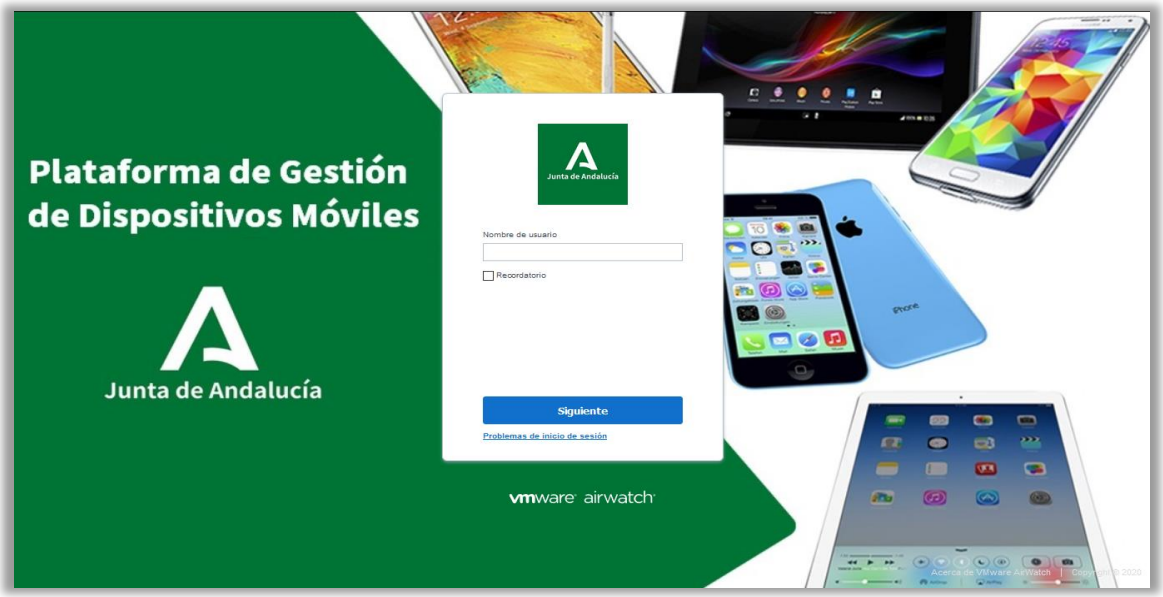
Agencia Digital de Andalucía
Consejería de la Presidencia, Administración Pública e Interior

Manual de usuario

Plataforma de Gestión de Dispositivos Móviles



CONTROL DE CAMBIOS

Fecha	Versión	Autor	Descripción del cambio
21/03/22	1.0	Ignacio Rodríguez Planas	Elaboración inicial del documento

Tabla de contenido

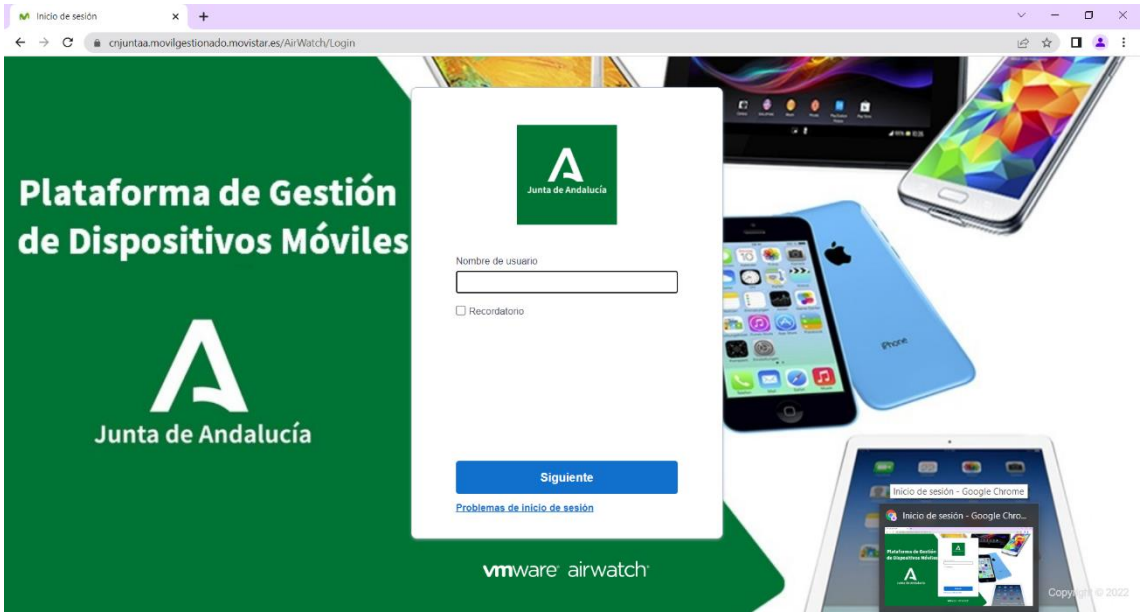
1. Introducción

Este documento describe el manual de uso de la herramienta de Gestión de Dispositivos Móviles (MDM) de la Junta de Andalucía para los administradores de organismo.

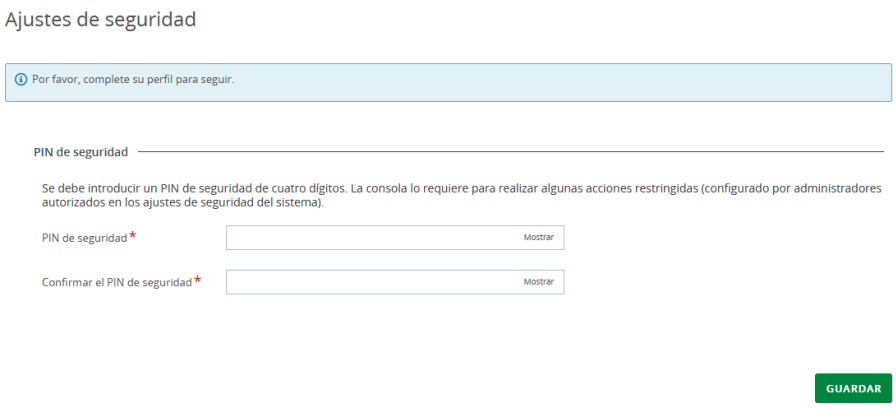
2. Acceso a la plataforma

Para acceder a la plataforma es necesario acceder a la siguiente url: https://cnjuntaa.movilgestionado.movistar.es/

En la pantalla principal se deberá introducir el nombre y usuario LDAP de un usuario administrador de la herramienta:



