaz de modo kiosco presentará el mensaje que aquí se configure. (100 caracteres como máximo)

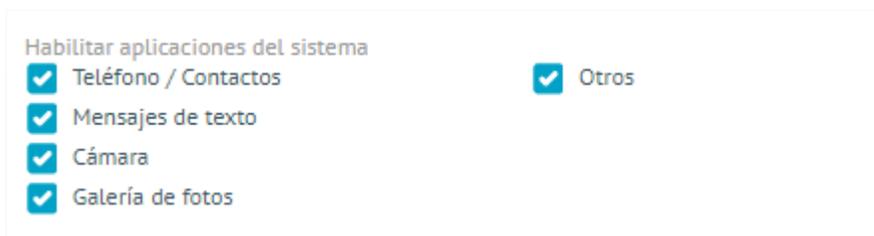
9.2.9.2. Android For Work

El modo kiosco para Android for Work está disponible únicamente para dispositivos vinculados en el modo AFW DO (Device Owner).

Para Android for Work, únicamente se podrán agregar aplicaciones que con anticipación hayan sido aprobadas para AFW.

Para agregarlas a kiosco se procede de igual forma que en el numeral anterior (9.2.8.1)

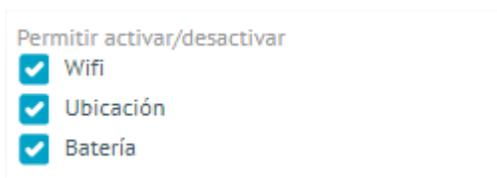
En el caso de las opciones de configuración se presentan los siguientes grupos adicionales a las del anterior numeral (9.2.8.1)



En este grupo se pueden activar/desactivar aplicaciones de sistema cuyos paquetes hayan sido agregados con anterior en la sección de configuración de Aplicaciones del Sistema Android. Al marcar cada casilla aparecerán en el kiosco las aplicaciones seleccionadas.



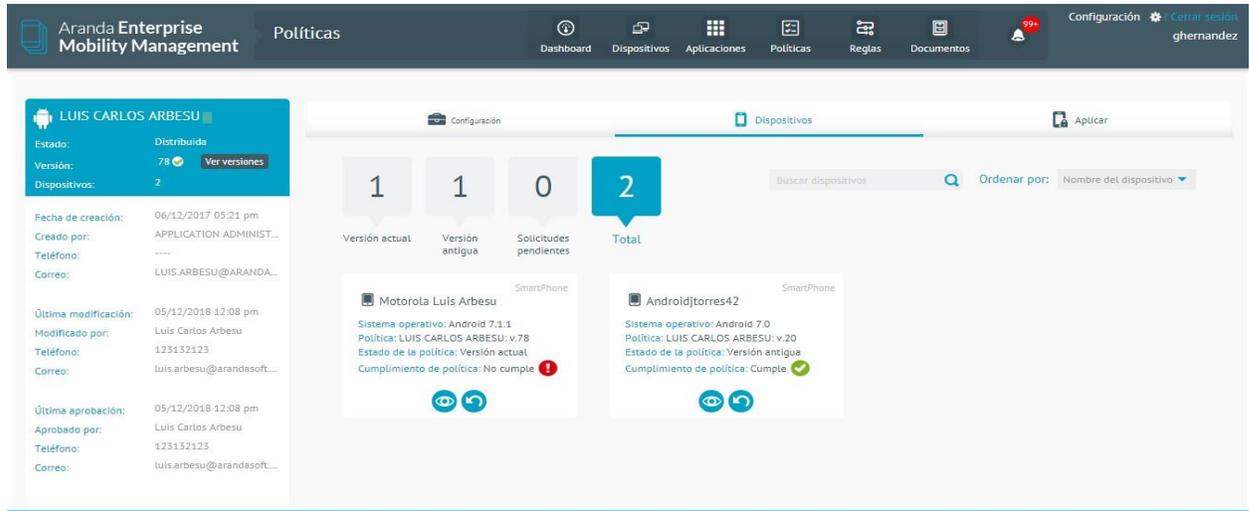
En este grupo se pueden activar/desactivar pantallas de configuración en modo kiosco para cada una de las opciones presentadas.



Para este grupo se pueden activar/desactivar interruptores de encendido en modo kiosco para apagar o prender cada una de las opciones presentadas.

9.2.10. Dispositivos asociados

En la pestaña dispositivos se visualizan los móviles que tienen asociada la política. Siempre que se aplica una política la solicitud se encuentra inicialmente en estado pendiente y pasa a versión actual cuando el móvil la recibe y la aplica. Si se realizan cambios en la política y no se actualiza la versión a los dispositivos que la tienen aplicada esta pasa a versión antigua. Dentro del listado de dispositivos asociados es posible realizar ordenamiento y búsqueda.



LUIS CARLOS ARBESU

Estado: Distribuida
 Versión: 78 [Ver versiones](#)
 Dispositivos: 2

Fecha de creación: 06/12/2017 05:21 pm
 Creado por: APPLICATION ADMINIST...
 Teléfono: 123132123
 Correo: LUIS.ARBESU@ARANDA...

Última modificación: 05/12/2018 12:08 pm
 Modificado por: Luis Carlos Arbesu
 Teléfono: 123132123
 Correo: luis.arbesu@arandasoft...

Última aprobación: 05/12/2018 12:08 pm
 Aprobado por: Luis Carlos Arbesu
 Teléfono: 123132123
 Correo: luis.arbesu@arandasoft...

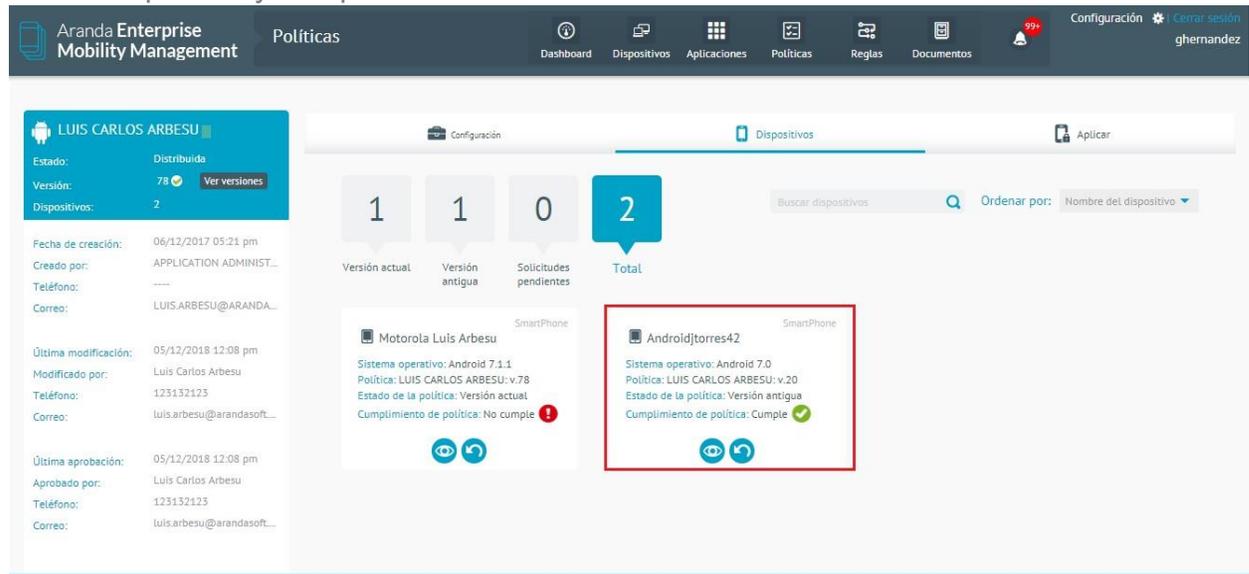
Dispositivos

1 Versión actual | 1 Versión antigua | 0 Solicitudes pendientes | 2 Total

Motorola Luis Arbesu (SmartPhone)
 Sistema operativo: Android 7.1.1
 Política: LUIS CARLOS ARBESU: v.78
 Estado de la política: Versión actual
 Cumplimiento de política: No cumple

Androidjtorres42 (SmartPhone)
 Sistema operativo: Android 7.0
 Política: LUIS CARLOS ARBESU: v.20
 Estado de la política: Versión antigua
 Cumplimiento de política: Cumple

El dispositivo muestra un resumen de la política aplicada, indicando: el nombre de dispositivo, tipo, sistema operativo y versión, nombre de la política junto con su versión, estado de política y cumplimiento.



LUIS CARLOS ARBESU

Estado: Distribuida
 Versión: 78 [Ver versiones](#)
 Dispositivos: 2

Fecha de creación: 06/12/2017 05:21 pm
 Creado por: APPLICATION ADMINIST...
 Teléfono: 123132123
 Correo: LUIS.ARBESU@ARANDA...

Última modificación: 05/12/2018 12:08 pm
 Modificado por: Luis Carlos Arbesu
 Teléfono: 123132123
 Correo: luis.arbesu@arandasoft...

Última aprobación: 05/12/2018 12:08 pm
 Aprobado por: Luis Carlos Arbesu
 Teléfono: 123132123
 Correo: luis.arbesu@arandasoft...

Dispositivos

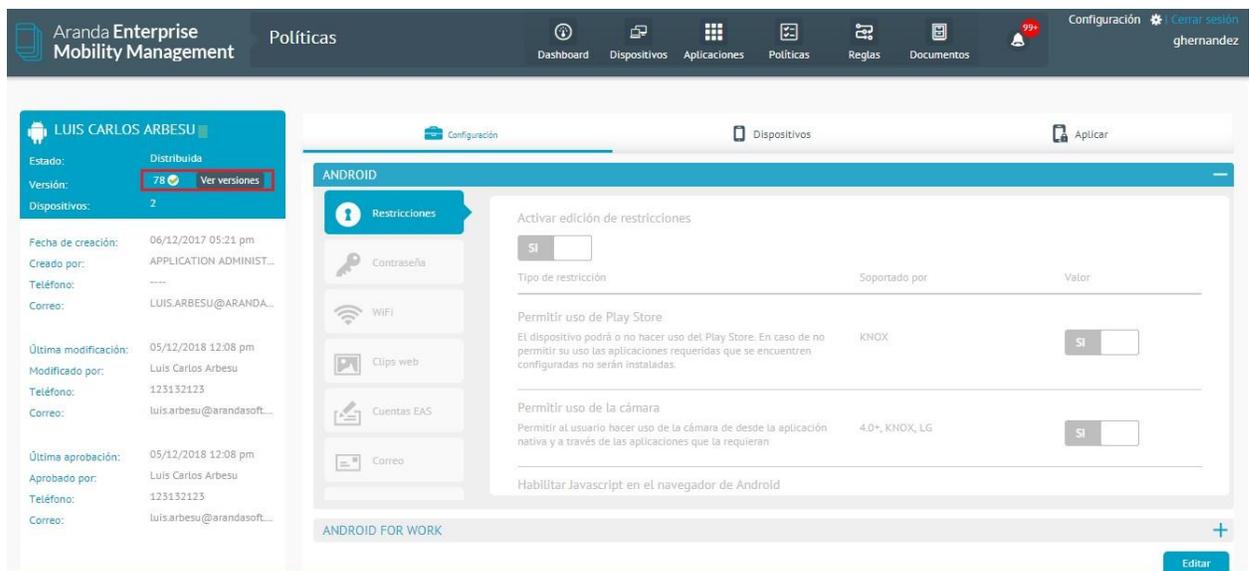
1 Versión actual | 1 Versión antigua | 0 Solicitudes pendientes | 2 Total

Motorola Luis Arbesu (SmartPhone)
 Sistema operativo: Android 7.1.1
 Política: LUIS CARLOS ARBESU: v.78
 Estado de la política: Versión actual
 Cumplimiento de política: No cumple

Androidjtorres42 (SmartPhone)
 Sistema operativo: Android 7.0
 Política: LUIS CARLOS ARBESU: v.20
 Estado de la política: Versión antigua
 Cumplimiento de política: Cumple

9.2.11. Aplicación de Políticas

Las políticas se pueden aplicar a usuario, grupos de usuarios o grupos de dispositivos en estado activo y pertenecer a la misma plataforma con la que se configuro la política.



The screenshot shows the 'Políticas' (Policies) section in the Aranda Enterprise Mobility Management interface. On the left, a user profile for 'LUIS CARLOS ARBESU' is displayed with details such as 'Estado: Distribuida', 'Versión: 78', and 'Dispositivos: 2'. The main area shows the configuration for an 'ANDROID' policy. A 'Restricciones' (Restrictions) section is active, with a toggle switch set to 'SI' (Yes). Below this, there are two rows of policy settings:

Tipo de restricción	Soportado por	Valor
Permitir uso de Play Store El dispositivo podrá o no hacer uso del Play Store. En caso de no permitir su uso las aplicaciones requeridas que se encuentren configuradas no serán instaladas.	KNOX	<input type="checkbox"/>
Permitir uso de la cámara Permitir al usuario hacer uso de la cámara de desde la aplicación nativa y a través de las aplicaciones que la requieran	4.0+, KNOX, LG	<input type="checkbox"/>

Other visible settings include 'Activar edición de restricciones' (checked), 'Habilitar Javascript en el navegador de Android', and a list of other policy categories like 'Contraseña', 'WIFI', 'Clips web', 'Cuentas EAS', and 'Correo'. An 'ANDROID FOR WORK' section is also visible at the bottom.

Para que la política se aplique correctamente es necesario aprobar la política.

Aranda Enterprise Mobility Management | Políticas

Dashboard | Dispositivos | Aplicaciones | Políticas | Reglas | Documentos | Configuración | Cerrar sesión ghermanez

LUIS CARLOS ARBESU | En edición

Estado: En edición
 Versión: 79 [Ver versiones](#)
 Dispositivos: 2

Fecha de creación: 06/12/2017 05:21 pm
 Creado por: APPLICATION ADMINIST...
 Teléfono: ----
 Correo: LUIS.ARBESU@ARANDA...

Última modificación: 21/01/2019 10:02 am
 Modificado por: German Hernandez
 Teléfono: 123123123
 Correo: german.hernandez@ara...

Última aprobación: 05/12/2018 12:08 pm
 Aprobado por: Luis Carlos Arbesu
 Teléfono: 123132123
 Correo: luis.arbesu@arandasoft...

ANDROID

Restricciones

Activar edición de restricciones: SI

Tipo de restricción	Soportado por	Valor
Permitir uso de Play Store El dispositivo podrá o no hacer uso del Play Store. En caso de no permitir su uso las aplicaciones requeridas que se encuentren configuradas no serán instaladas.	KNOX	<input checked="" type="checkbox"/> SI
Permitir uso de la cámara Permitir al usuario hacer uso de la cámara de desde la aplicación nativa y a través de las aplicaciones que la requieran	4.0+, KNOX, LG	<input checked="" type="checkbox"/> SI
Habilitar Javascript en el navegador de Android		

ANDROID FOR WORK

La política se guardó correctamente

9.3. Versionamiento y re- distribución de políticas

Por cada cambio que se realice sobre la política aumenta el número de versión. Cabe aclarar que si la política no se aprueba la versión que se aplica al dispositivo es la última aprobada.

Aranda Enterprise Mobility Management | Políticas

Dashboard | Dispositivos | Aplicaciones | Políticas | Reglas | Documentos | Configuración | Cerrar sesión ghermanez

LUIS CARLOS ARBESU | En edición

Estado: En edición
 Versión: 79 [Ver versiones](#)
 Dispositivos: 2

Fecha de creación: 06/12/2017 05:21 pm
 Creado por: APPLICATION ADMINIST...
 Teléfono: ----
 Correo: LUIS.ARBESU@ARANDA...

Última modificación: 21/01/2019 10:04 am
 Modificado por: German Hernandez
 Teléfono: 123123123
 Correo: german.hernandez@ara...

Última aprobación: 05/12/2018 12:08 pm
 Aprobado por: Luis Carlos Arbesu
 Teléfono: 123132123
 Correo: luis.arbesu@arandasoft...

ANDROID

Restricciones

Activar edición de restricciones: NO

ANDROID FOR WORK

Editar | Aprobar

Las versiones almacenadas se pueden visualizar al dar clic en "Ver versiones"

Aranda Enterprise Mobility Management | Políticas

Dashboard | Dispositivos | Aplicaciones | Políticas | Reglas | Documentos

Configuración | Cerrar sesión ghermanez

LUIS CARLOS ARBESU | En edición | Versión: 79 | Ver versiones

Dispositivos: Versiones de políticas

Versión	Estado	Fecha de creación
Versión: 79	Actual	05/12/2018 12:06 pm
Versión: 78		05/12/2018 12:08 pm
Versión: 77		05/12/2018 12:06 pm
Versión: 76		04/12/2018 04:24 pm
Versión: 75		04/12/2018 02:54 pm
Versión: 74		29/11/2018 07:03 pm
Versión: 73		29/11/2018 06:57 pm
Versión: 72		29/11/2018 05:56 pm
Versión: 71		29/11/2018 05:07 pm
Versión: 70		29/11/2018 04:35 pm

Activar edición de restricciones: NO

ANDROID FOR WORK

Editar | Aprobar

Se tiene la posibilidad de ver la versión actual o restaurar la versión

Aranda Enterprise Mobility Management | Políticas

Dashboard | Dispositivos | Aplicaciones | Políticas | Reglas | Documentos

Configuración | Cerrar sesión ghermanez

LUIS CARLOS ARBESU | En edición | Versión: 74 | Ver versiones

Dispositivos:

Fecha de creación: 06/12/2017 05:21 pm
Creado por: APPLICATION ADMINIST...
Teléfono: ----
Correo: LUIS.ARBESU@ARANDA...

Última modificación: 29/11/2018 07:03 pm
Modificado por: APPLICATION ADMINIST...
Teléfono: ----
Correo: LUIS.ARBESU@ARANDA...

Última aprobación: ---
Aprobado por: APPLICATION ADMINIST...
Teléfono: ----
Correo: LUIS.ARBESU@ARANDA...

Restricciones

Activar edición de restricciones: SI

Tipo de restricción	Soportado por	Valor
Permitir uso de Play Store El dispositivo podrá o no hacer uso del Play Store. En caso de no permitir su uso las aplicaciones requeridas que se encuentren configuradas no serán instaladas.	KNOX	<input type="checkbox"/> SI
Permitir uso de la cámara Permitir al usuario hacer uso de la cámara de desde la aplicación nativa y a través de las aplicaciones que la requieran	4.0+, KNOX, LG	<input type="checkbox"/> SI

Habilitar Javascript en el navegador de Android

ANDROID FOR WORK

Ver version actual | Restaurar versión

La política se restaura.