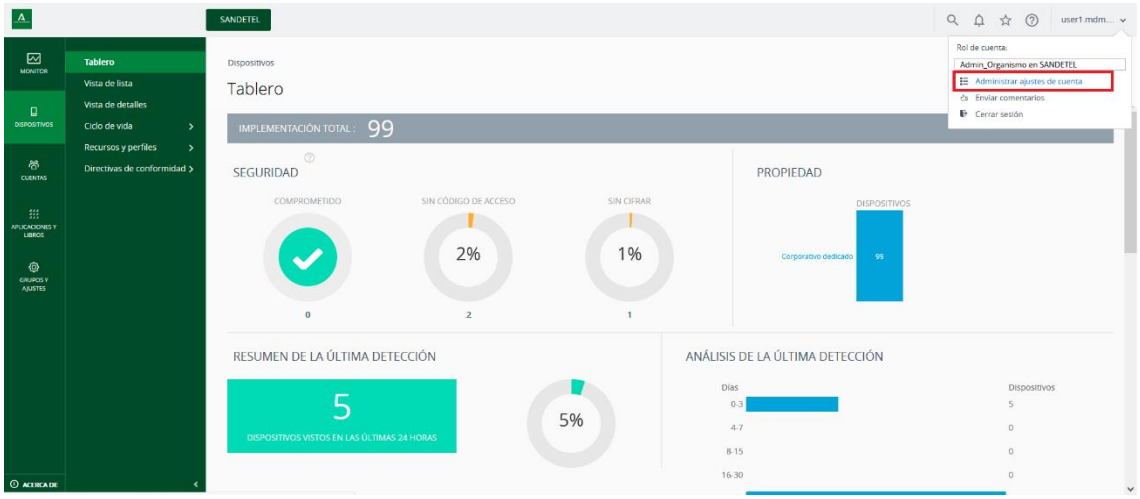
Cuando se realiza el primer acceso como administrador de la herramienta, se solicita que se introduzcan unos ajustes de seguridad asociado a la nueva cuenta de usuario creada. La herramienta solicita que se introduzca un PIN de seguridad de cuatro dígitos:

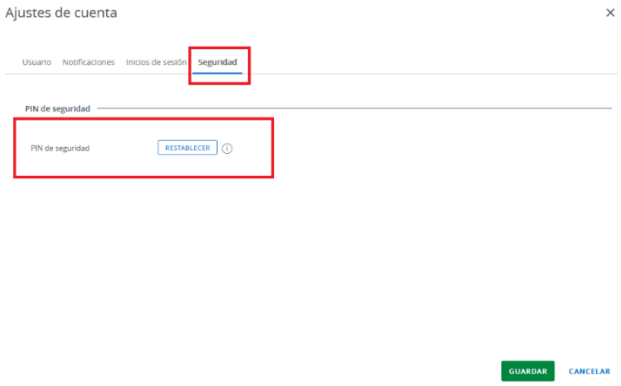


Este PIN es necesario recordarlo pues será necesario para realizar algunas acciones para la gestión de los dispositivos móviles (como por ejemplo, realizar un reset de fábrica de un dispositivo).

2.1. Restablecimiento del PIN de seguridad

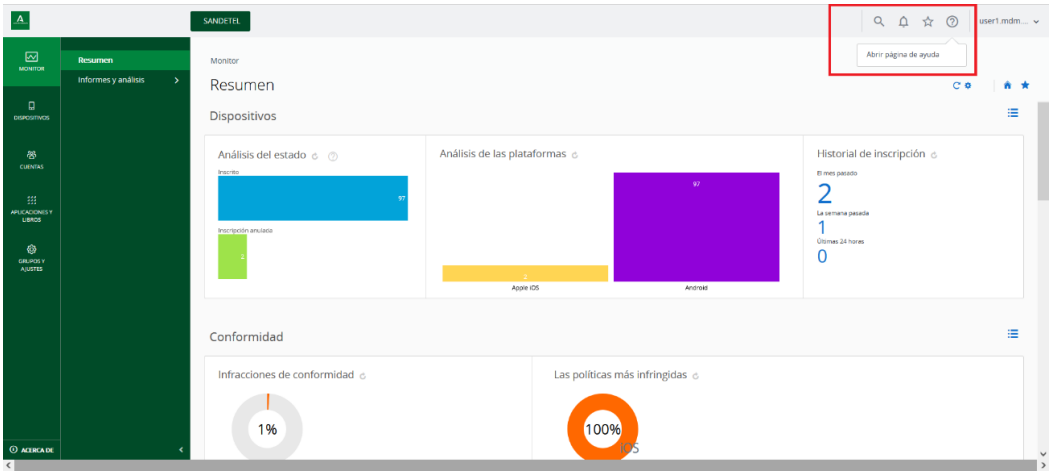
En caso de olvido es posible volver a restablecer y generar un nuevo PIN accediendo a la **administración de los ajustes de la cuenta**, en la pestaña **seguridad**:





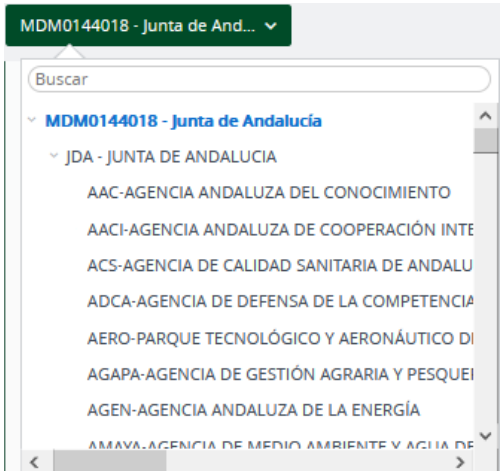
2.2. Menú de ayuda

Para consultar la ayuda que ofrece la herramienta, basta con pulsar en el icono  que aparece en la barra superior de la consola y hacer click en “Abrir la página de ayuda”

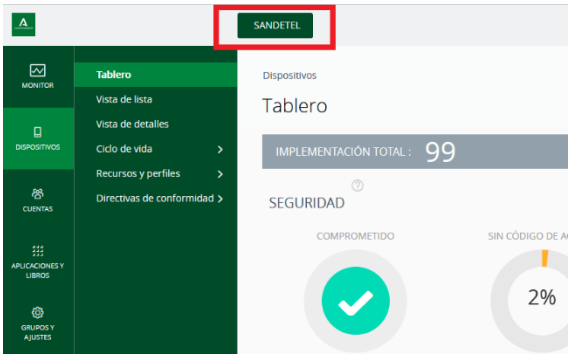


3. Menús principales

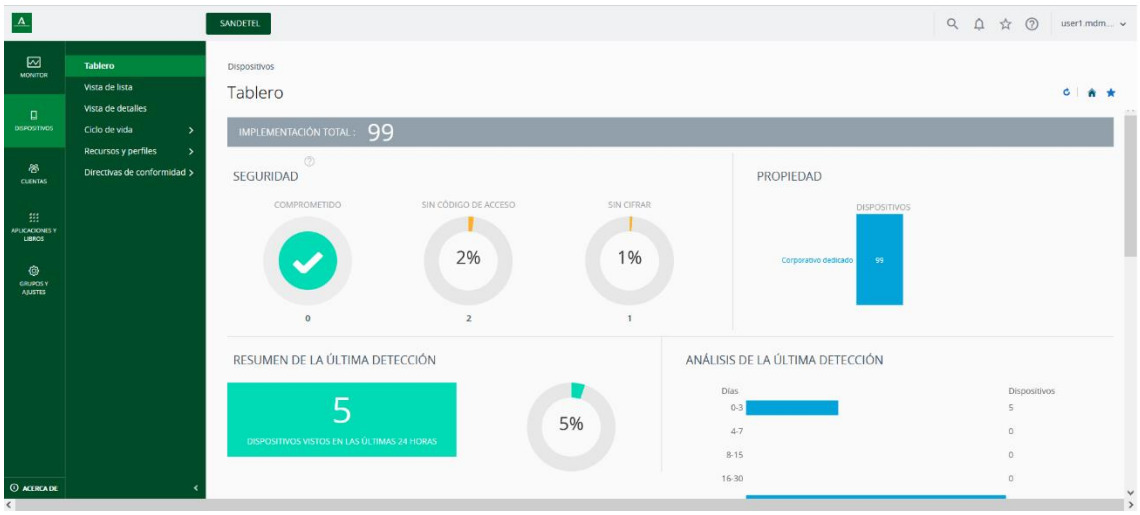
En el momento que se accede a la plataforma, el usuario administrador accede a la pantalla principal de su **grupo organizativo**. Los grupos organizativos son las carpetas en las que está dividido el MDM para toda la Junta de Andalucía. Se pueden entender los grupos organizativos como las ramas de un árbol genealógico. Cada organismo tiene configurado su propio grupo organizativo y solo el Centro de Atención a Usuarios (CAU), el Centro de Operación de Gestión de Telecomunicaciones 24x7 y el personal responsable de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía (RCJA) tienen acceso completo a todos los grupos organizativos configurados.