Aranda Enterprise Mobility Management Políticas

Dashboard Dispositivos Aplicaciones Políticas Reglas Documentos Configuración gherandez

LUIS CARLOS ARBESU
 Estado: En edición
 Versión: 79 Ver versiones
 Dispositivos: 2

Fecha de creación: 06/12/2017 05:21 pm
 Creado por: APPLICATION ADMINIST...
 Teléfono: ----
 Correo: LUIS.ARBESU@ARANDA...

Última modificación: 24/01/2019 10:09 am
 Modificado por: German Hernandez
 Teléfono: 123123123
 Correo: german.hernandez@ara...

Última aprobación: 05/12/2018 12:08 pm
 Aprobado por: ----
 Teléfono: ----
 Correo: ----

ANDROID

Restricciones

Activar edición de restricciones

Tipo de restricción	Soportado por	Valor
Permitir uso de Play Store El dispositivo podrá o no hacer uso del Play Store. En caso de no permitir su uso las aplicaciones requeridas que se encuentren configuradas no serán instaladas.	KNOX	<input type="checkbox"/>
Permitir uso de la cámara Permitir al usuario hacer uso de la cámara de desde la aplicación nativa y a través de las aplicaciones que la requieran	4.0+, KNOX, LG	<input type="checkbox"/>

Habilitar Javascript en el navegador de Android

ANDROID FOR WORK

La política se restableció con éxito a la versión solicitada

Esta se debe aprobar.

Aranda Enterprise Mobility Management Políticas

Dashboard Dispositivos Aplicaciones Políticas Reglas Documentos Configuración Central sesión gherandez

LUIS CARLOS ARBESU
 Estado: En edición
 Versión: 79 Ver versiones
 Dispositivos: 2

Fecha de creación: 06/12/2017 05:21 pm
 Creado por: APPLICATION ADMINIST...
 Teléfono: ----
 Correo: LUIS.ARBESU@ARANDA...

Última modificación: 24/01/2019 10:09 am
 Modificado por: German Hernandez
 Teléfono: 123123123
 Correo: german.hernandez@ara...

Última aprobación: 05/12/2018 12:08 pm
 Aprobado por: ----
 Teléfono: ----
 Correo: ----

ANDROID

Restricciones

Activar edición de restricciones

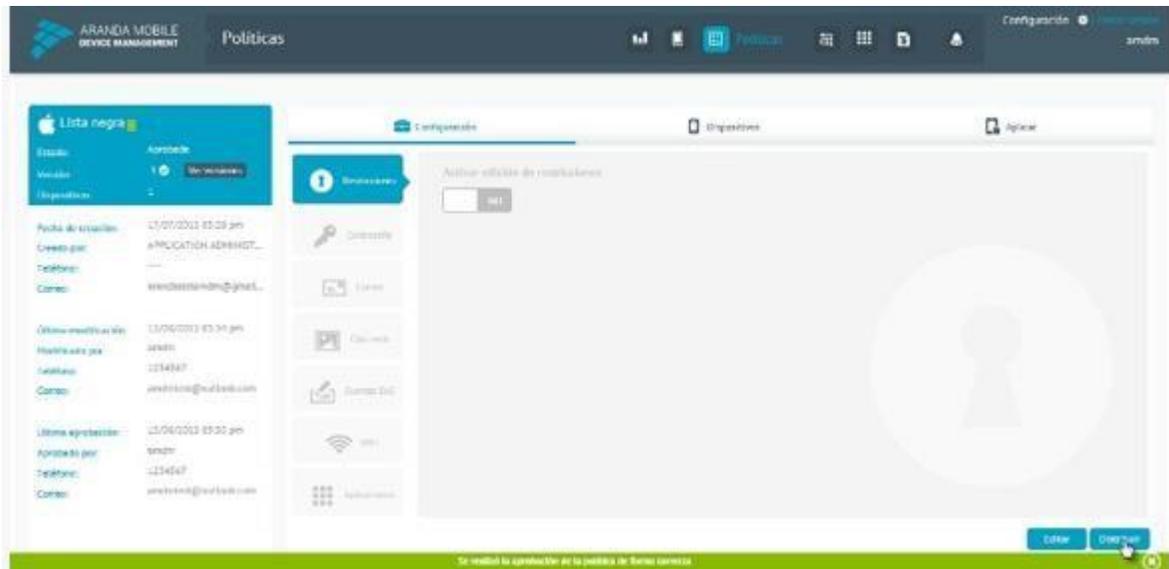
Tipo de restricción	Soportado por	Valor
Permitir uso de Play Store El dispositivo podrá o no hacer uso del Play Store. En caso de no permitir su uso las aplicaciones requeridas que se encuentren configuradas no serán instaladas.	KNOX	<input type="checkbox"/>
Permitir uso de la cámara Permitir al usuario hacer uso de la cámara de desde la aplicación nativa y a través de las aplicaciones que la requieran	4.0+, KNOX, LG	<input type="checkbox"/>

Habilitar Javascript en el navegador de Android

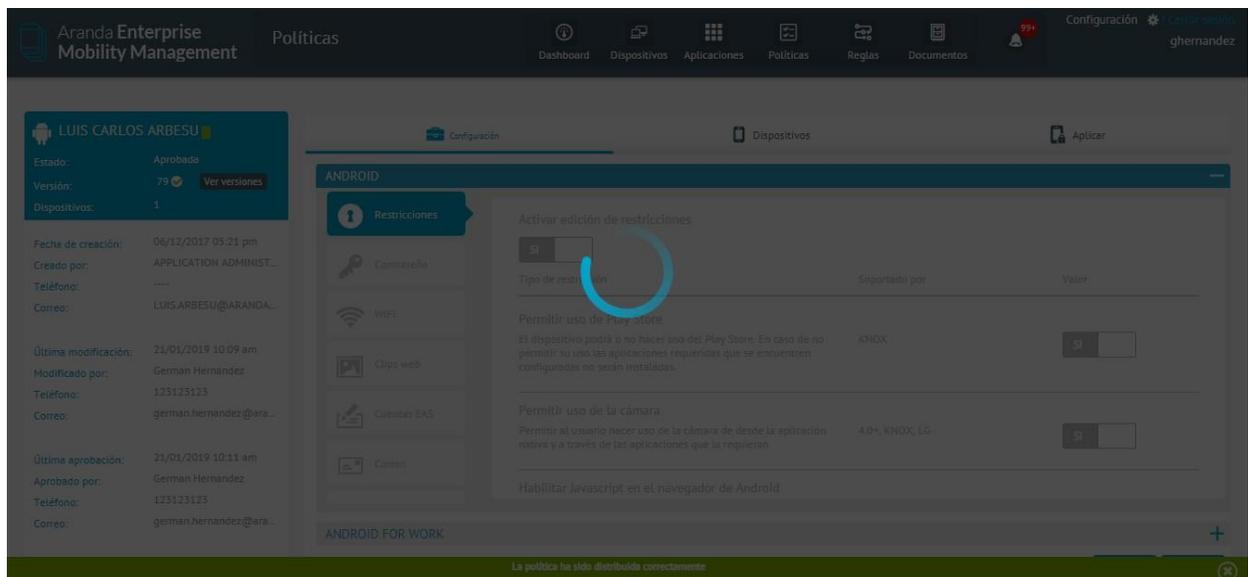
ANDROID FOR WORK

Aprobar

Y distribuir para aplicar todos los cambios a los dispositivos que tienen asociada la política.



La política se distribuye exitosamente.



Problemas comunes en el manejo de políticas

- Si la política se aplica y esta permanece como “Solicitudes pendientes” es necesario validar si el dispositivo móvil tiene problemas de conectividad.

The screenshot shows the Aranda Enterprise Mobility Management interface. The top navigation bar includes 'Políticas', 'Dashboard', 'Dispositivos', 'Aplicaciones', 'Políticas', 'Reglas', 'Documentos', 'Configuración', and 'Cerrar sesión gherandez'. The main content area is divided into two sections. On the left, a profile card for 'LUIS CARLOS ARBESU' shows details such as 'Estado: Distribuida', 'Versión: 79', 'Dispositivos: 1', and various dates and contact information. On the right, a summary dashboard displays four metrics: 'Versión actual' (0), 'Versión antigua' (0), 'Solicitudes pendientes' (1, highlighted with a red box), and 'Total' (1). Below these metrics, two device cards are shown: 'Motorola Luis Arbesu' (SmartPhone) with system version 7.1.1 and policy status 'No cumple' (indicated by a red exclamation mark), and 'Androidtorres42' (SmartPhone) with system version 7.0 and policy status 'Cumple' (indicated by a green checkmark).

- Cuando aplique una política de cuenta EAS o correo a un dispositivo Android genérico, esta nunca la recibirá el dispositivo móvil, ya que solo aplica para dispositivos Samsung Knox
- La única restricción que es posible aplicar a Android genérico es bloqueo de cámara.
- No es posible aplicar una política en estado Edición, está siempre debe estar aprobada, solo se aplica en edición si la política ya se encontraba en estado aprobada.

10. REGLAS

Reglas de negocio en EMM

Actualmente se manejan cuatro tipos de reglas de negocio:

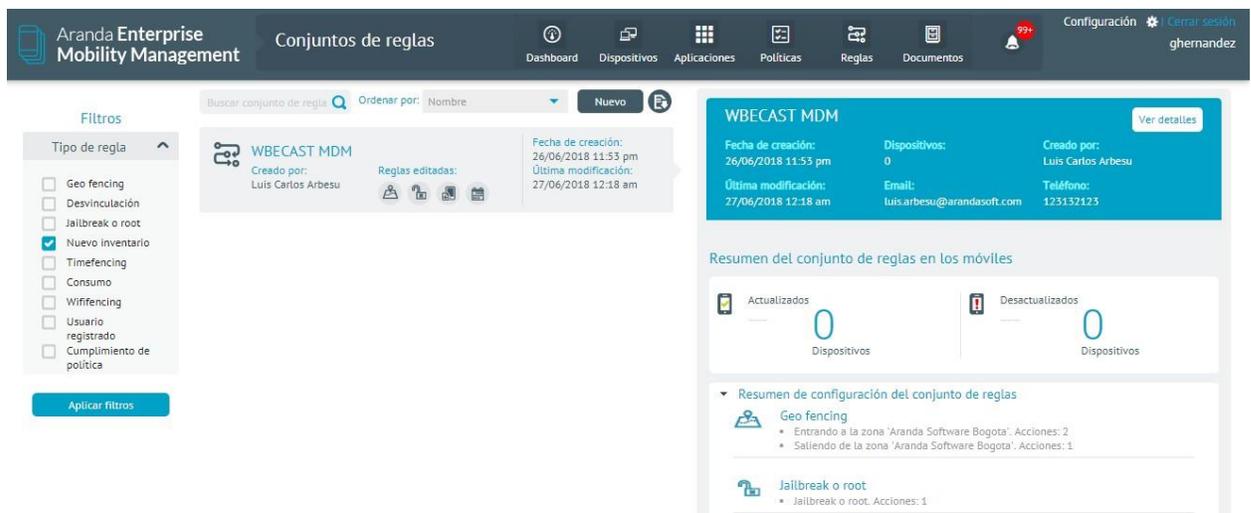
- **Geofencing:** seguimiento de la ubicación del dispositivo en determinada área geográfica con el fin de saber si el dispositivo entra o sale de esa área.
- **Desvinculación:** notificar al sistema cuando el dispositivo fue desvinculado.
- **Jailbreak o root:** notificar al sistema si el dispositivo tiene jailbreak o root.
- **Nuevo inventario:** Siempre que se solicita un nuevo inventario, se genera un evento para que sea evaluado por las condiciones del conjunto de reglas.

- **Timefencing:** Es el seguimiento del horario en el cual se encuentra un dispositivo con el fin de saber si este entra o sale del horario establecido.
- **Consumo:** Función permite consultar el consumo realizado de voz y/o datos tanto local como en roaming.
- **Wififencing:** Función que permite controlar las redes inalámbricas a las que se conecta el dispositivo dentro de un listado de redes, con el fin de saber si el dispositivo se conecta o se desconecta a una determinada o autorizada red wi-fi.
- **Usuario Registrado:** Esta función notifica al sistema el cumplimiento de distintas reglas y aplica acciones sobre usuario. (**Aplica solo para usuarios autenticados con Directorio Activo de Windows**).
- **Cumplimiento de política:** notificar al sistema si el dispositivo cumple con una política determinada.

Cuando alguna de estas reglas se cumple el sistema realiza determinadas acciones definidas por el usuario.

10.1. Configuración de conjuntos de reglas

Para acceder a la sección del conjunto de reglas se debe seleccionar desde el menú superior de la consola web.



The screenshot displays the 'Aranda Enterprise Mobility Management' console. The main header shows 'Conjuntos de reglas' and a navigation menu with options like Dashboard, Dispositivos, Aplicaciones, Políticas, Reglas, and Documentos. A search bar and 'Nuevo' button are visible. On the left, a 'Filtros' (Filters) sidebar lists various rule types, with 'Nuevo inventario' selected. The main content area shows a list of rule sets, with 'WBECAST MDM' selected. This rule set is created by 'Luis Carlos Arbesu' and has a creation date of 26/06/2018 11:53 pm. Below the list, a 'Resumen del conjunto de reglas en los móviles' (Summary of rule set on mobile devices) shows 0 updated and 0 outdated devices. A 'Resumen de configuración del conjunto de reglas' (Summary of rule set configuration) lists actions for 'Geo fencing' (2 actions) and 'Jailbreak o root' (1 action).

Para agregar una nueva regla presione de clic en **Nuevo**, ubicado en la parte superior del panel de listados de reglas.

En el formulario para agregar una nueva regla se debe ingresar el nombre de la regla, y luego se puede habilitar cualquiera de las disponibles, cuando se habilita cualquiera de estas se despliega un formulario para indicar la acción asociada a la regla.

Dentro del formulario de acciones en cada una de las reglas se puede configurar una serie de condiciones y agregarlas según su configuración.

The screenshot displays the 'Aranda Enterprise Mobility Management' dashboard. The main navigation bar includes 'Conjuntos de reglas' and various tool icons. The left sidebar shows a list of management actions, with 'Timefencing' highlighted. The central panel is titled 'Configuración' and shows the configuration for a rule named 'Timefencing 1'. A red box highlights the 'Condiciones' section, where a rule is defined as 'Si Plataforma = Android'. Below this, the 'Acciones' section shows 'Crear alerta' as the selected action. The interface includes buttons for 'Adicionar regla', 'Agregar', 'Guardar', 'Cancelar', and 'Borrar'.

Después de esto en la parte inferior se puede configurar acciones a tomar dentro de las que encontramos las siguientes:

- Desvinculación
- Enviar mail
- Crear alerta
- Enviar mensaje
- Cambiar política
- Enviar sonido
- Servicio web de ASDK
- Bloquear dispositivo
- Bloquear contenido
- Desbloquear contenido
- Cambiar contraseña
- Bloquear la pantalla
- Bloqueo Total

Para almacenar los cambios realizados de clic en **Guardar** en la parte inferior derecha del formulario.

Nota: La totalidad de las acciones mencionadas previamente **NO** aplican en todas las reglas.

10.2. Listado y pre visualización de conjuntos de reglas

La lista de reglas almacenadas se visualiza desde la vista principal del menú de reglas. Los filtros permiten buscar por:

- Regla de negocio
- Nombre

Además, estas se pueden ordenar por:

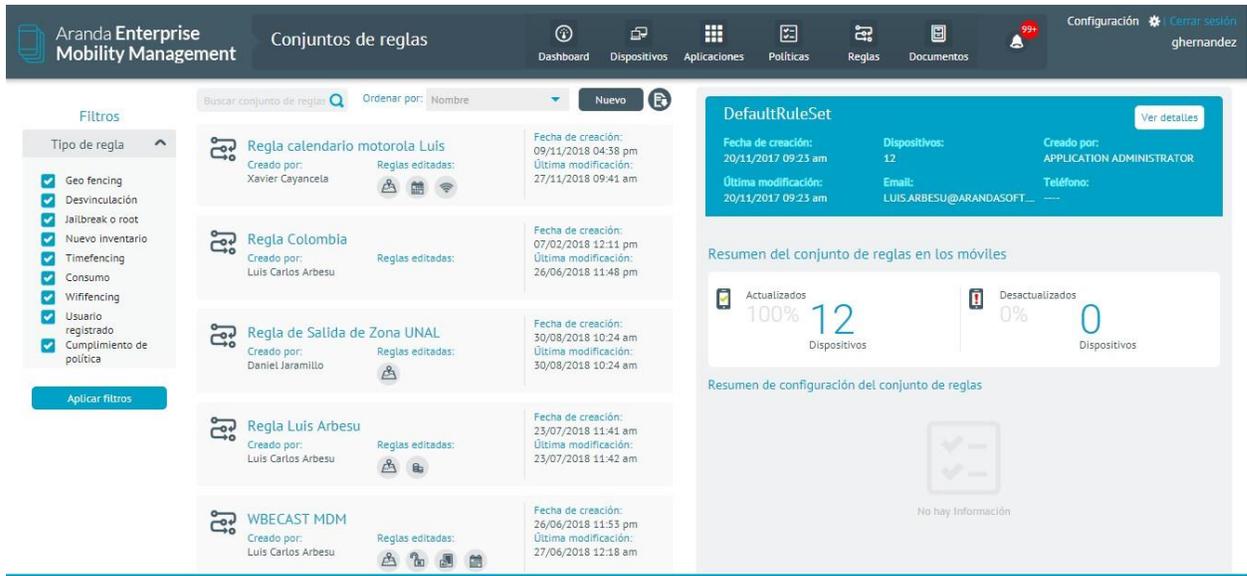
- Nombre
- Usuario creador
- Fecha de creación
- Fecha de modificación

En la parte derecha de la vista se presenta un resumen de la regla seleccionada, en la parte superior del resumen se presenta la siguiente información:

- Fecha de creación
- Última modificación
- Dispositivos
- Email
- Creado por

- Teléfono

En la parte media del resumen se presenta el número de dispositivos que tienen aplicada la regla separada por los que están actualizados y los que no están actualizados. En la parte inferior del resumen se presentan las acciones asociadas a cada regla de negocio existente en EMM.

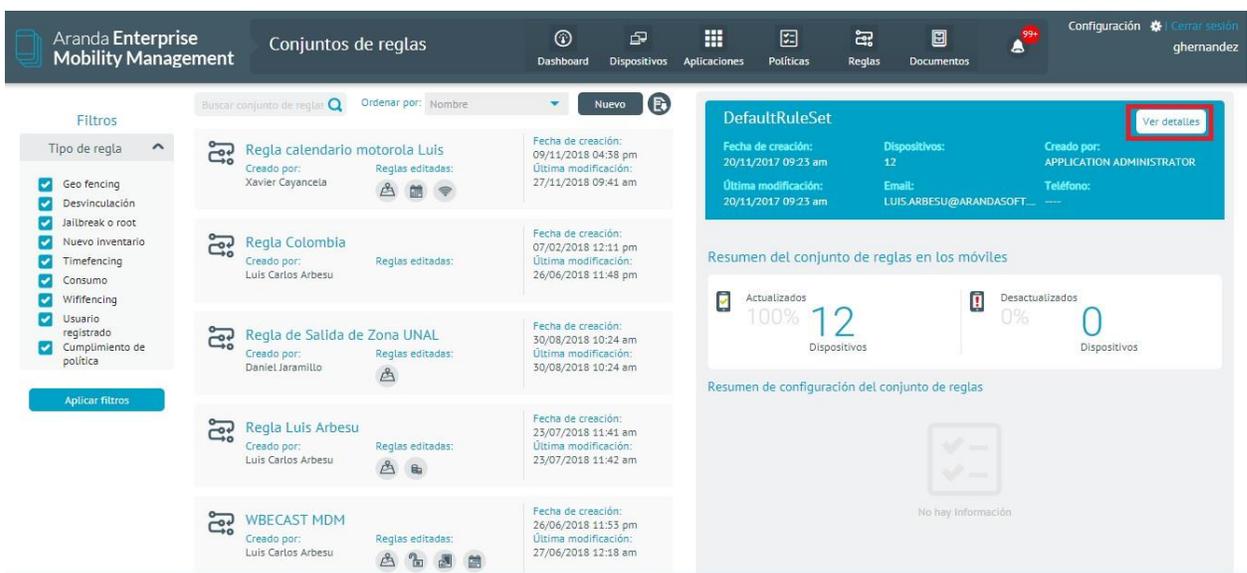


The screenshot shows the 'Conjuntos de reglas' (Rule Sets) page in Aranda Enterprise Mobility Management. The interface includes a navigation bar with 'Dashboard', 'Dispositivos', 'Aplicaciones', 'Políticas', 'Reglas', and 'Documentos'. A search bar and 'Ordenar por: Nombre' dropdown are present. A 'Filtros' sidebar on the left lists various rule types like 'Geo fencing', 'Desvinculación', etc. The main area displays a list of rule sets, each with its name, creator, and creation/modification dates. A 'DefaultRuleSet' summary card is visible on the right, showing 'Actualizados 100% 12 Dispositivos' and 'Desactualizados 0% 0 Dispositivos'. A 'Ver detalles' button is highlighted in the top right of the DefaultRuleSet card.

10.3. Dispositivos asociados

10.3.1. Visualizar dispositivos

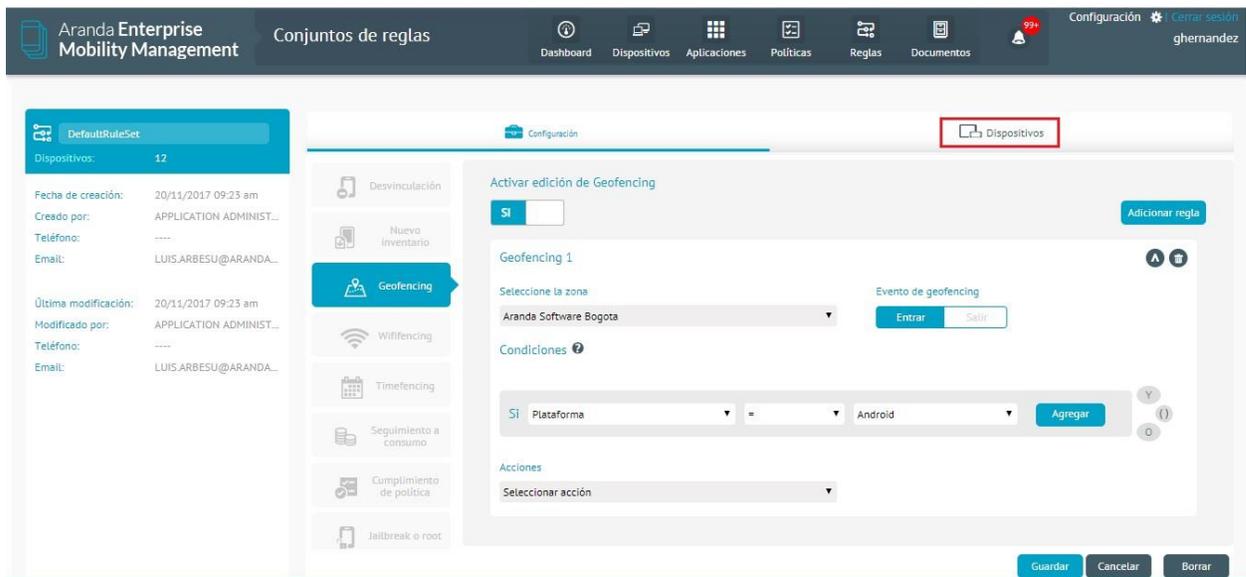
Para visualizar la lista de dispositivos a los cuales se le aplicó una regla, se debe seleccionar el botón Ver detalles ubicado en la parte superior derecha del resumen de la regla.



This screenshot is identical to the previous one, but with a red box highlighting the 'Ver detalles' button in the top right corner of the 'DefaultRuleSet' summary card, indicating the action to view associated devices.

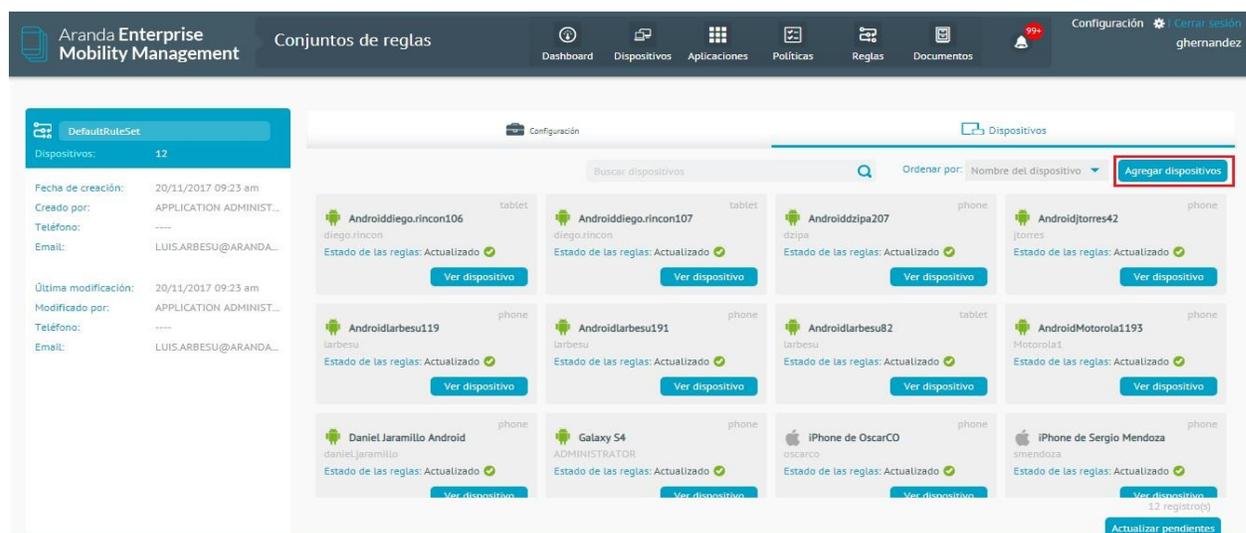
En el detalle de la regla seleccione la pestaña **Dispositivos**. En esta vista se puede visualizar la lista de dispositivos asociados a la regla, mostrando el tipo de dispositivos (teléfono o tableta), el nombre del dispositivo, su dueño y si la regla está actualizada, además presenta opciones para actualizar la regla y ver la información detallada del dispositivo.

En la parte inferior de la vista está el botón **Actualizar pendientes** para hacer una actualización masiva de la regla a los dispositivos asociados.

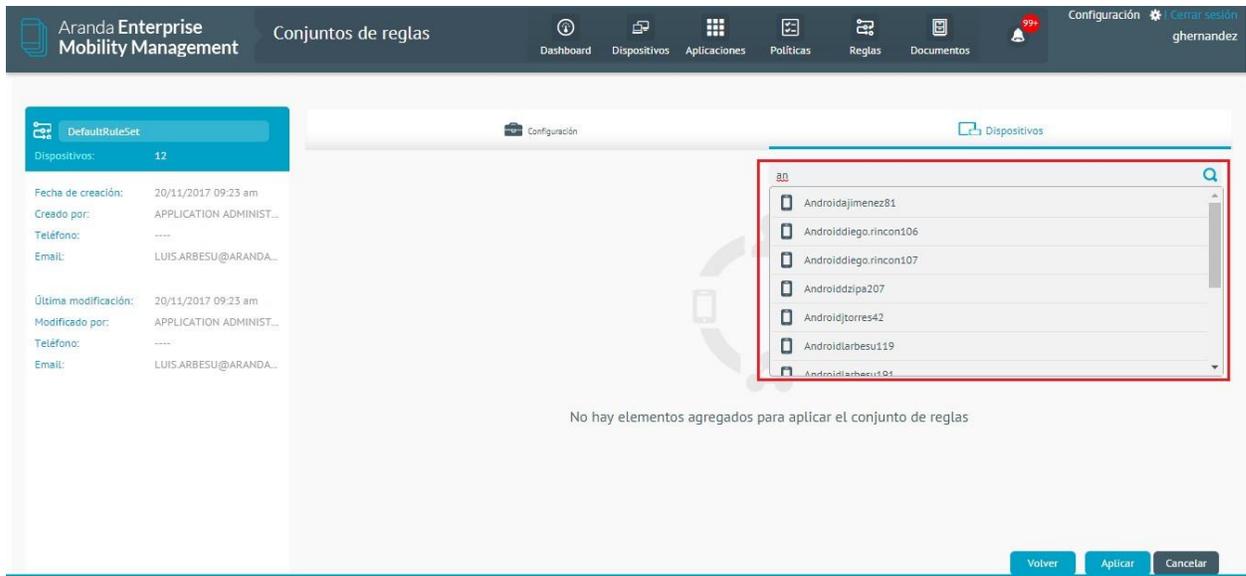


10.3.2. Agregar dispositivos

Para agregar dispositivos a una regla determinada se debe ver el detalle de la regla y dar clic en la pestaña **Dispositivos**, al seleccionar la pestaña, en la parte derecha se debe seleccionar el botón **Agregar dispositivos**.



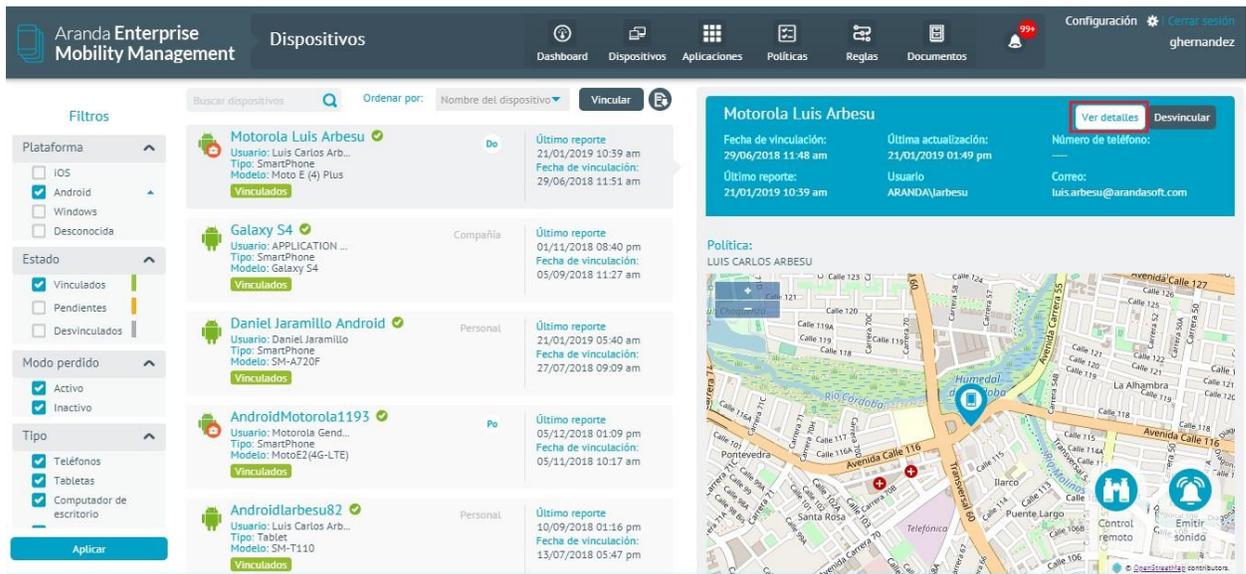
En el campo de búsqueda se filtran y agregan los dispositivos, grupos de dispositivos, usuarios y grupos de usuarios que se quieren agregar para aplicarles la regla.



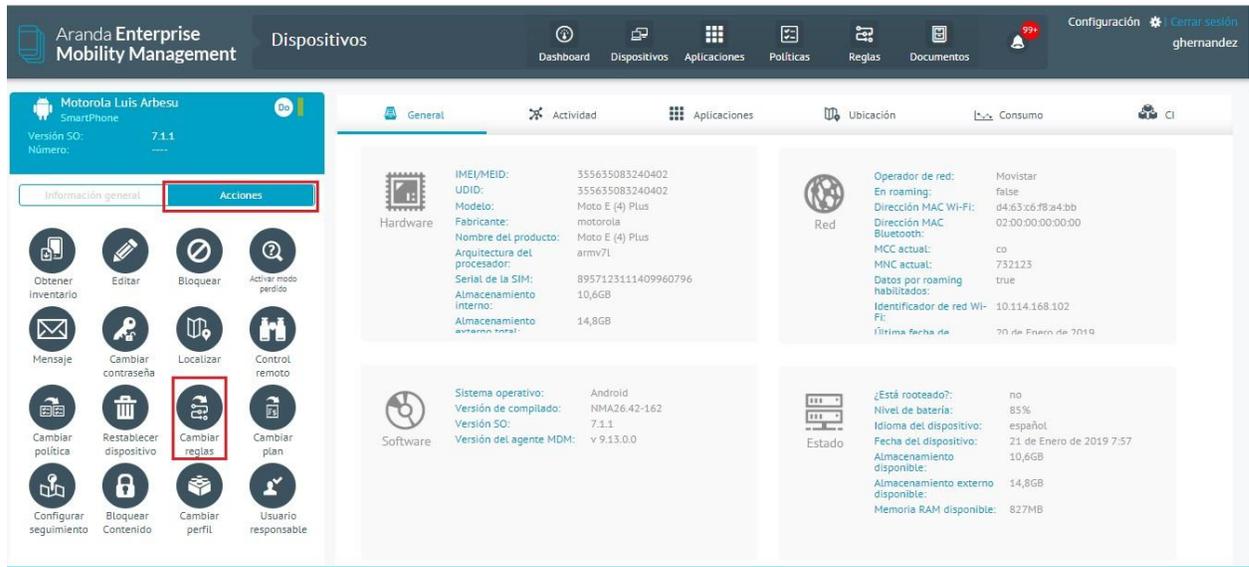
10.4. Aplicación de conjuntos de reglas

Las reglas pueden ser aplicadas para todos los dispositivos a los que aplican o de forma individual. Para aplicar un conjunto de reglas desde la sección de Reglas del menú principal se deben seguir los pasos explicados en la sección **Dispositivos asociados**.

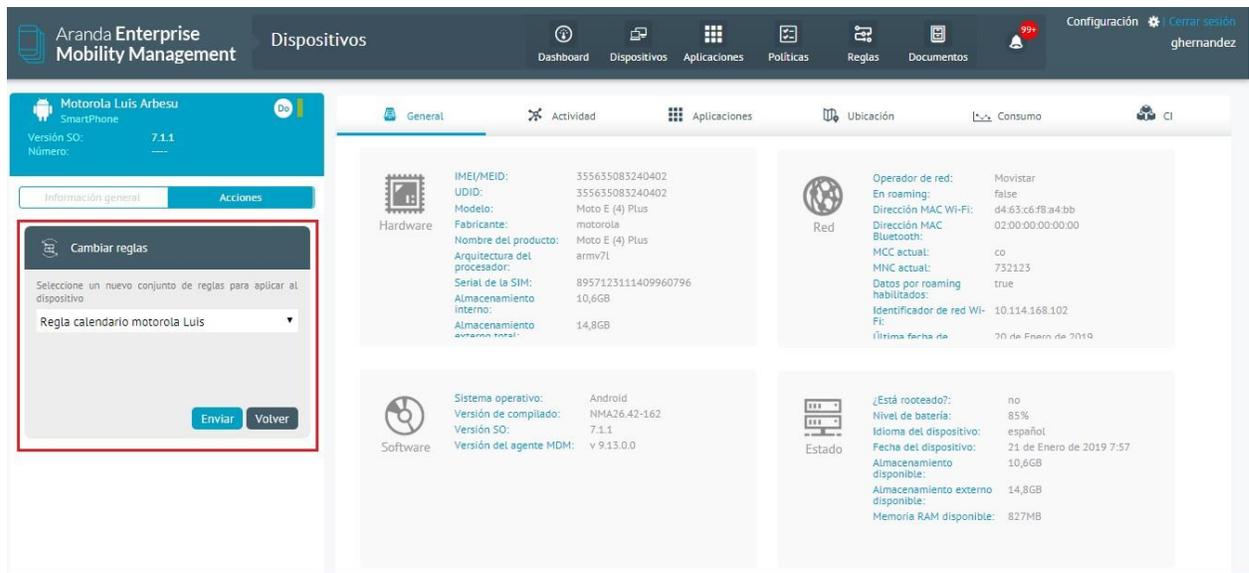
También se pueden aplicar un conjunto de reglas desde la hoja de vida del dispositivo, para esto se debe seleccionar la sección **Dispositivos** del menú principal, seleccionar un dispositivo de la lista y presionar el botón **Ver detalles** del panel ubicado a la derecha



Al presionar el botón de **ver detalles**, aparece la hoja de vida del dispositivo, en la parte inferior izquierda se presenta un menú con una lista de acciones para realizar con ese dispositivo, entre las cuales se encuentra la opción **Cambiar conjunto de reglas**.