El grupo organizativo al que accede cada administrador de organismo se visualiza en la barra superior, en el lado izquierdo:



Una vez se accede a la plataforma, nos encontramos con la pantalla principal donde se diferencian 5 tableros: “Monitor”, “Dispositivos”, “Cuentas”, “Aplicaciones y Libros” y “Grupos y Ajustes”:



El tablero “Monitor” es el portal central para obtener acceso rápido a información importante. Gracias a sus coloridos gráficos de barras y circulares, puede identificar rápidamente problemas importantes y actuar desde una única ubicación. También tendrá acceso a revisar los logs asociados a la plataforma y descargar los informes que se generen.

El tablero de “Dispositivos” proporciona una vista de alto nivel de toda la flota y permite realizar acciones en cada dispositivo rápidamente.

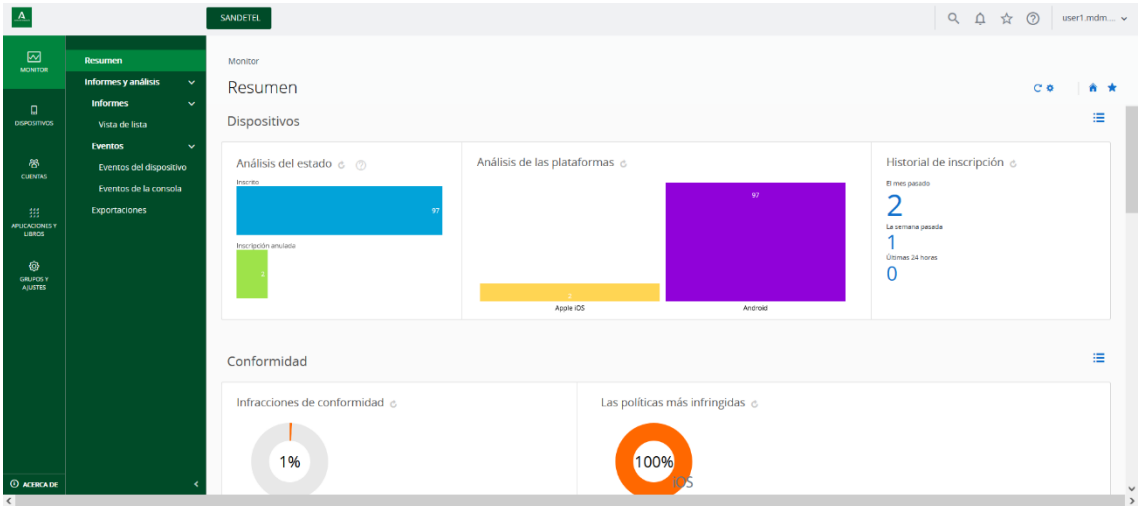
El tablero “Cuentas” proporciona información de los usuarios, grupos de usuario y usuarios administradores creados en su grupo organizativo.

El tablero “Aplicaciones y Libros” muestra las aplicaciones que son gestionadas desde el MDM.

Por último, el tablero “Grupos y Ajustes” ofrece información del grupo organizativo configurado.

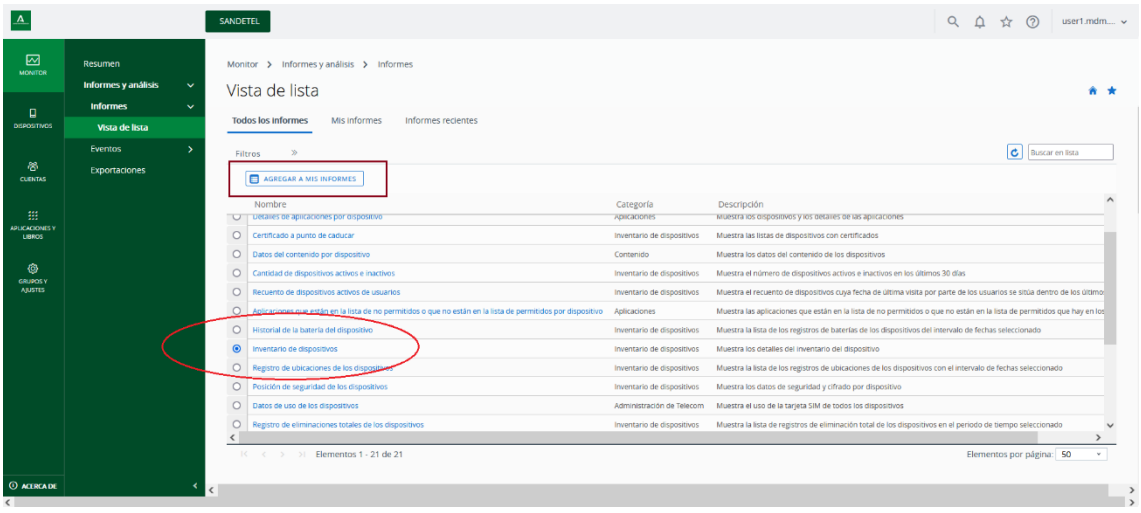
4. Tablero Monitor

En el tablero Monitor, en el menú Resumen, ofrece información rápida importante.

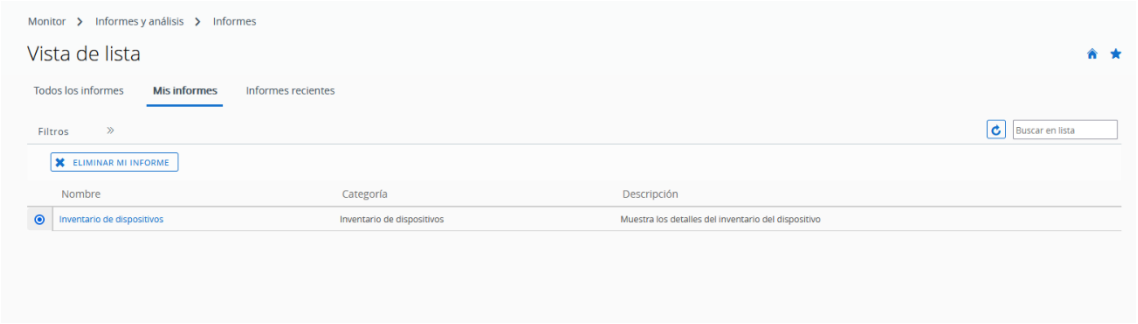


4.1. Generación de Informes (Informes y exportaciones)

Desde el tablero Monitor, en el menú de Informes y análisis -> Informes -> Vista de listas el administrador podrá generar una serie de informes preconfigurados que ofrece la herramienta. Para ello tendrá que seleccionar el informe que desee y hacer click en el botón “AGREGAR A MIS INFORMES” que se encuentra en la pestaña “Todos los informes”.

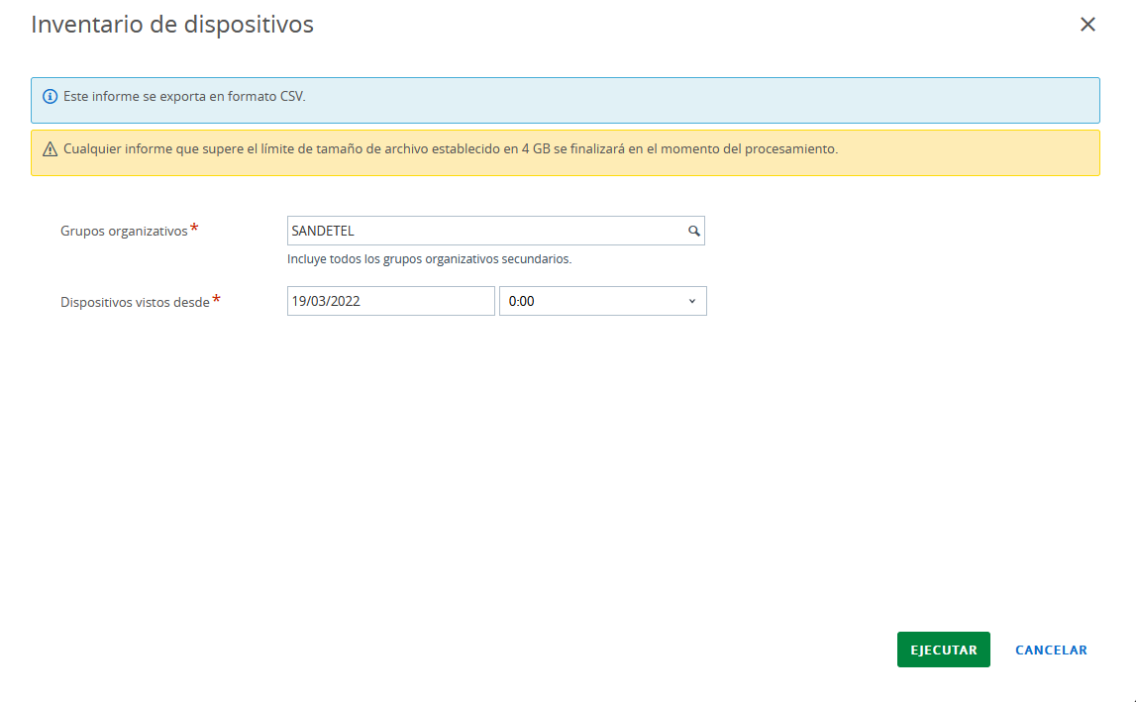


Una vez seleccionado, será necesario pulsar sobre la pestaña “Mis informes”, donde veremos disponible el informe antes seleccionado.



Seleccionándolo de nuevo, se activará el botón “ELIMINAR MI INFORME”, que permitirá borrarlo del listado de “Mis informes”.

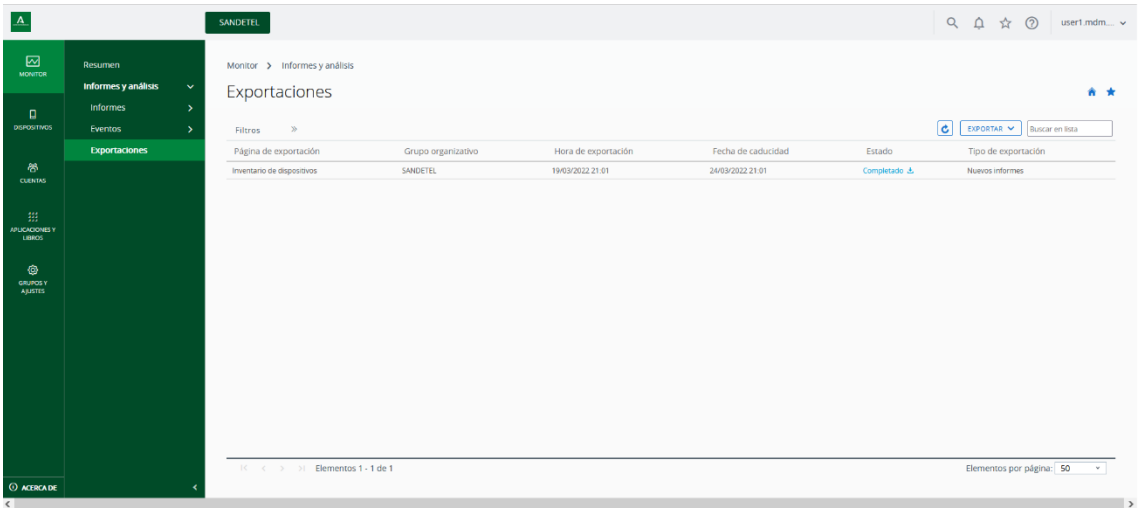
Para obtener el informe, será necesario pulsar sobre el nombre del mismo con el ratón, momento en el cual aparecerá un nuevo menú de configuración que nos permitirá seleccionar los detalles con los que queremos generar el informe:



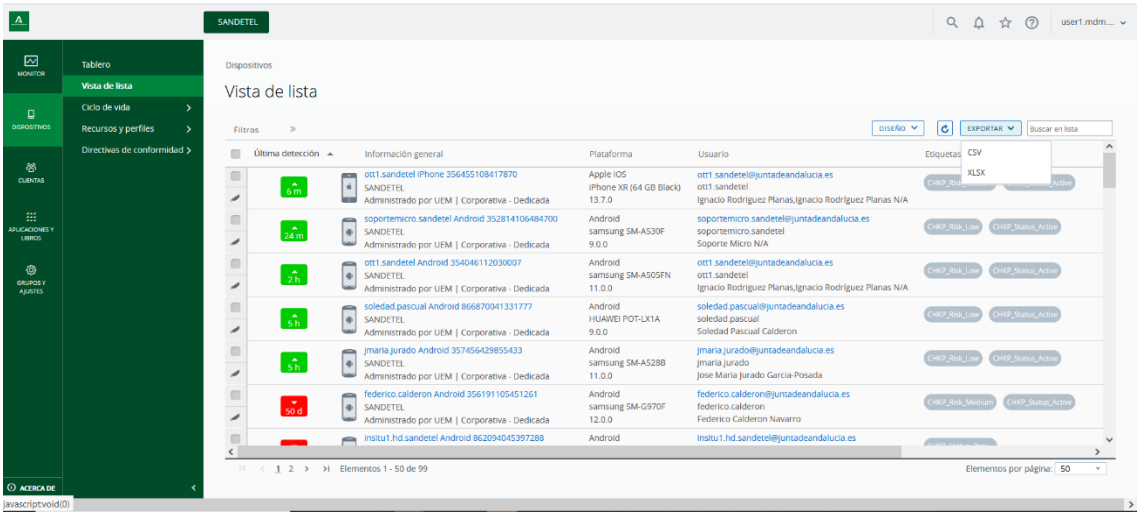
Una vez elegido las opciones deseadas, se deberá pulsar sobre el botón “EJECUTAR” para generar el informe.