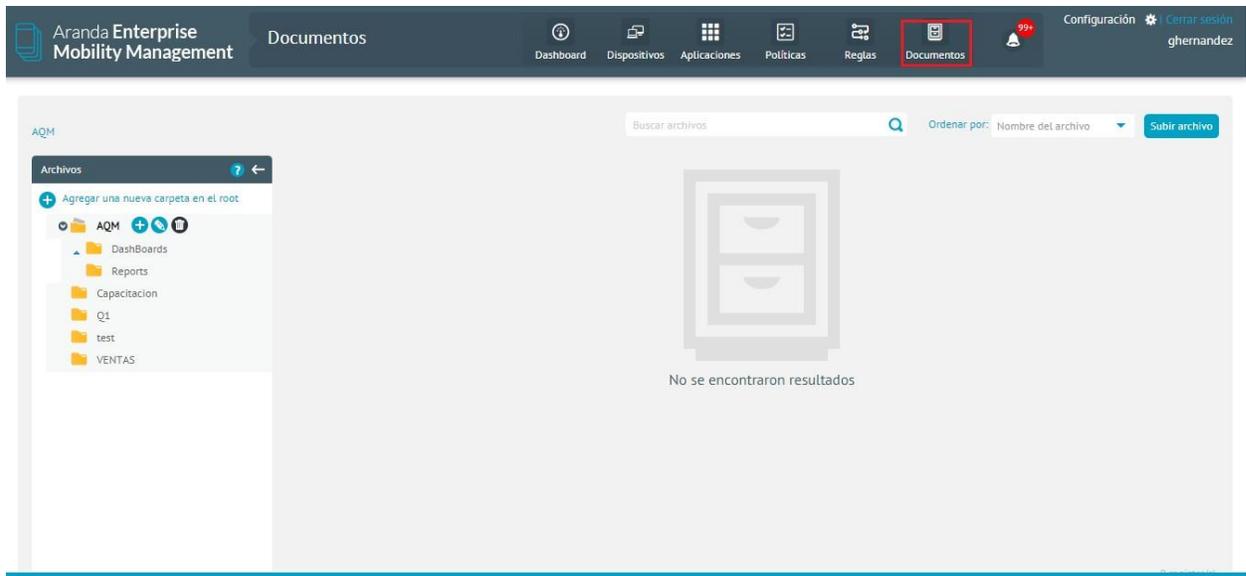


Al seleccionar la opción aparece un cuadro con una lista desplegable que contiene la lista de reglas existentes, se puede seleccionar una de las reglas y aplicarla al dispositivo.



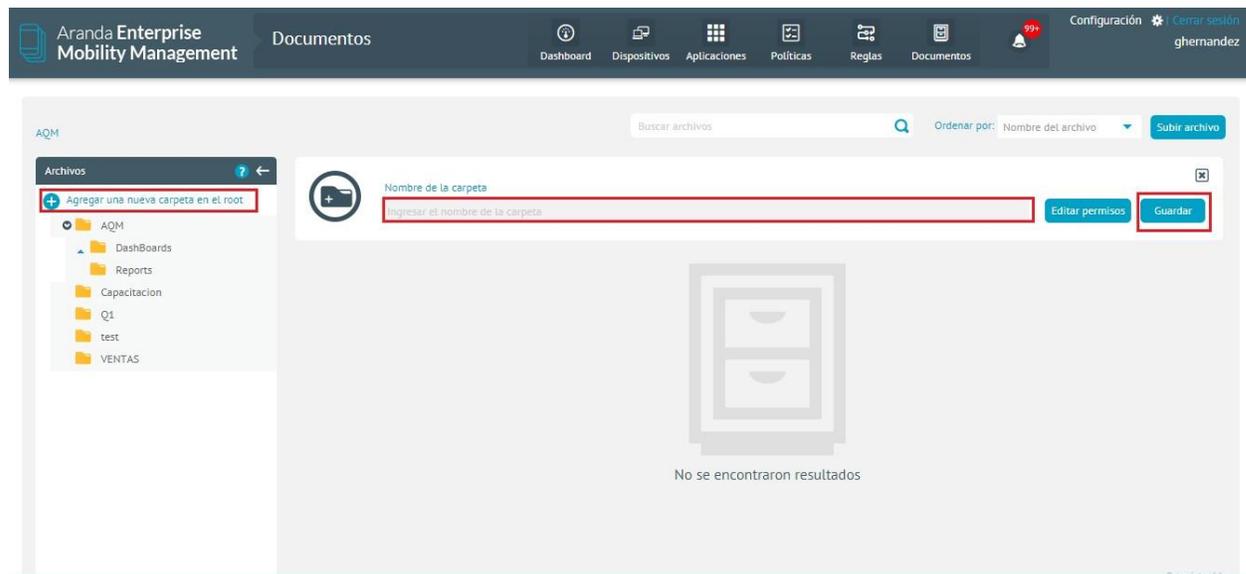
11. DOCUMENTOS

La sección de documentos permite la administración de contenido, ubicaciones y permisos sobre estas ubicaciones, para ingresar, debe seleccionar a la sección **Documentos** del menú principal. Para visualizar y administrar los contenidos desde los dispositivos móviles se cuenta con la aplicación (Content Manager).

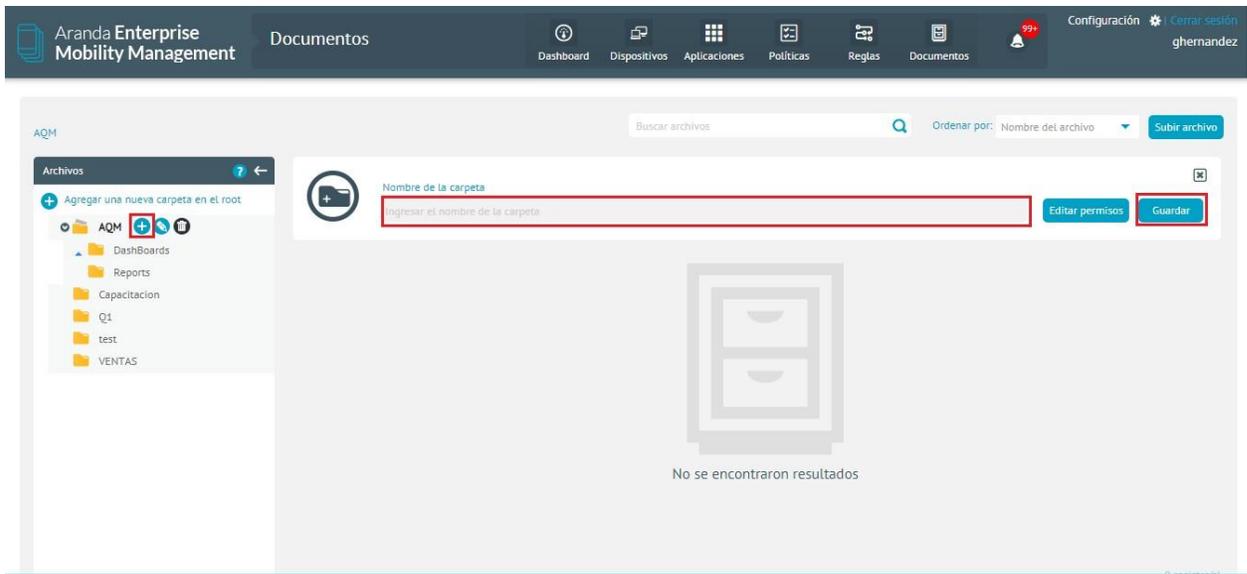


11.1. Administración de contenidos Creación de carpetas y Sub-carpetas

Para realizar la creación de una carpeta se dé clic en **Agregar una nueva carpeta** en el root, luego observará una pantalla en donde debe ingresar el nombre de la carpeta y posteriormente debe dar clic en **Guardar**.

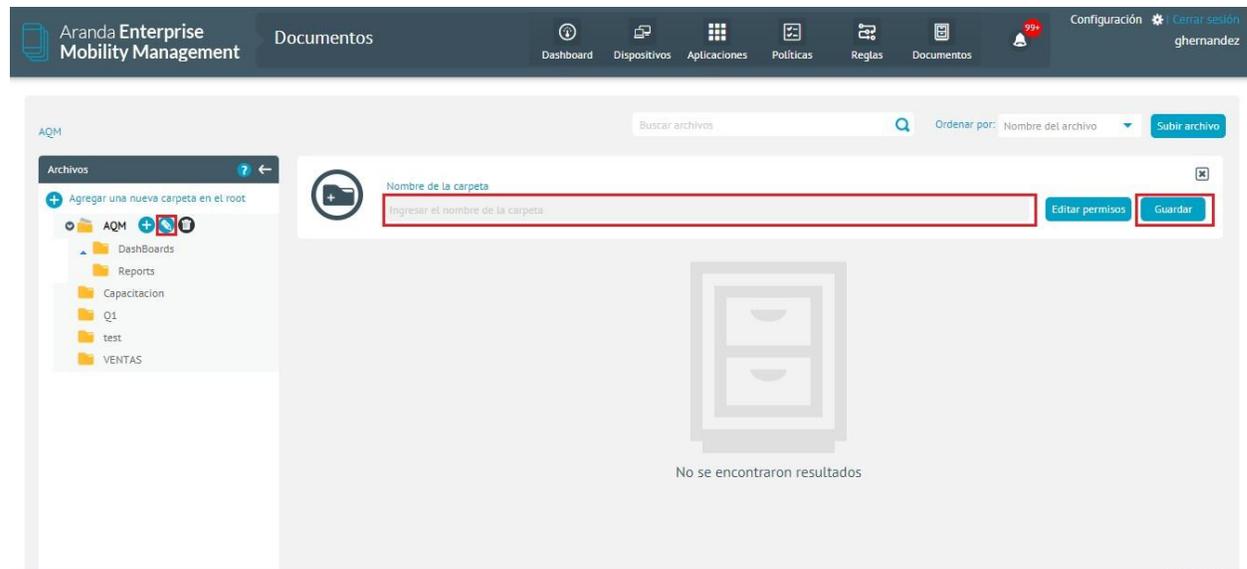


Para crear una sub- carpeta, diríjase hasta la carpeta contenedora y de clic en el icono **Agregar**, luego observará una pantalla en donde debe ingresar el nombre de la carpeta y posteriormente de clic en **Guardar**.

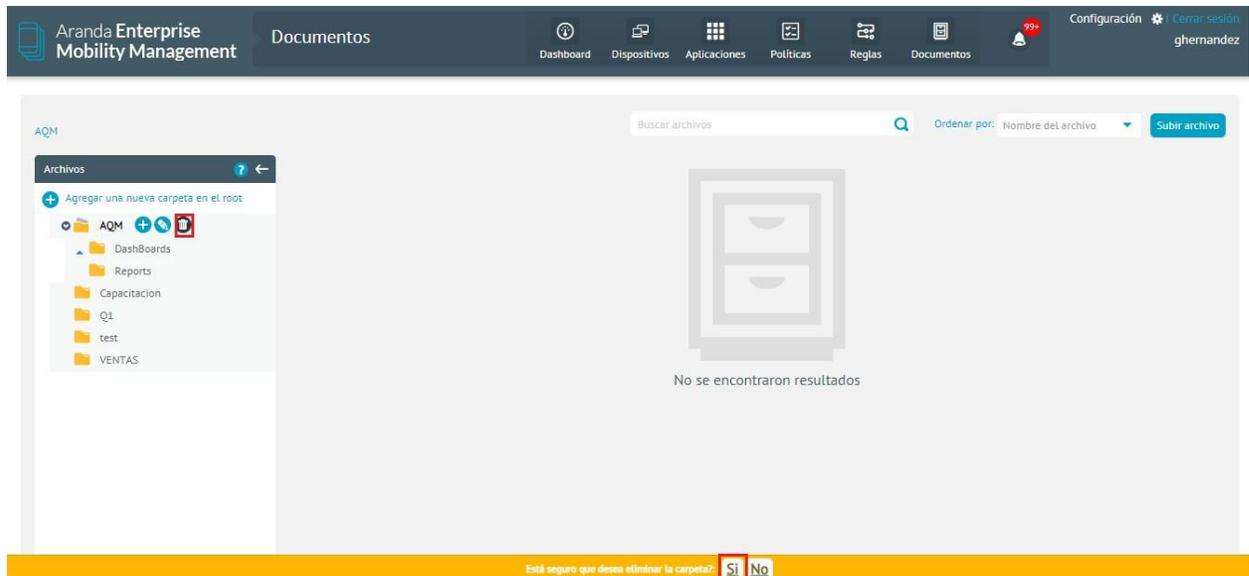


11.2. Edición y eliminación de carpetas

Para editar una carpeta de clic en el icono de **editar**, luego observará una pantalla en donde debe ingresar el nuevo nombre de la carpeta y posteriormente dar clic en **Guardar**.

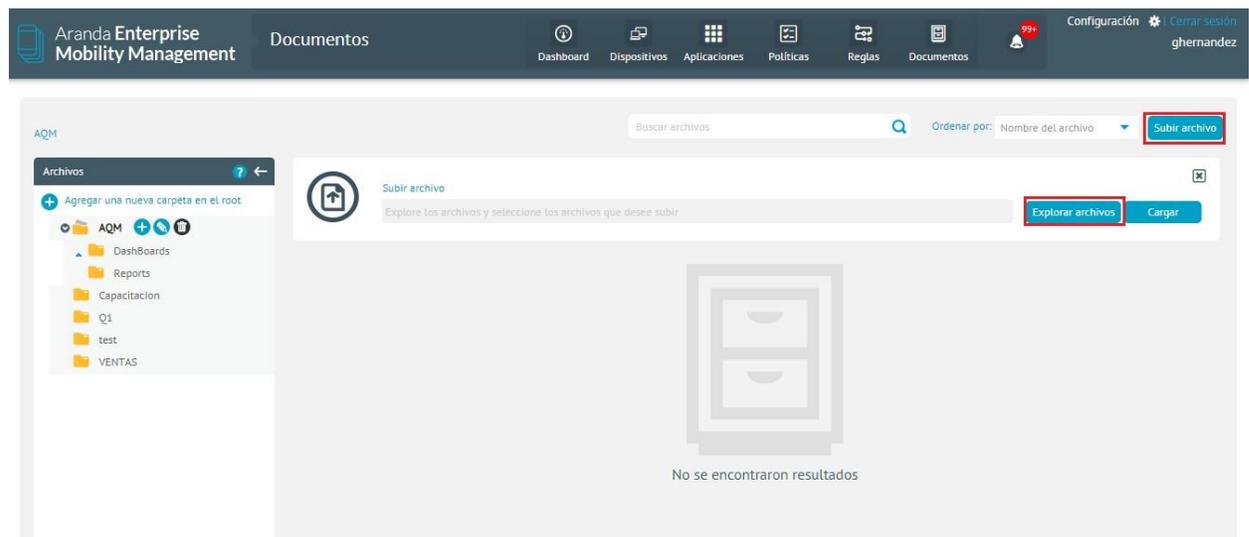


Para eliminar una carpeta de clic en el icono de **eliminar**, Luego aparecerá una ventana emergente en donde se solicita confirmar la eliminación, allí debe confirmar la eliminación de la carpeta que se eliminará siempre y cuando no contenga ni archivos ni sub-carpetas dentro de ella.

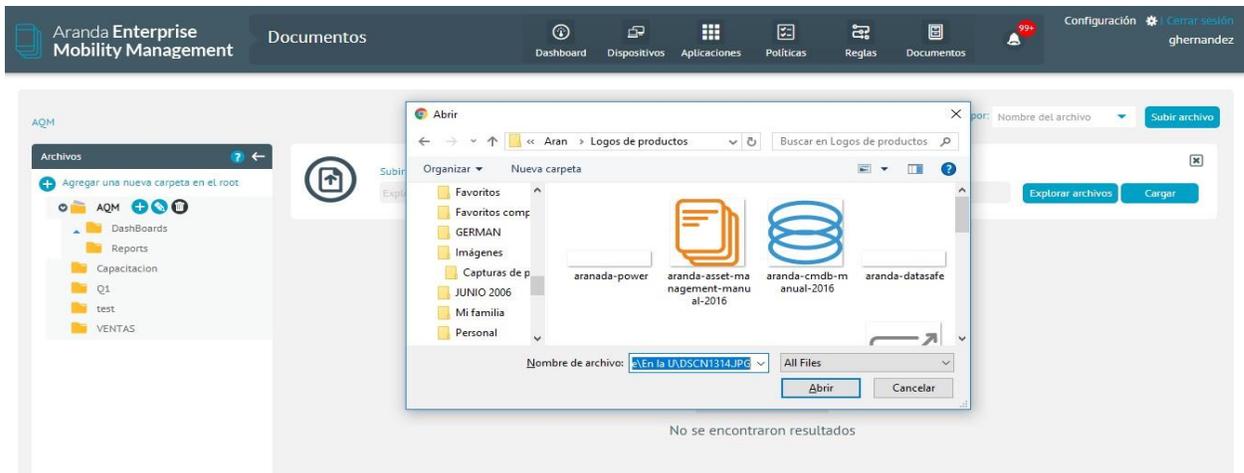


11.3. Agregar Archivos

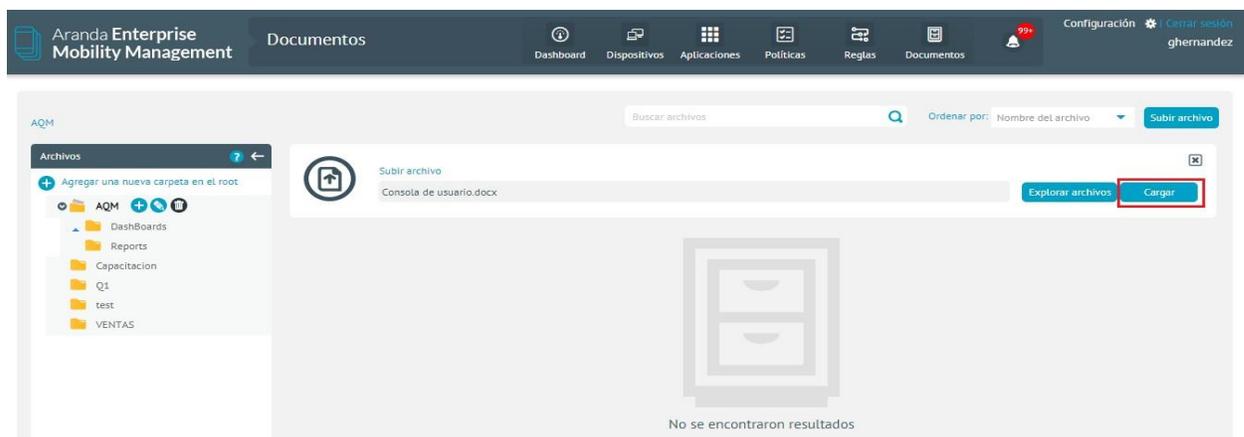
Para agregar archivos de clic en **subir archivo** y posteriormente en **Explorar archivos**.