Una vez realizado nos mostrará la siguiente pantalla que nos indica que el informe está generándose y transcurriendo un tiempo estará disponible en la página de Exportaciones:

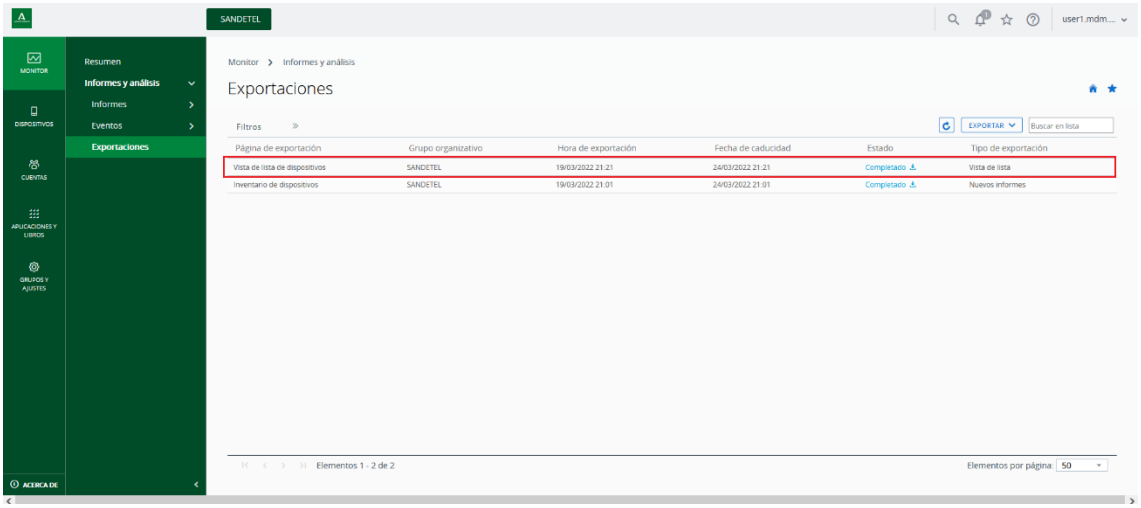
Una vez completada la acción, el informe generado aparecerá disponible para su descarga en Monitor -> Informes y análisis -> Exportaciones.



Otra forma alternativa de generar informes es pulsando en el botón “EXPORTAR” que aparece en las páginas de vista en lista de los tableros de “Dispositivos”, “Cuentas” y “Aplicaciones y Libros”, de donde podrá exportar la información de sus dispositivos, los usuarios y las aplicaciones asignadas a su grupo organizativo.



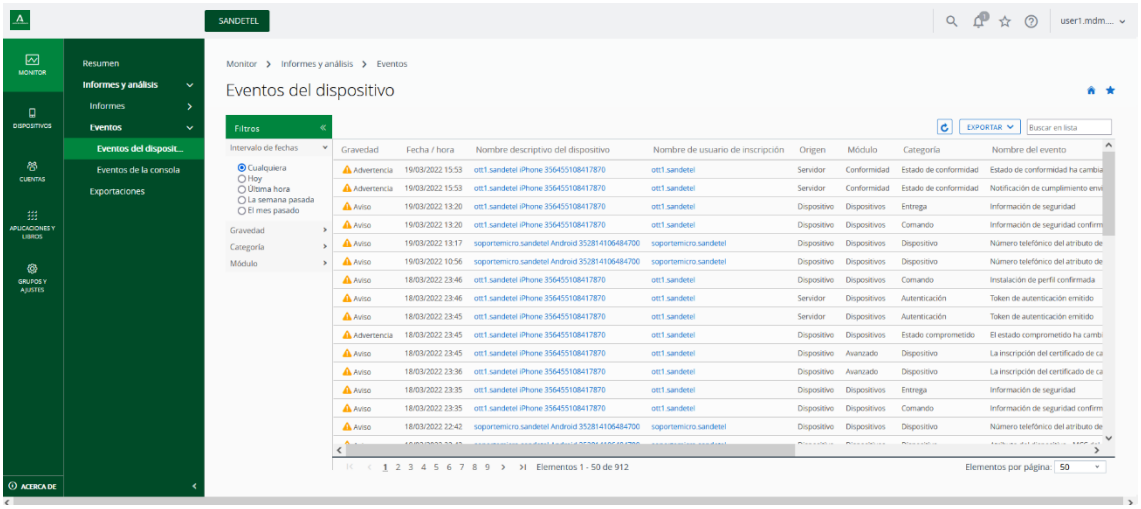
El informe generado se encontrará disponible en la misma página de Exportaciones antes indicada.

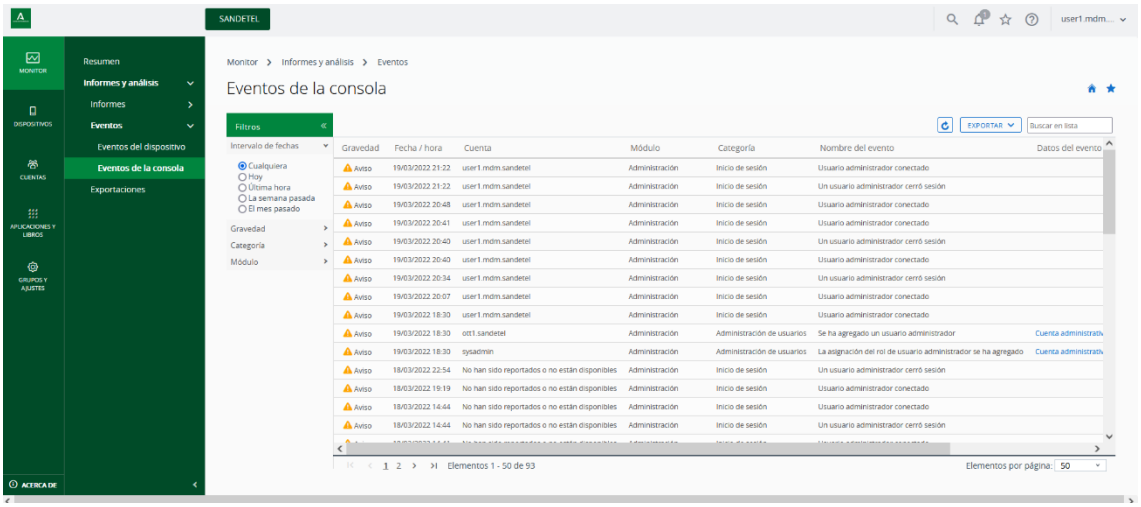


Todos los informes generados tienen una fecha de caducidad, momento a partir del cual se elimina de la plataforma.

4.2. Visualización de logs (Eventos)

Navegando a Monitor -> Eventos -> *Eventos del dispositivo* y a Monitor -> Eventos -> *Eventos de la consola* podrá visualizar los logs generados por los dispositivos vinculados a su grupo organizativo y los generados por los usuarios administradores en sus interacciones con la consola respectivamente.

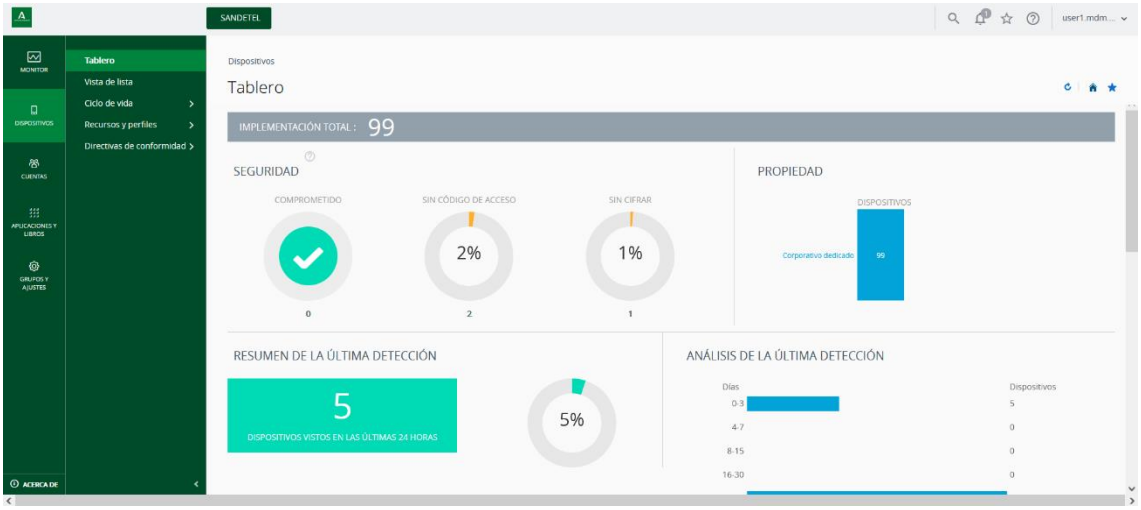

SANDETEL
user1.mdm...
MONITOR
DISPOSITIVOS
CUENTAS
APLICACIONES Y LIBROS
GRUPOS Y AJUSTES
ACERCA DE
Resumen
Informes y análisis
Informes
Eventos
Eventos del disposit...
Eventos de la consola
Exportaciones
Monitor › Informes y análisis › Eventos
Eventos del dispositivo
Filtros
EXPORTAR
Buscar en lista
Intervalo de fechas
Cualquiera
Hoy
Última hora
La semana pasada
El mes pasado
Gravedad
Categoría
Módulo
Gravedad
Fecha / hora
Nombre descriptivo del dispositivo
Nombre de usuario de inscripción
Origen
Módulo
Categoría
Nombre del evento
Elementos 1 - 50 de 912
Elementos por página: 50


SANDETEL
user1.mdm...
MONITOR
DISPOSITIVOS
CUENTAS
APLICACIONES Y LIBROS
GRUPOS Y AJUSTES
ACERCA DE
Resumen
Informes y análisis
Informes
Eventos
Eventos del dispositivo
Eventos de la consola
Exportaciones
Monitor › Informes y análisis › Eventos
Eventos de la consola
Filtros
EXPORTAR
Buscar en lista
Intervalo de fechas
Cualquiera
Hoy
Última hora
La semana pasada
El mes pasado
Gravedad
Categoría
Módulo
Gravedad
Fecha / hora
Cuenta
Módulo
Categoría
Nombre del evento
Datos del evento
Elementos 1 - 50 de 93
Elementos por página: 50

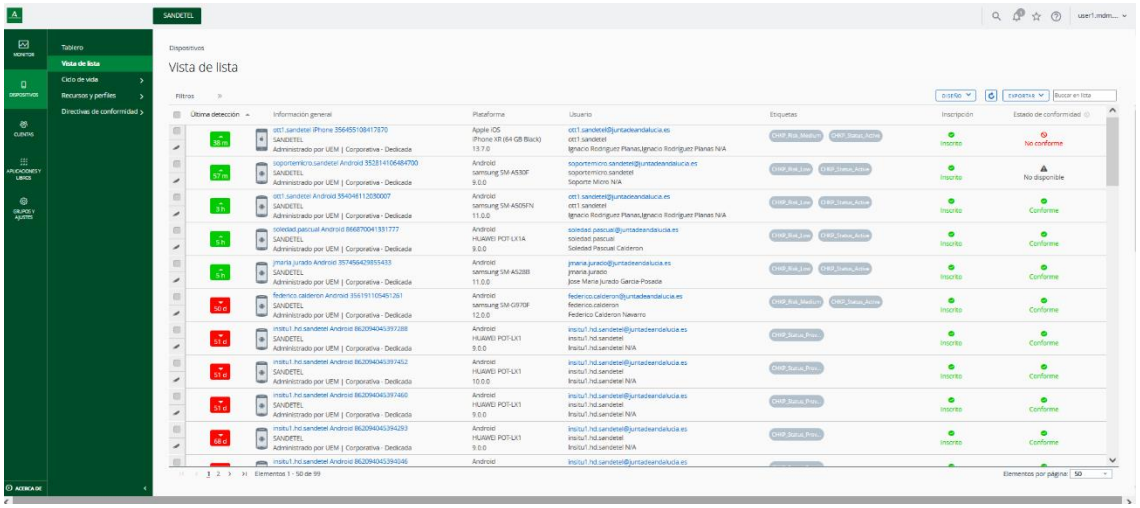
5. Tablero Dispositivos

El tablero Dispositivos muestra el parque de dispositivos móviles asociados al grupo organizativo. Dado que el MDM está vinculado al LDAP corporativo de la Junta de Andalucía, los dispositivos que se podrán visualizar serán aquellos que se hayan enrolado con los usuarios que pertenezcan a la rama LDAP del organismo. Para obtener más detalles, el responsable del organismo puede consultar con su gestor de cuentas de Sandetel qué ramas del LDAP se han asociado a su grupo organizativo.

En la página Dispositivos -> Tablero se muestra un resumen informativo de los dispositivos asociados al grupo organizativo.



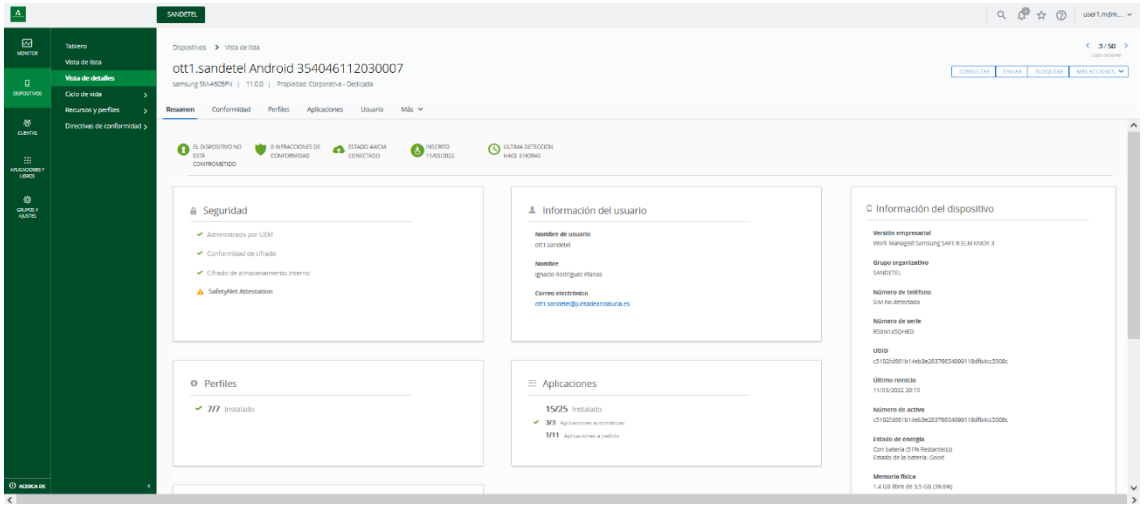
En la página Dispositivos -> *Vista de Lista* se muestran todos los dispositivos asociados al organismo.



Vista en lista

Desde esta página es posible realizar diversas acciones en masa sobre varios dispositivos.

Para ver detalles sobre un dispositivo en concreto, es necesario pulsar sobre el mismo en ***vista en lista*** para acceder a la ***vista de detalles***.