Se observa una ventana en la cual se debe buscar y seleccionar los archivos que desea subir, una vez seleccionados de clic en **Abrir**.



Visualizará la cantidad de archivos que se seleccionaron, y luego dar clic en cargar.

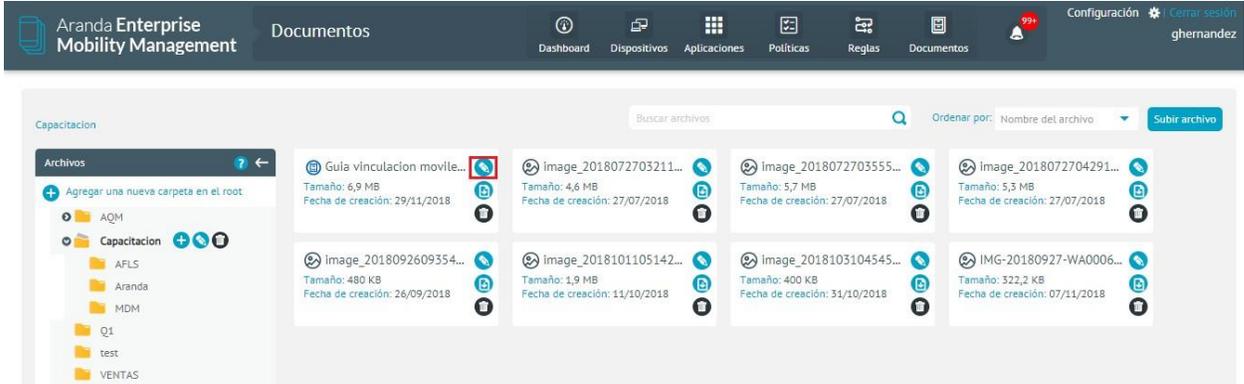


La subida de archivos a una carpeta específica también se puede realizar por medio de drag and drop. En este caso se debe ubicar el archivo que desea subir y a través de un clic sostenido llevarlo hasta la carpeta en la cual se desea cargar.

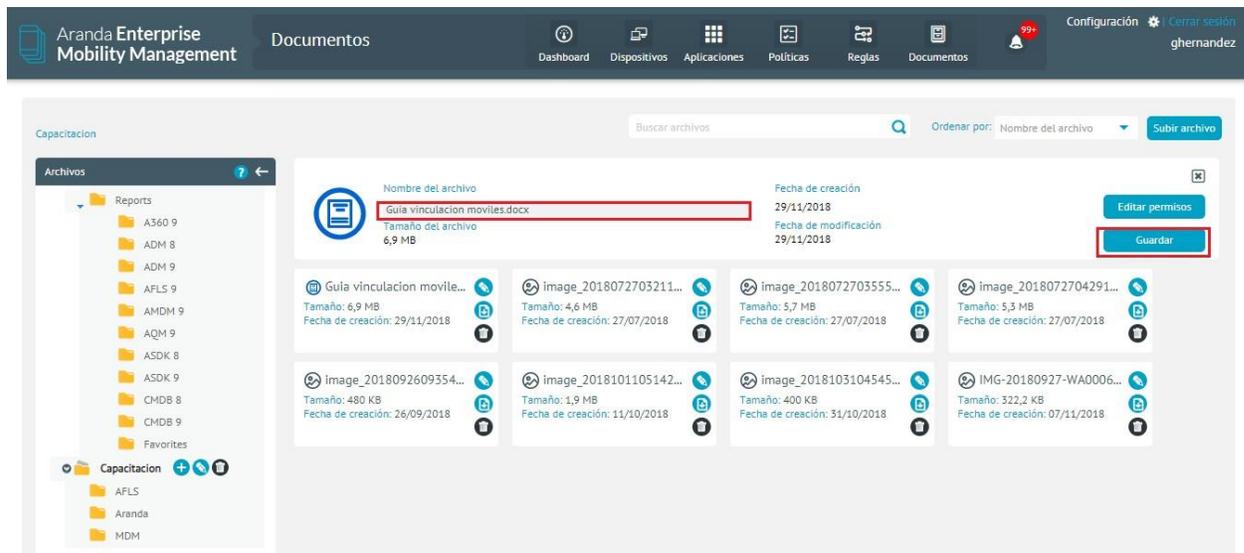


11.4. Editar, Descargar y Eliminar Archivos

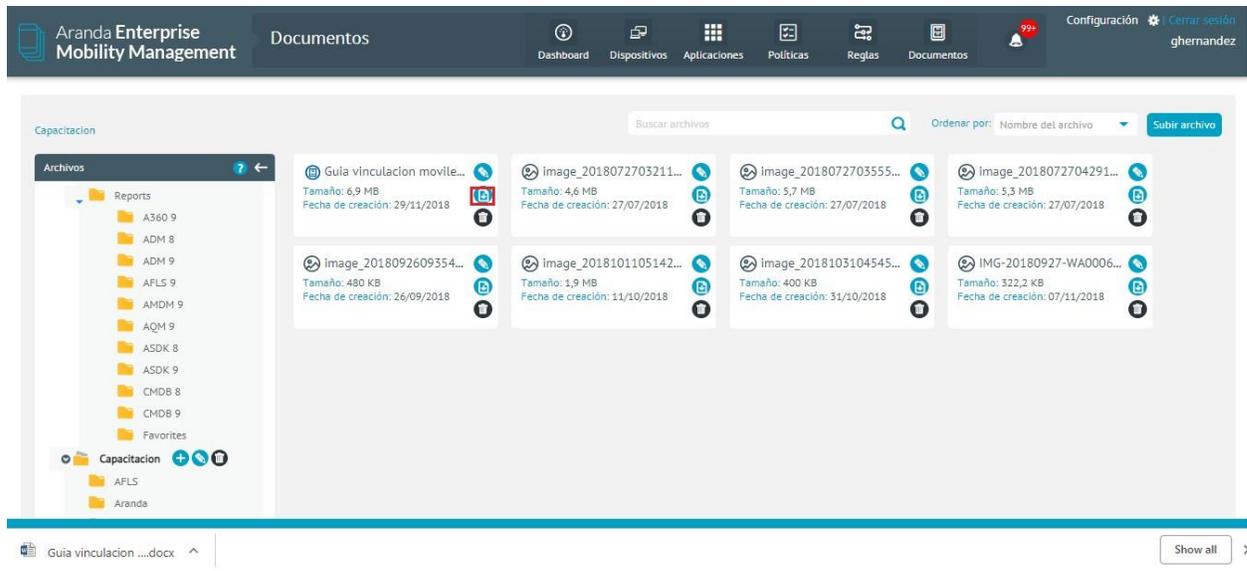
Para editar un archivo se debe seleccionar el icono **editar** en el archivo a modificar.



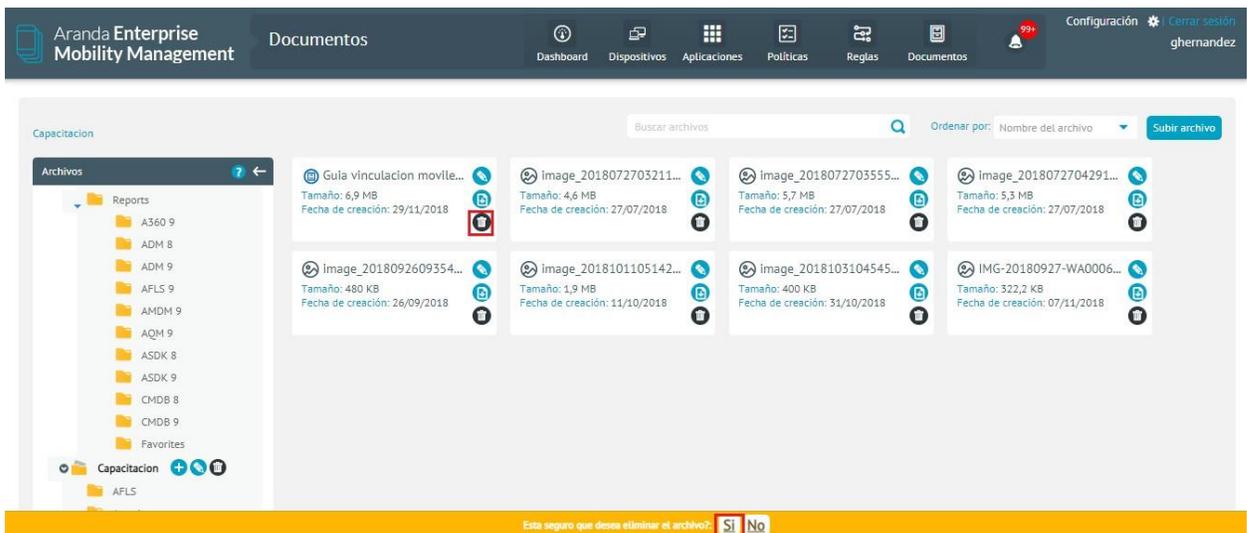
Ingrese el nuevo nombre del archivo y de clic en **Guardar**.



Para descargar un archivo seleccione el icono descargar sobre el archivo que desea visualizar.



Para eliminar un archivo de clic en el icono **eliminar**, Seguido de esto se muestra una ventana emergente en donde se solicita confirmar la eliminación, posterior a esto se debe confirmar la eliminación.



11.5. Administración de permisos

En la sección de documentos hay tres roles; CMReader, CMPublisher, CMManager.

- CMReader: Solo permite la lectura de contenido.
- CMPublisher: Permite lectura, edición y cargue de contenido, además de asignar permisos de Reader o Publisher sobre los contenidos a los que tenga acceso.
- CMManager: Permite lectura, edición, cargue y eliminación, además de la administración de permisos sobre los contenidos.

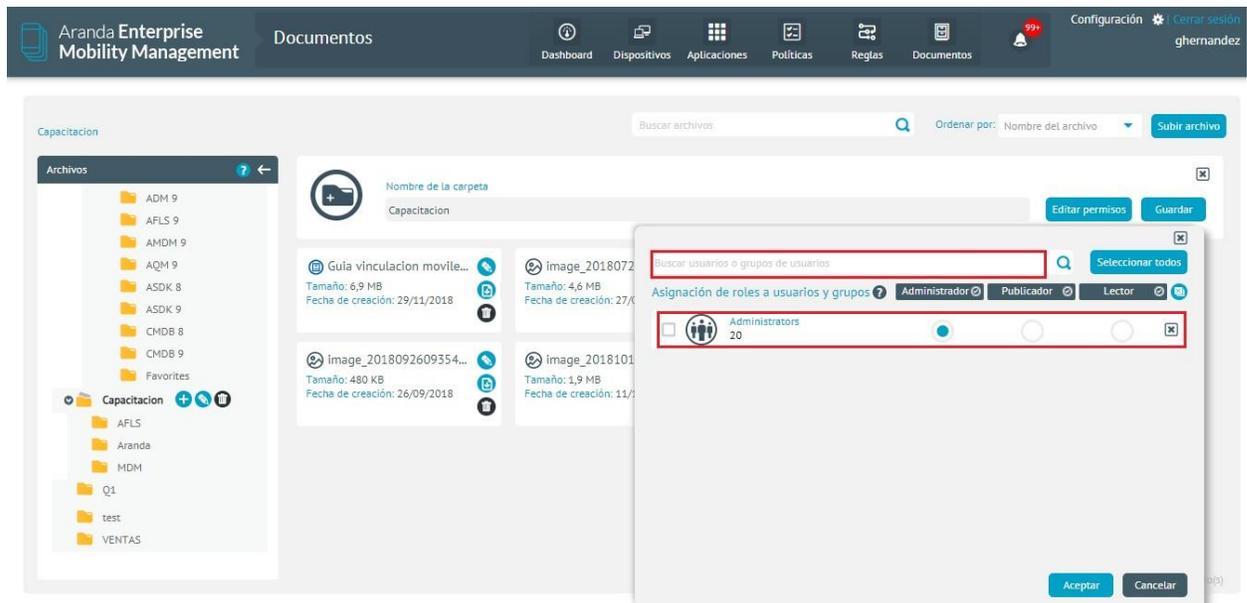
Se debe tener en cuenta que si se asignan roles sobre una carpeta específica dichos roles serán heredados por los archivos que se encuentren en ella mas no por las carpetas.

The screenshot shows the 'Usuarios' (Users) management interface. On the left, there is a sidebar with navigation options like 'Administración', 'Integración empresarial', 'Usuarios', 'Grupos', etc. The main area displays a list of users with details such as name, email, phone, and status. On the right, the 'Roles' tab is active, showing a grid of roles. The role 'App Catalog Manager' is highlighted with a red box. At the bottom of the roles grid, there are 'Guardar' (Save) and 'Cancelar' (Cancel) buttons.

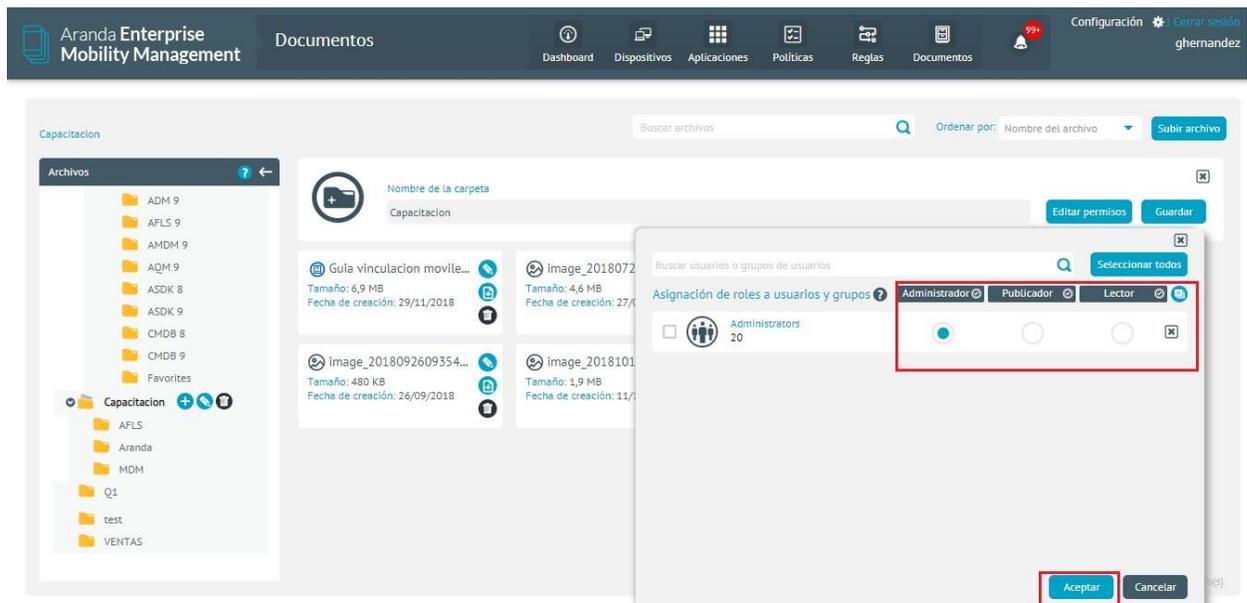
Para agregar un permiso sobre una carpeta específica seleccione el icono **editar** y posteriormente de clic en **Editar permisos**.

The screenshot shows the 'Documentos' (Documents) management interface. The left sidebar shows a file tree with folders like 'Reports', 'A360 9', 'ADM 8', etc., and a folder named 'Capacitacion'. The main area displays a list of files within the 'Capacitacion' folder, including file names, sizes, and creation dates. A red box highlights the 'Editar permisos' (Edit permissions) button for the selected folder. At the bottom right, there are 'Guardar' (Save) and 'Subir archivo' (Upload file) buttons.

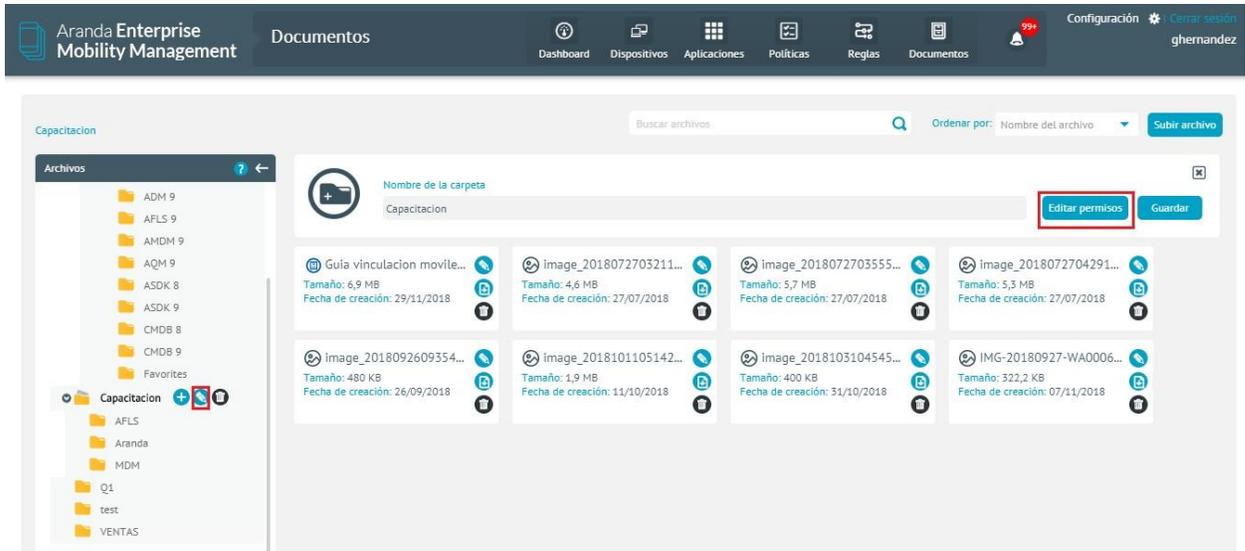
Realice la búsqueda del usuario y selecciónelo dentro de resultados según los criterios de búsqueda ingresados.



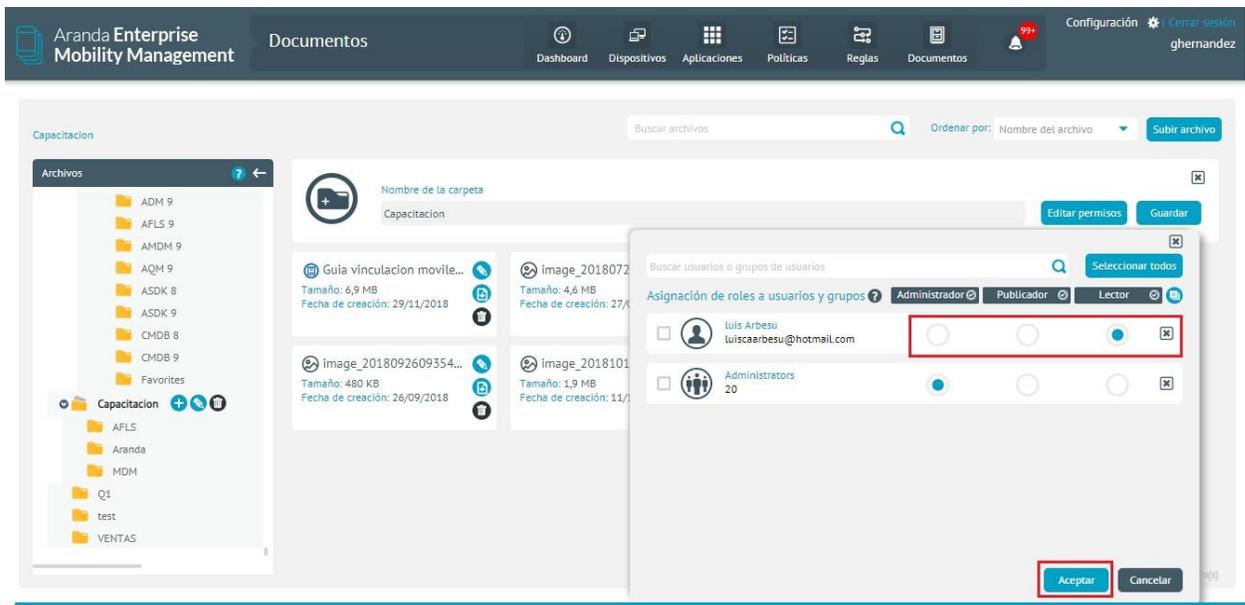
Seleccione el rol que se desea asignar al usuario, de clic en **Aceptar** y finalmente en **Guardar**.



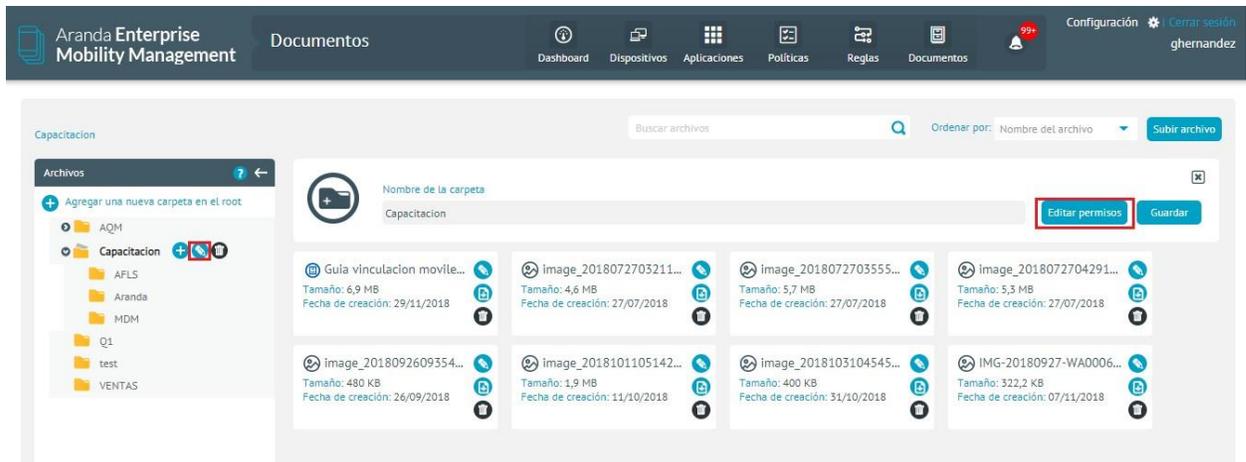
Para editar un permiso sobre una carpeta especifica seleccione el icono **editar** y posteriormente de clic en **Editar permisos**.



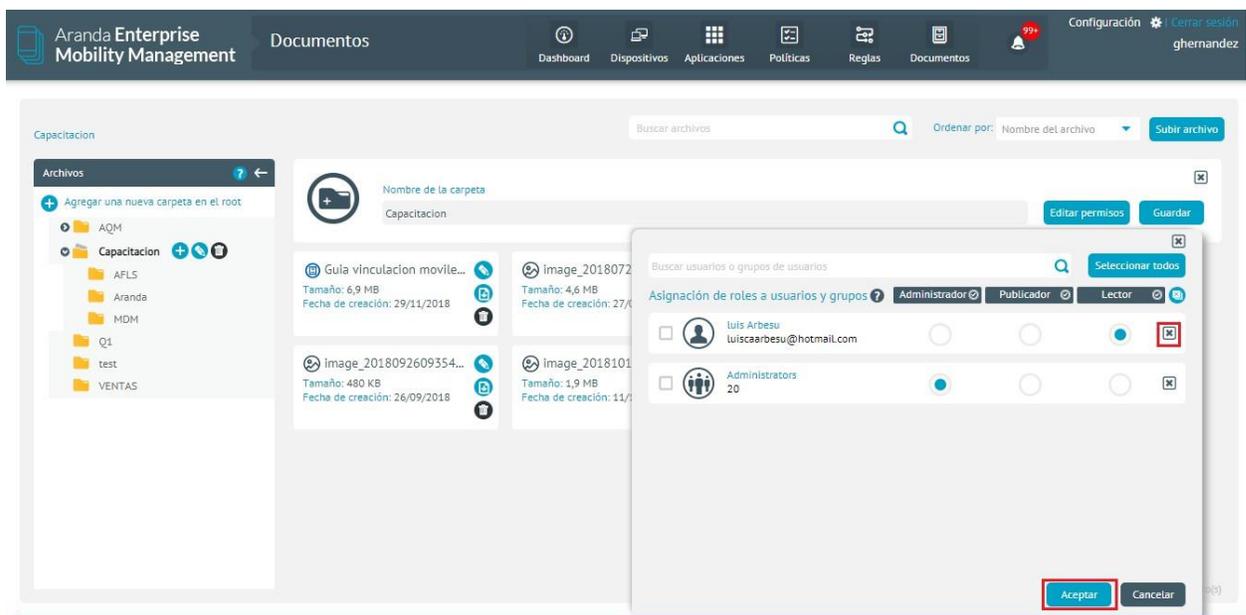
Seleccione el rol nuevo rol que se desea asignar al usuario, de clic en **Aceptar** y finalmente de clic en **Guardar**.



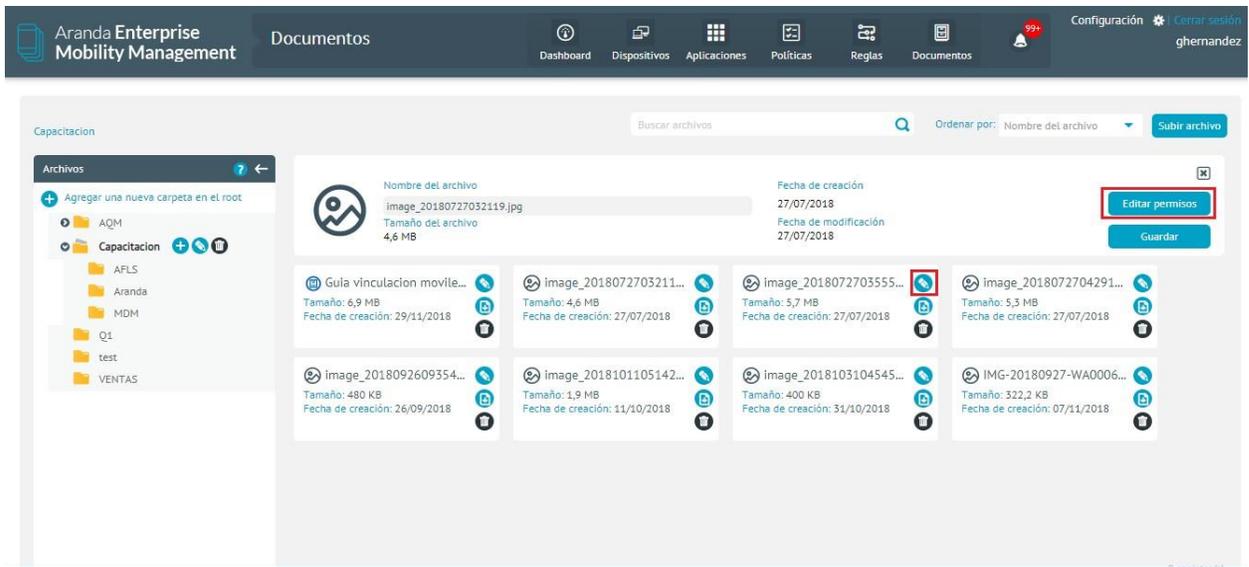
Para quitar un permiso sobre una carpeta especifica seleccione el icono **editar** y posteriormente de clic en **Editar permisos**.



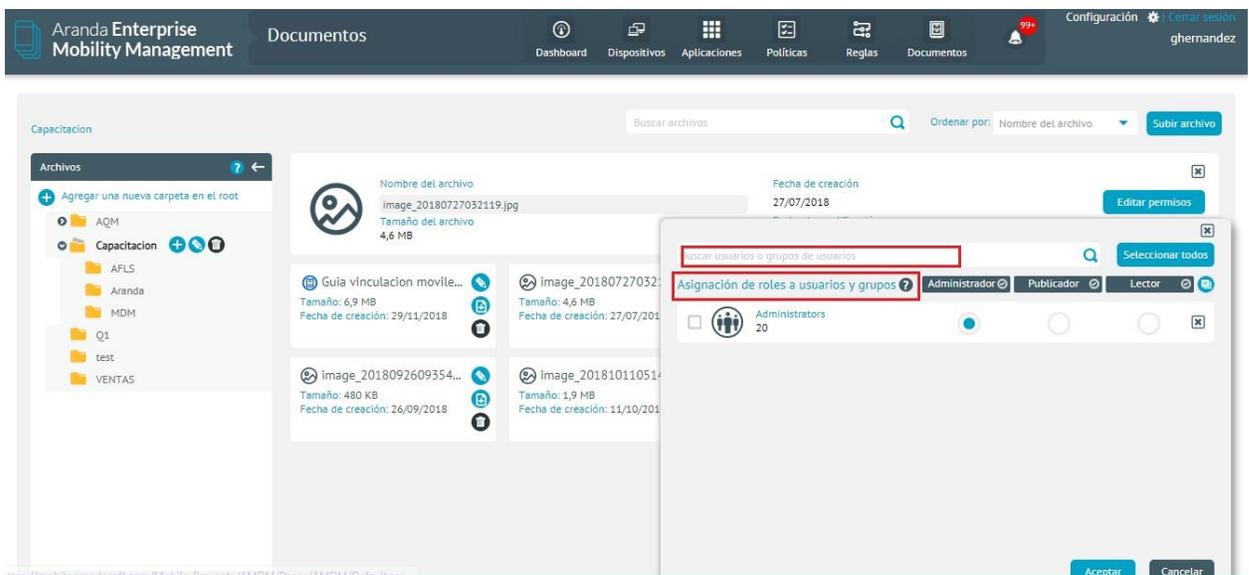
De clic en el icono **eliminar** al usuario que se desea retirar, luego de clic en **Aceptar** y finalmente en **Guardar**.



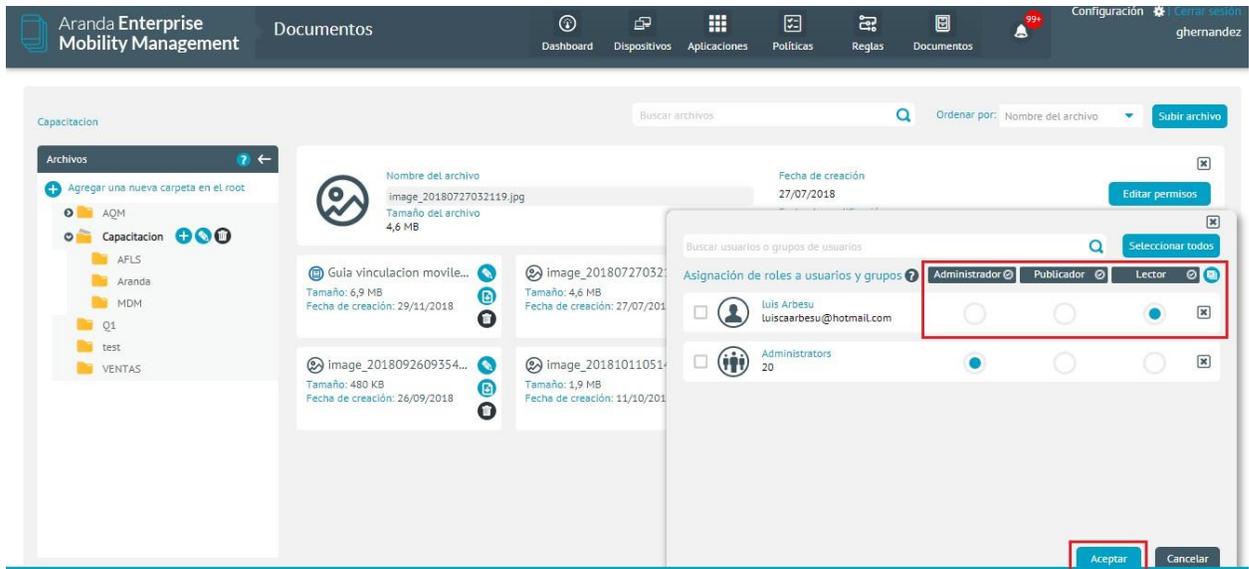
Para agregar un permiso sobre un archivo específico debe seleccionar el icono **editar** y posteriormente hacer clic en **Editar permisos**.



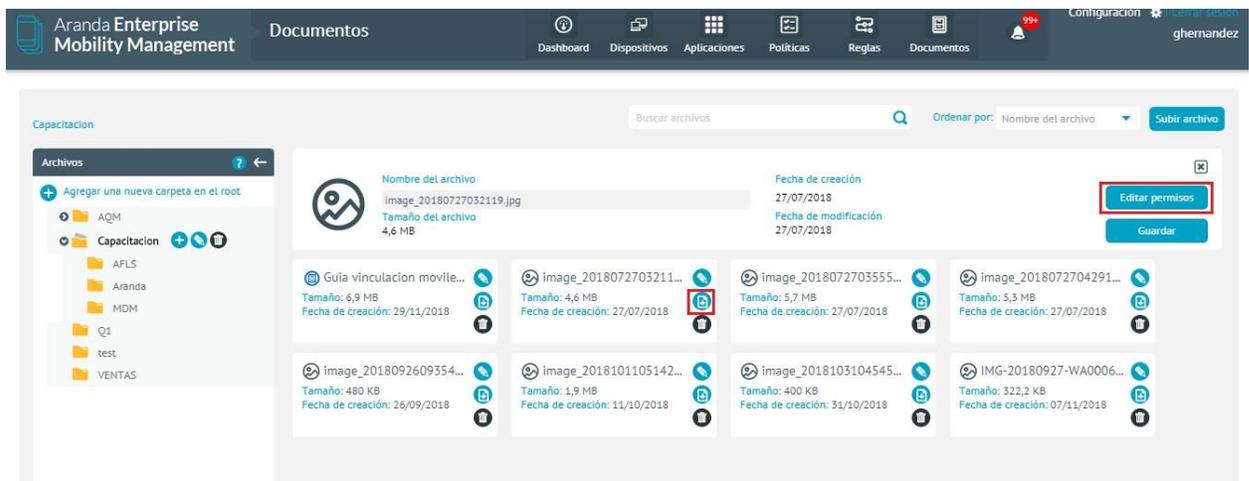
Realice la búsqueda del usuario y selecciónelo dentro de los resultados según los criterios de búsqueda ingresados.



Seleccione el rol que se desea asignar al usuario, de clic en Aceptar y finalmente de clic en **Guardar**.



Para editar un permiso sobre un archivo específico seleccione el icono **editar** y finalmente de clic en **Editar permisos**.



Seleccione el rol nuevo rol que se desea asignar al usuario, de clic en **Aceptar** y finalmente en **Guardar**.

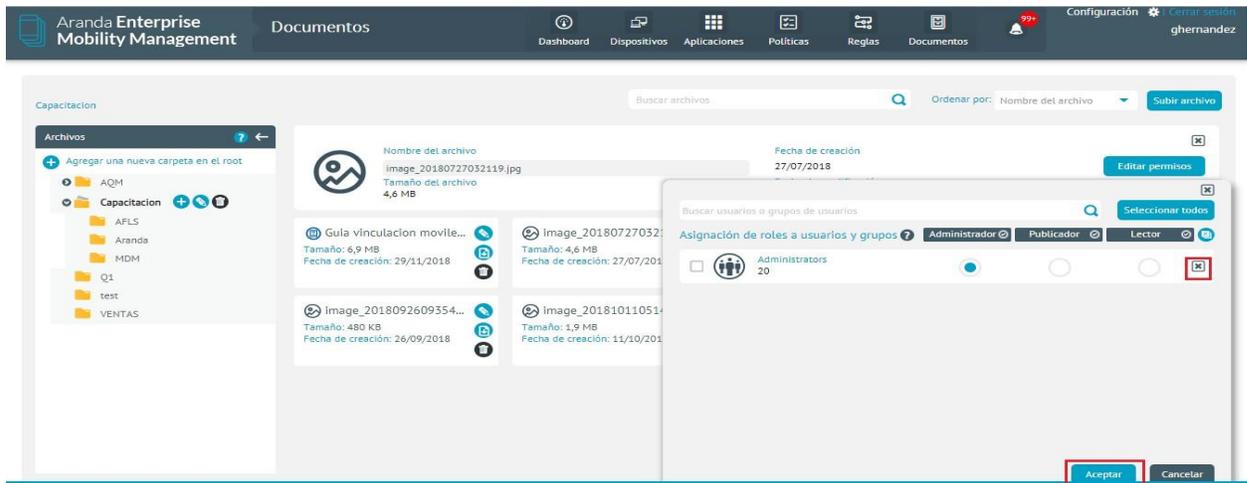
The screenshot shows the 'Aranda Enterprise Mobility Management' interface. The top navigation bar includes 'Documentos', 'Dashboard', 'Dispositivos', 'Aplicaciones', 'Políticas', 'Reglas', 'Documentos', 'Configuración', and 'Cerrar sesión ghemandez'. The main content area is titled 'Capacitación' and displays a list of files. A modal window titled 'Asignación de roles a usuarios y grupos' is open, showing a table of roles and users. The 'Administrators' user is selected, and the 'Lector' role is highlighted with a red box. The 'Aceptar' button at the bottom of the modal is also highlighted with a red box.

Nombre del archivo	Tamaño del archivo	Fecha de creación
image_20180727032119.jpg	4,6 MB	27/07/2018
Guía vinculación móvil...	6,9 MB	29/11/2018
image_2018092609354...	480 KB	26/09/2018
image_2018101105142...	1,9 MB	11/10/2018
image_2018103104545...	400 KB	31/10/2018
image_2018072703555...	5,7 MB	27/07/2018
image_2018072704291...	5,3 MB	27/07/2018
IMG-20180927-WA0006...	322,2 KB	07/11/2018

Para quitar un permiso sobre un archivo específico, seleccione el icono **editar** y posteriormente de clic en **Editar permisos**.

The screenshot shows the 'Aranda Enterprise Mobility Management' interface after editing permissions. The 'Capacitación' folder is selected in the left sidebar. The file 'image_20180727032119.jpg' is highlighted. The 'Editar permisos' button is highlighted with a red box. The 'Guardar' button is also visible.

De clic en el icono eliminar en el usuario que se desea retirar, y luego de clic en **Aceptar** y finalmente en **Guardar**.



12.ALERTAS

Las alertas son una lista de mensajes tipo notificación que se presentan en la consola. Listado y pre visualización. Para visualizar el resumen de las alertas en la consola, se debe poner el puntero de mouse sobre el icono de **alertas** ubicado en la parte superior del menú.

Dispositivos

Alertas por nivel de severidad

Nivel de Severidad	Cantidad
Crítica	99+
Alta	0
Media	0
Baja	47

Para visualizar las alertas de forma detallada, seleccione el ícono de alertas, o cualquiera de las opciones que presenta la vista emergente con el resumen de las alertas, de esta forma se puede ver el detalle de las alertas filtradas por su severidad o ver todas las alertas.

Alertas

Estado de la alerta

Nueva • Revisada • Cerrada

Detalle de la alerta

Saliendo de aranda

Comentarios anteriores

No hay comentarios

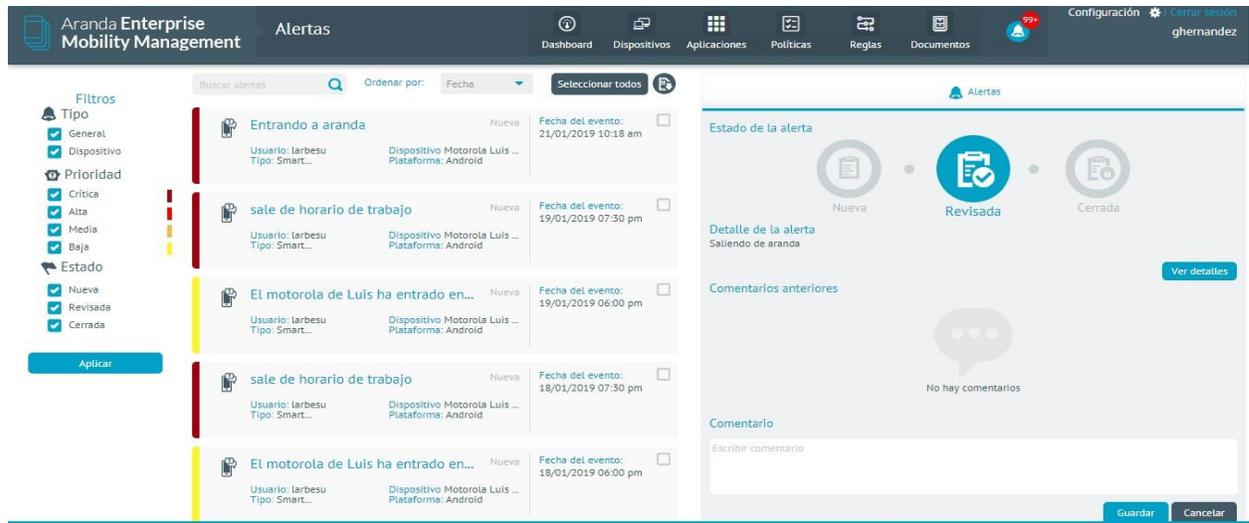
12.1. Generación y manejo de alertas

Las alertas son una de las acciones que se pueden definir para el cumplimiento de una regla, cuando se define un conjunto de reglas y esta(s) se cumple(n) el sistema dispara las acciones determinadas, en este caso generaría alertas que se visualizan en la consola.

Al seleccionar una alerta de la lista, en el costado derecho se ve el detalle de esta con opciones para edición. Se manejan tipos de estado para la alerta:

- Nueva
- Revisada
- Cerrada

Además, se puede ver el detalle del dispositivo asociado a la alerta y agregar comentarios a esta.



13.CONTENT MANAGEMENT PARA ANDROID

Aranda EMM Content Management provee una forma intuitiva de acceder y ver documentos almacenados por medio de la sección de documentos de la consola de administración de AEMM o directamente desde el Content Management. Ayuda a proteger su contenido sensible en un contenedor corporativo. Permite que usuarios con dispositivos móviles accedan de forma fácil y segura a los documentos requeridos para

su trabajo, ellos pueden compartir de manera sencilla y segura contenido con sus compañeros de trabajo reduciendo el riesgo de comprometer información corporativa. Content Management Para Android.

13.1. Ingreso a la aplicación

Se puede ingresar el servidor de conexión a través de un código QR el cual se escanea de la consola web o se puede ingresar manualmente la dirección web del servidor.



Si selecciona la opción ingresar servidor se muestra el campo para digitarlo, si ha ingresado anteriormente al servidor en la parte superior al campo se muestran los servidores a los que ha ingresado con anterioridad para que no sea necesario ingresarlos nuevamente.



Posteriormente se debe ingresar el usuario y la contraseña de inicio de sesión (Aranda para un usuario local o si tiene integrada la consola a un dominio puede seleccionarlo e ingresar con un usuario y contraseña de red)



Luego acepte los términos y condiciones y presione en **continuar**.



Se muestra a nivel información de la aplicación, pulse **saltar**.



13.2. Visualización general

Ingresa al menú en los tres puntos de la barra de opciones ubicados en la parte superior derecha, allí observará los archivos en dos formas de visualización.

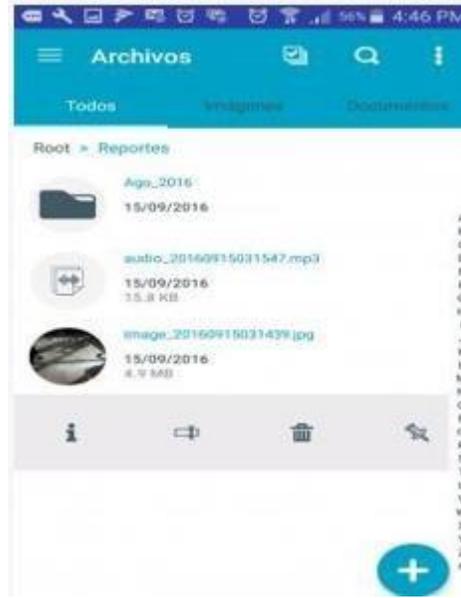
En modo lista



Visualización de grilla.



Realizando Swipe hacia la izquierda sobre un archivo, visualizará las opciones Información, renombrar, Eliminar y Marcar como favorito (Descargar archivo para consultarlo sin conexión).



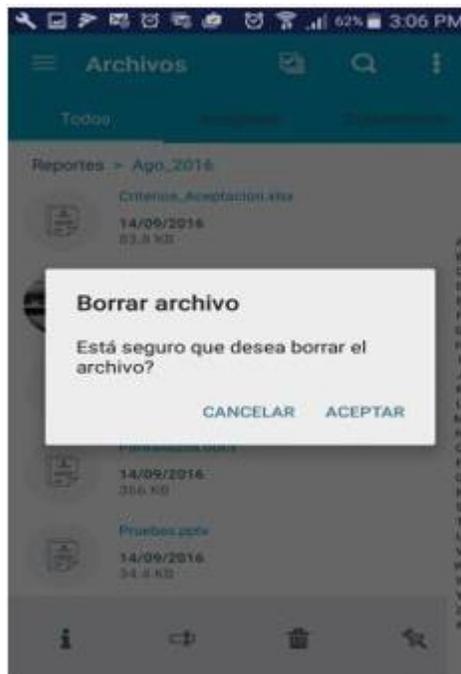
Información del archivo, para salir pulse fuera del cuadro de información.



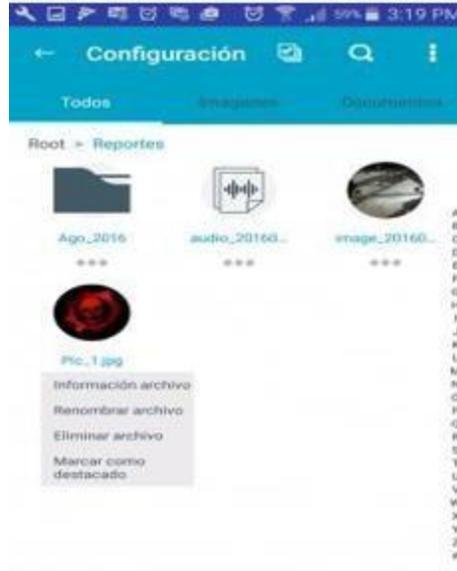
Para renombrar el archivo ingrese el nuevo nombre y presione en **guardar**.



Para borrar el archivo presione en **Aceptar**.



En vista de grilla puede acceder a las opciones de los archivos pulsando sobre los puntos ubicados en la parte inferior del archivo.



13.3. Menú de vistas

Cuenta con las vistas de Archivos (Visualización de todos los archivos y carpetas), Favoritos, Descargas, Configuración. Se puede ingresar a este menú realizando un Swipe al hacia la derecha o pulsando el icono de tres líneas en la parte superior izquierda.



Favoritos, Visualización de archivos marcados como favoritos.



Descargas, Visualización de descargas realizadas.



Configuración, Se puede seleccionar si desea la visualización de archivos conectado a los datos móviles o solo cuando se encuentra conectado a una red Wifi.



Desplace el selector según la configuración deseada.

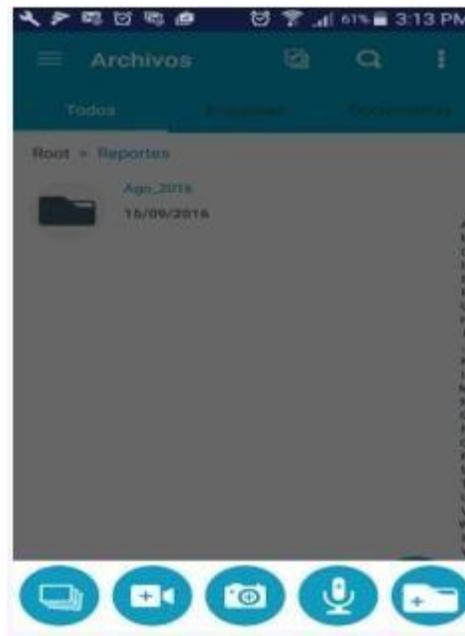


13.4. Subir archivos

Para subir un archivo pulse en el icono “+”



Posteriormente seleccione el tipo de archivo que desea subir.



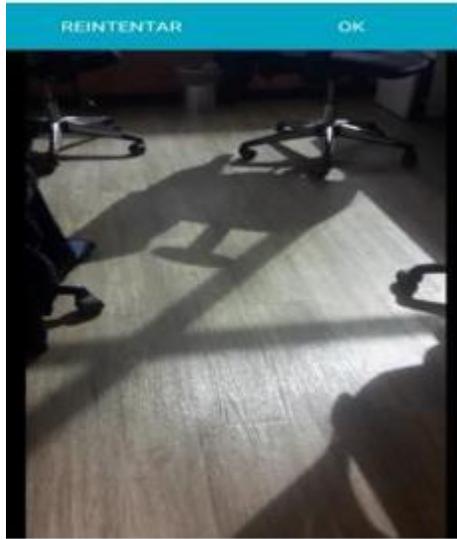
Para subir una imagen debe seleccionar el origen



Al seleccionar la imagen se muestra un mensaje informando el inicio y final del cargue.



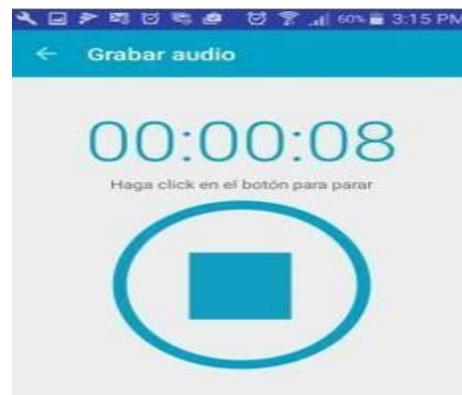
Para subir foto y/o vídeo debe realizar la captura y pulsar en **Ok** (según el móvil se puede tardar uno o dos segundos mientras carga la imagen).



Para subir un audio debe pulsar en el icono de micrófono para iniciar la grabación



Posteriormente debe pulsar en el icono stop para finalizarla.



Se visualiza un control para reproducir el audio, adelantarlo, atrasarlo, subirlo (Icono de nube) o descartarlo (Icono de caneca).



13.5. Controles de la barra de opciones

Puede realizar búsquedas de archivos pulsando el icono de lupa en la barra de opciones de la aplicación y posteriormente ingresando el criterio de búsqueda.



Con base en el criterio ingresado se visualizarán los archivos existentes en todas las carpetas.



Puede realizar una selección múltiple de archivos para eliminar o descargar en forma masiva con los controles habilitados en la barra de opciones.



13.6. Filtros

Puede refinar la visualización de archivos por medio de las opciones de las pestañas ubicadas debajo de la barra de opciones, pulsando imágenes.



Pulsando documentos se visualizan los archivos en formato Word, Excel, PowerPoint y Pdf.



14. CONTENT MANAGEMENT PARA IOS

Se puede ingresar el servidor de conexión a través de un código QR el cual se escanea de la consola web o se puede ingresar manualmente la dirección del servidor.



Si selecciona la opción ingresar servidor se muestra el campo para digitarlo, si ha ingresado anteriormente al servidor en la parte superior al campo se muestran los servidores a los que ha ingresado con anterioridad para que no sea necesario ingresarlos nuevamente.



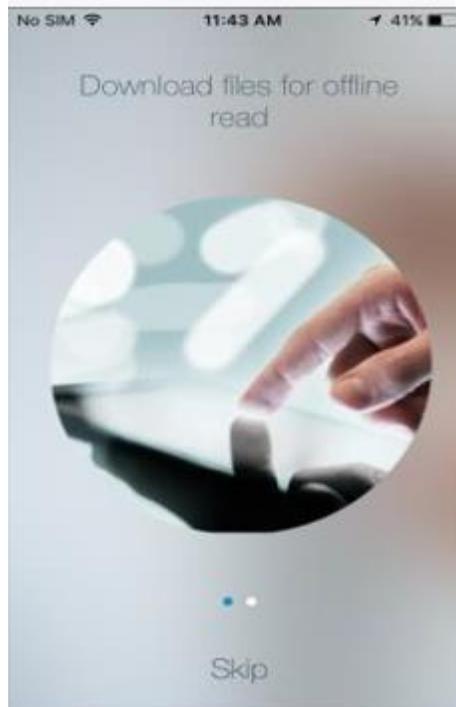
Posteriormente se debe ingresar el usuario y la contraseña de inicio de sesión (Aranda para un usuario local o si tiene integrada la consola a un dominio puede seleccionarlo e ingresar con un usuario y contraseña de red).



Luego acepte los términos y condiciones y pulse en **continuar**.

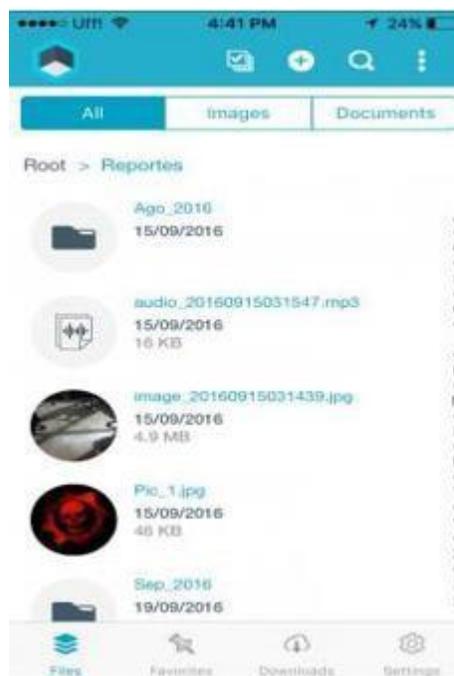


Se muestra a nivel información de la aplicación, pulse en saltar.

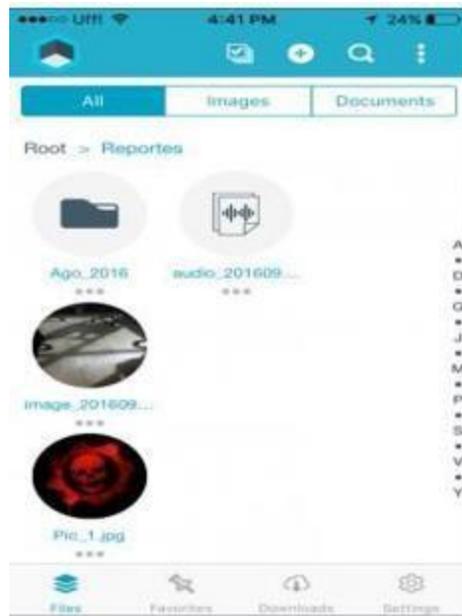


14.1. Visualización general

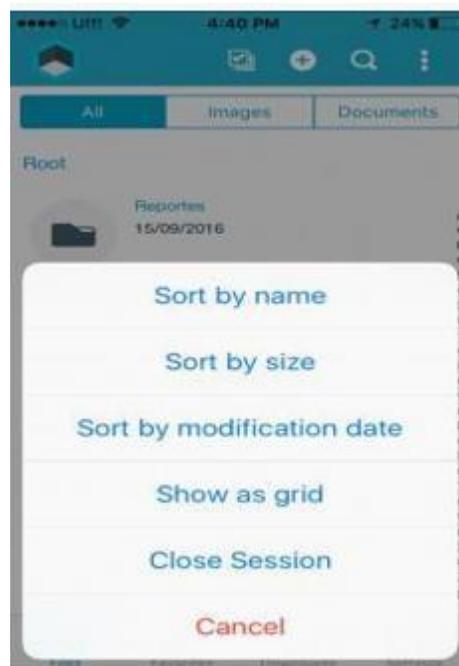
Puede visualizar los archivos en dos formas de visualización, en modo lista.



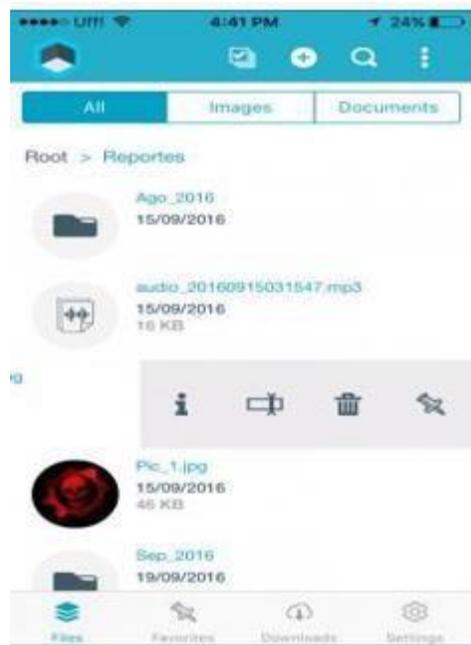
O en visualización de grilla.



Seleccione las visualizaciones ingresando al menú con los tres puntos de la barra de opciones en la parte superior derecha.



Realizando Swipe hacia la izquierda sobre un archivo visualice las opciones Información, renombrar, Eliminar y Marcar como favorito (Descargar archivo para consultarlo sin conexión).



Información del archivo, para salir puede pulsar fuera del cuadro de información.

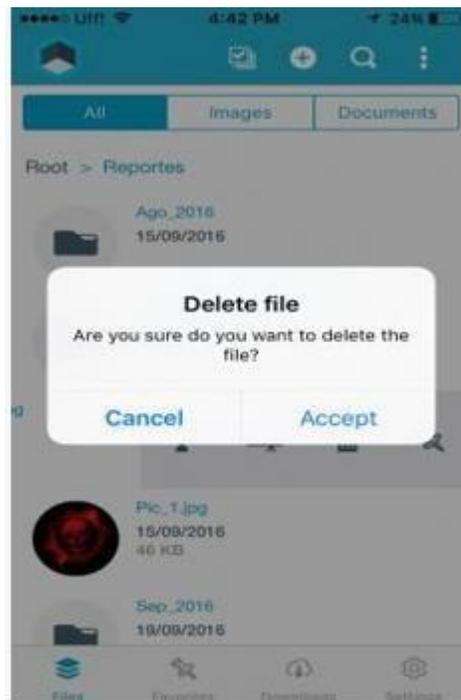


Para renombrar archivo ingrese el nuevo nombre y pulse **guardar**.

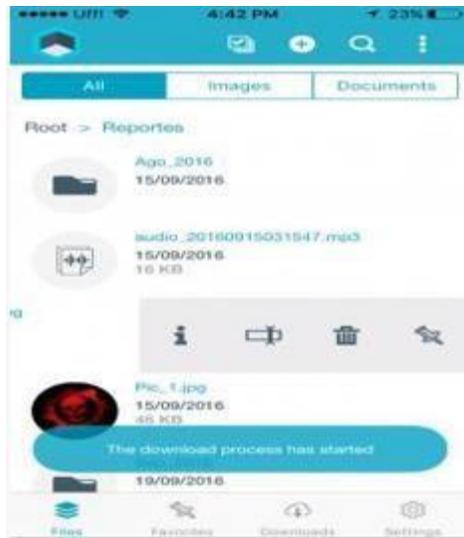


Para

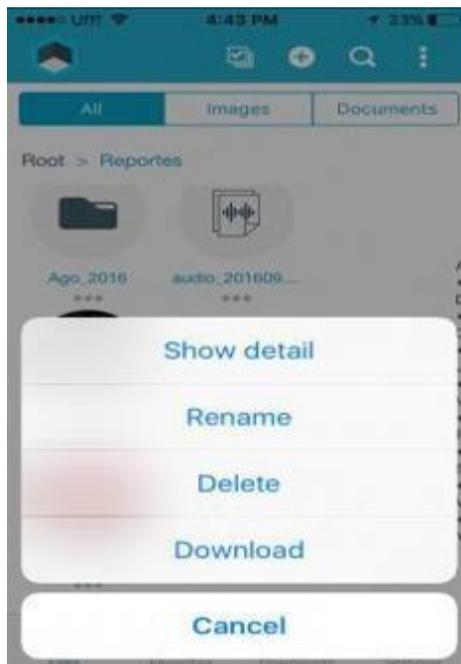
borrar el archivo pulse **aceptar**.



Para marcar un archivo como favorito debe pulsar en el icono de pin y se mostrara un mensaje indicando el proceso de inicio y fin de descarga de dicho archivo.



En vista de grilla puede acceder a las opciones de los archivos pulsando sobre los puntos ubicados en la parte inferior del archivo.



14.2. Menú de vistas

Cuenta con las vistas Archivos (Visualización de todos los archivos y carpetas), Favoritos, Descargas, Configuración. Este menú se encuentra visible en la barra de opciones ubicada en la parte inferior de la pantalla.



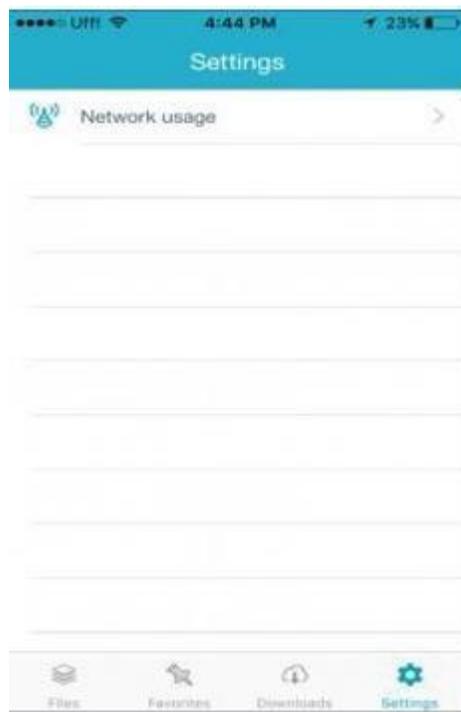
Favoritos, Visualización de archivos marcados como favoritos.



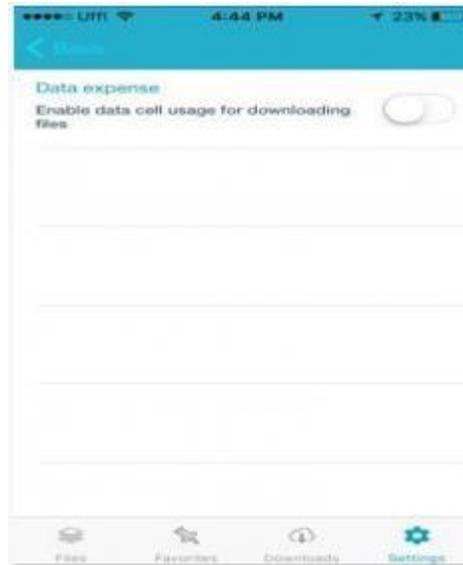
Descargas, Visualización de descargas realizadas.



Configuración, Se puede seleccionar si se desea la visualización de archivos con datos móviles o solo cuando se encuentra conectado a una red Wifi.

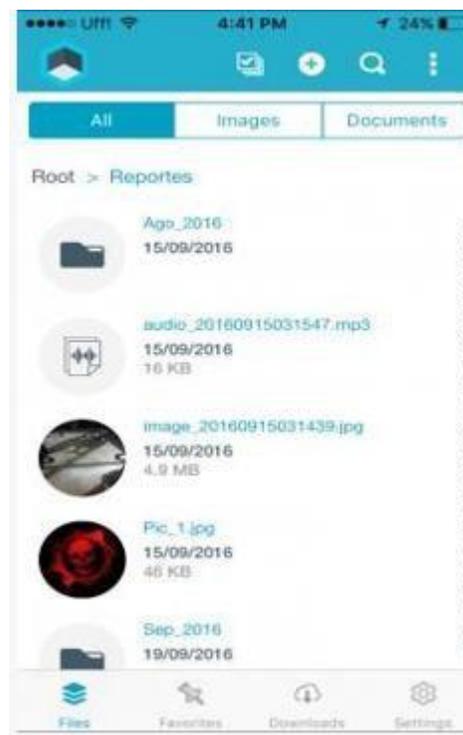


Desplazar el selector según la configuración deseada.

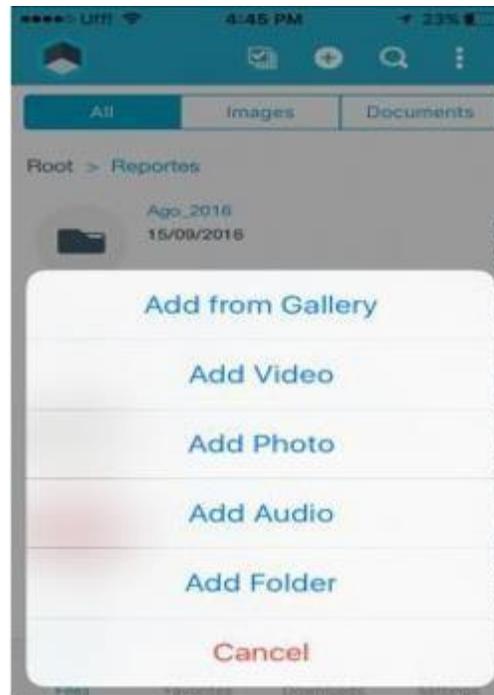


14.3. Subir archivos

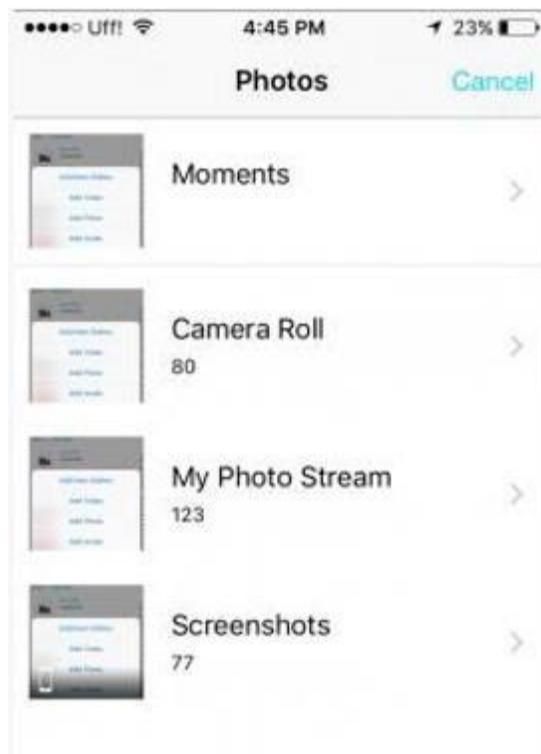
Para subir un archivo debe pulsar en el icono “+” ubicado en la barra de opciones.



Posteriormente seleccione el tipo de archivo que desea subir.



Para subir una imagen debe seleccionar el origen.



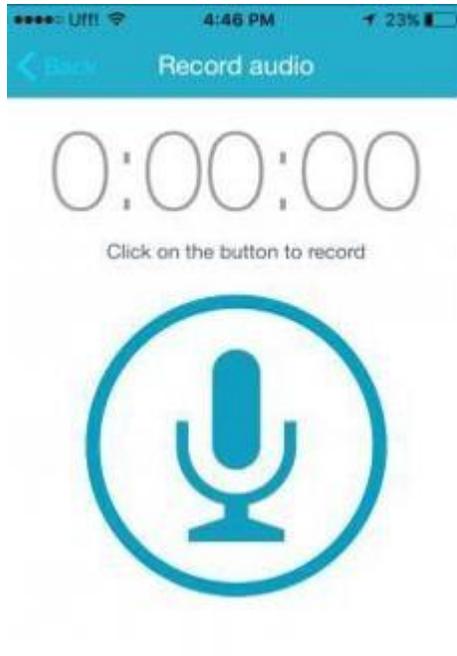
Al seleccionar la imagen se muestra un mensaje informado el inicio y final del cargue.



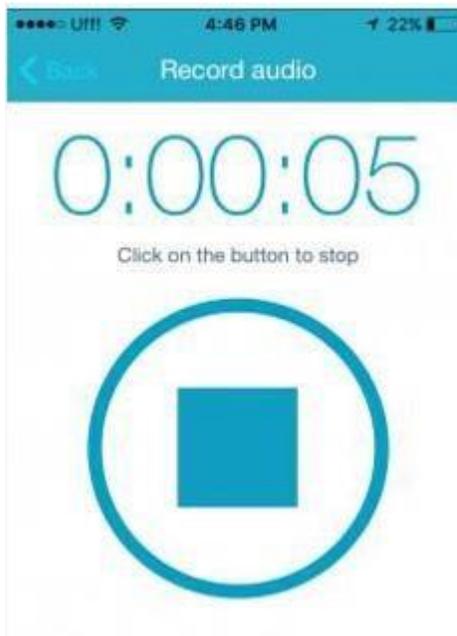
Para subir una foto y/o vídeo debe realizar la captura y pulsar en **Ok**.



Para subir un audio debe pulsar en el icono de micrófono para iniciar la grabación.



Posteriormente debe pulsar en el icono stop para finalizarla.

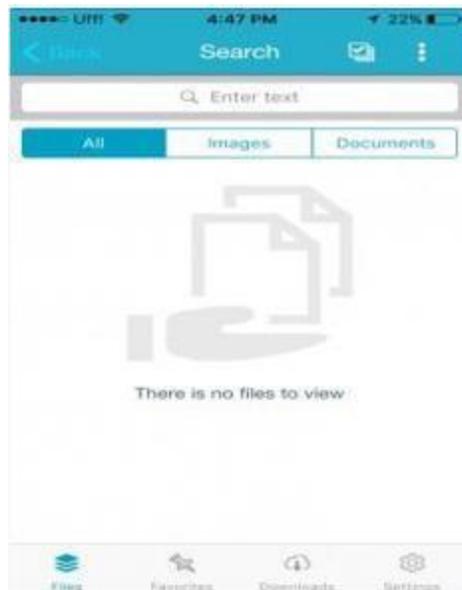


Se visualiza un control para reproducir el audio, adelantar, atrasarlo, subirlo (Icono de nube) o descartarlo (Icono de caneca).



14.4. Controles de la barra de opciones

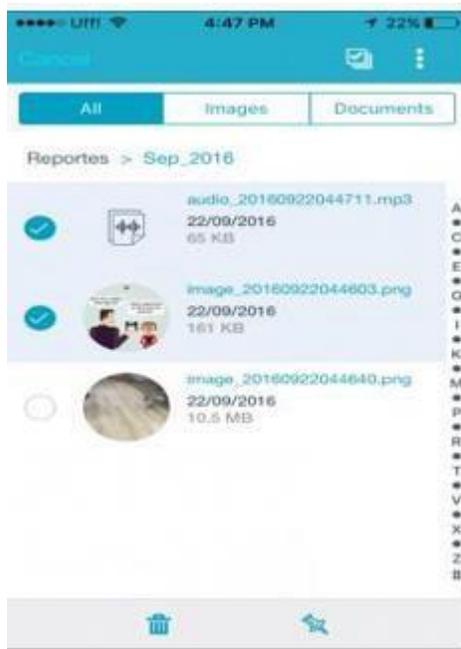
Puede realizar búsquedas de archivos pulsando el icono de lupa en la barra de opciones de la aplicación y posteriormente ingresando el criterio de búsqueda.



Con base en el criterio ingresado visualizará los archivos existentes en todas las carpetas.



Puede realizar una selección múltiple de archivos para eliminar o descargar en forma masiva con los controles habilitados en la barra de opciones.



14.5. Filtros

Puede refinar la visualización de archivos por medio de las opciones de la barra segmentada ubicada debajo de la barra de opciones, pulsando imágenes.



Pulsando documentos se visualizarán los archivos en formato Word, Excel, PowerPoint y PDF.