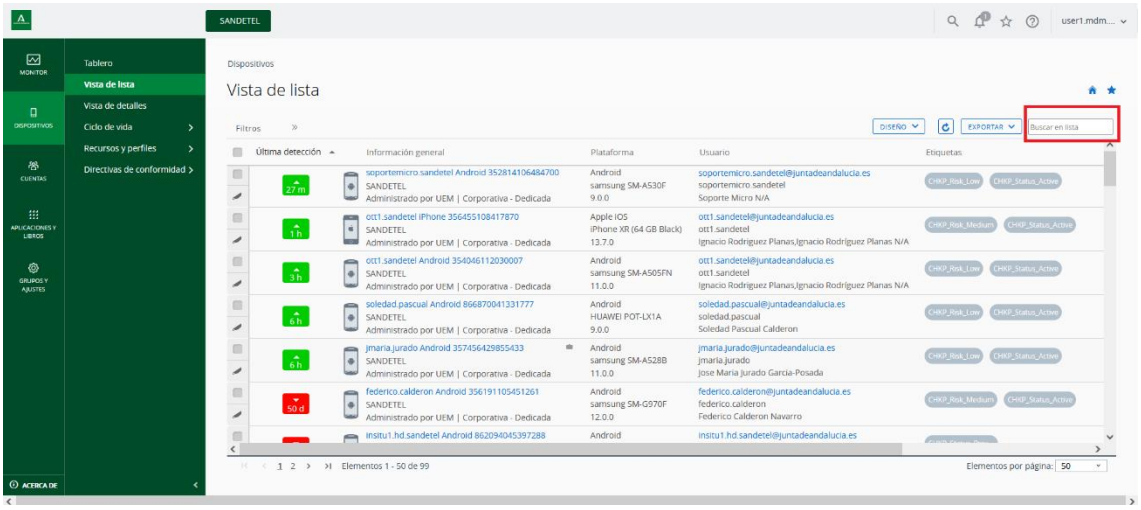
Vista de detalles

5.1. Acciones en masa (vista de lista)

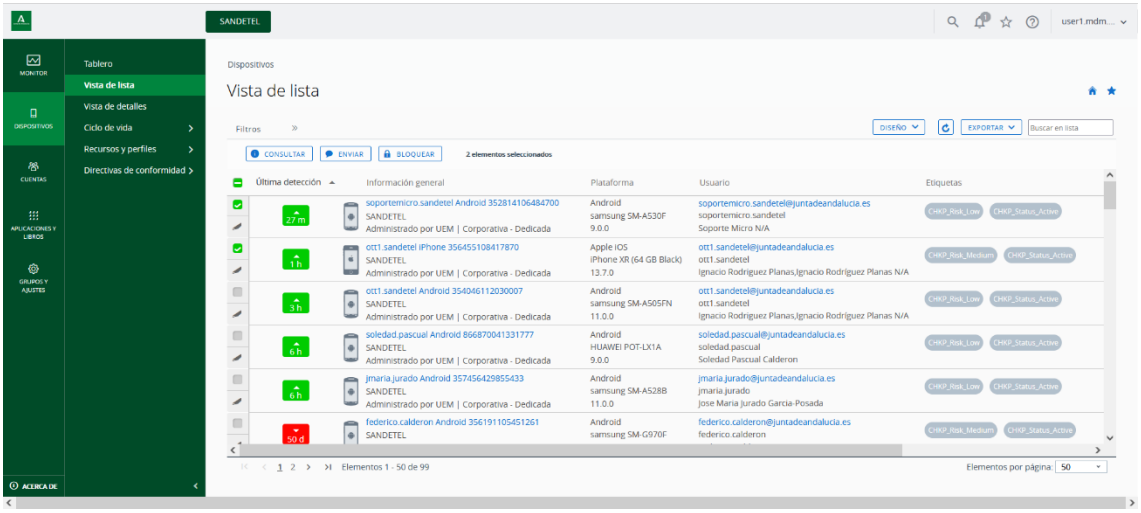
Desde la página de vista de lista del tablero Dispositivos es posible visualizar información de los dispositivos enrolados en nuestro grupo organizativo. La información que se puede obtener de la plataforma es la siguiente:

- **Última detección**. Información del tiempo que ha transcurrido desde la última vez que el dispositivo se sincronizó con la plataforma MDM.
- **Información general**. Información del dispositivo, que incluye:
  - Nombre común: Por defecto está formado por: nombre de usuario LDAP, sistema operativo e IMEI del dispositivo. Este nombre es posible modificarlo en la vista de detalles del dispositivo.
  - Información del grupo organizativo al que está asociado el dispositivo.
  - Información de la propiedad del dispositivo.
- **Plataforma**. Información del sistema operativo, el modelo del dispositivo y la versión del sistema operativo instalada.
- **Usuario**. Información del usuario del dispositivo.
- **Etiquetas**. Estado del dispositivo informado por el antivirus Harmony Mobile Protect. Las etiquetas indicarán si el antivirus está activo o provisionado, y en caso de estar activo, si está en riesgo bajo, medio, alto o sin riesgo.
- **Inscripción**. Información sobre el estado de inscripción del dispositivo, si está inscrito o anulada.
- **Estado de conformidad**. Información si el dispositivo está conforme o no conforme respecto a las políticas de conformidad configuradas. Solo podrán aparer como no conforme los dispositivos iOS que no tengan el Intelligent Hub instalado.

Se pueden hacer búsquedas sobre cualquier detalle del dispositivo en el cuadro de “Buscar en lista”:

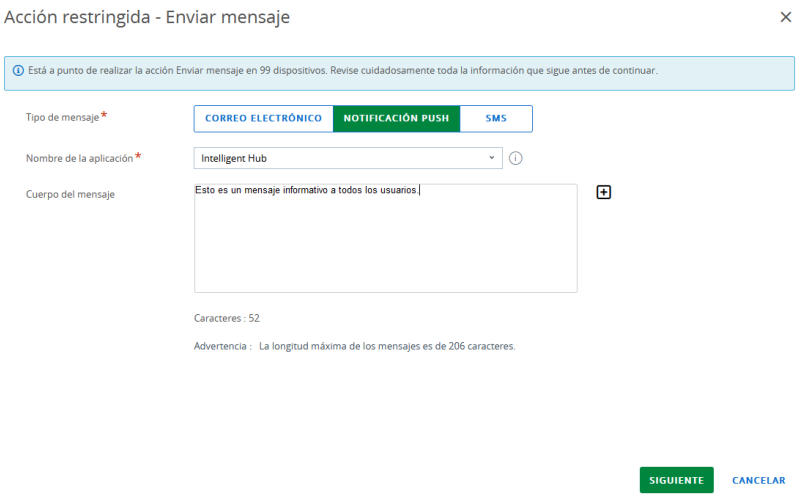


El administrador de organismo puede realizar algunas acciones en masa sobre los dispositivos. Para ello deberá seleccionar 1 o más dispositivos para que aparezcan las distintas opciones:



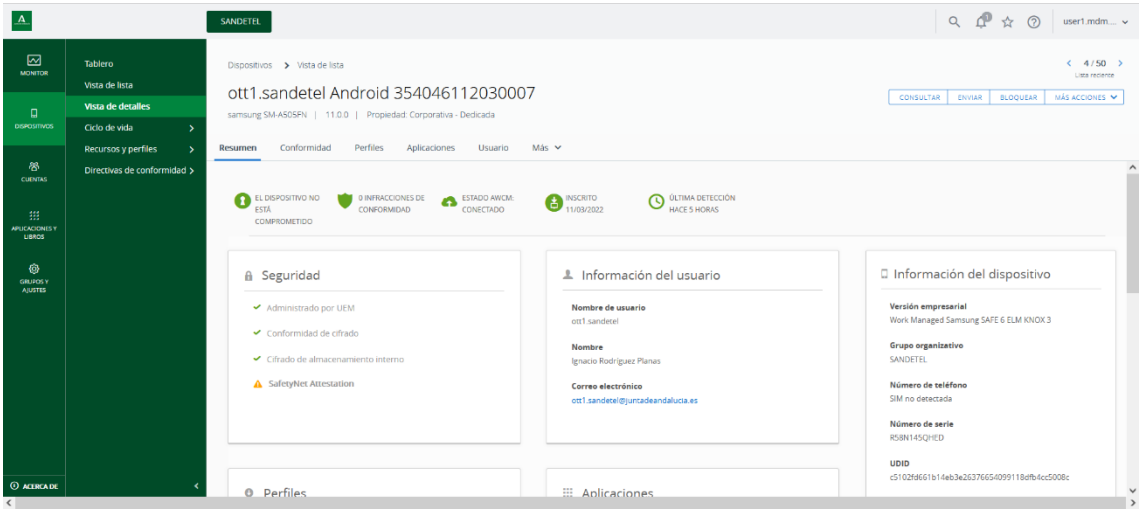
Las acciones posibles son:

- CONSULTAR. Envía un comando al dispositivo para ordenarle que sincronice con la plataforma. Permite actualizar la información que la plataforma ha detectado del dispositivo.
- ENVIAR. Permite enviar mensajes a los usuarios. Pueden ser al correo electrónico, mediante mensaje tipo push a la aplicación “Intelligent Hub” o por SMS. Se recomienda que los mensajes se envíen por “Notificación Push” al “Intelligent Hub” si se desea asegurar que el mensaje llegue a todos los usuarios (no todos los usuarios tienen que tener obligatoriamente correo electrónico y puede haber dispositivos enrolados sin tarjeta SIM).
- BLOQUEAR. Envía un comando para ordenar a los dispositivos que se active el bloqueo de pantalla.



5.2. Acciones individuales (vista de detalles)

Al pulsar con el ratón sobre el nombre del dispositivo en la pantalla de vista de lista accedemos a la pantalla de vista de detalles del dispositivo.

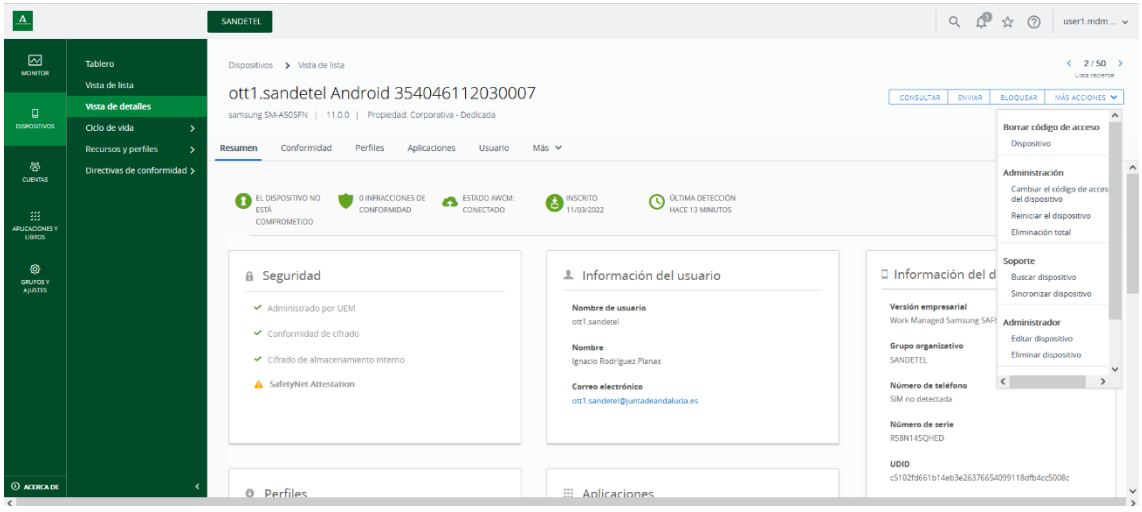


Desde esta pantalla se pueden acceder a las siguientes pestañas:

- Resumen. Muestra información general asociado al dispositivo.
- Conformidad. Muestra el estado de conformidad del dispositivo.
- Perfiles. Muestra los perfiles que tiene asignado e instalado el dispositivo. El administrador puede forzar la instalación de los perfiles asignados.
- Aplicaciones. Muestra las aplicaciones instaladas y asignadas en el dispositivo. El administrador puede forzar la instalación de las aplicaciones asignadas al dispositivo.
- Usuario. Muestra información del usuario asociado al dispositivo.
- Red. Muestra el estado de la red actual del dispositivo (Celular, Wi-Fi, Bluetooth)
- Seguridad. Muestra la información de seguridad del dispositivo.
- Notas. Permite ver y agregar notas sobre el dispositivo.

- Términos de uso. Muestra el estado de aceptación de los términos de uso de la Junta de Andalucía por parte del usuario.
- Solución de problemas. Muestra los logs generados por el dispositivo en lo correspondiente al MDM.
- Historial del estado. Muestra información histórica de la inscripción del dispositivo.

Desde la pantalla de vista de detalles también se tiene acceso a los botones de comandos del administrador:



Los comandos son los siguientes:

- **CONSULTAR**. Envía un comando al dispositivo para ordenarle que sincronice con la plataforma. Permite actualizar la información que la plataforma ha detectado del dispositivo.
- **ENVIAR**. Permite enviar mensajes a los usuarios. Pueden ser al correo electrónico, mediante mensaje tipo push a la aplicación “Intelligent Hub” o por SMS. Se recomienda que los mensajes se envíen por “Notificación Push” al “Intelligent Hub” si se desea asegurar que el mensaje llegue a todos los usuarios (no todos los usuarios tienen que tener obligatoriamente correo electrónico y puede haber dispositivos enrolados sin tarjeta SIM).
- **BLOQUEAR**. Envía un comando para ordenar a los dispositivos que se active el bloqueo de pantalla.

Más acciones:

- Borrar código de acceso del dispositivo.
  - **Dispositivo**. Elimina el código de bloqueo de pantalla configurado en el dispositivo.
- Administración:
  - **Cambiar el código de accceso del dispositivo**. Permite modificar el código de bloqueo del dispositivo y establecer un nuevo PIN o contraseña para el mismo.

- **Reiniciar el dispositivo**. Permite reiniciar el dispositivo.

- **Eliminación total**. Permite realizar un reset de fábrica en el dispositivo. Una vez realizado, el dispositivo seguirá apareciendo en la plataforma pendiente de eliminarlo definitivamente mediante el comando Administrador -> ***Eliminar dispositivo***.

- Soporte:
  - **Buscar dispositivo**. Permite enviar un sonido audible diseñado para ayudar al usuario a ubicar un dispositivo que se haya perdido. Entre las opciones de sonido audible se incluye la reproducción de un sonido una cantidad configurable de veces y la duración del intervalo, en segundos, entre los sonidos.

  - **Sincronizar dispositivo**. Permite sincronizar el dispositivo seleccionado con la consola de administración para alinear el estado de Última detección.

- Administrador:
  - **Editar dispositivo**. Permite editar la información del dispositivo, como el Nombre común, Número de activo, Propiedad del dispositivo, Grupo de dispositivos y Categoría del dispositivo.

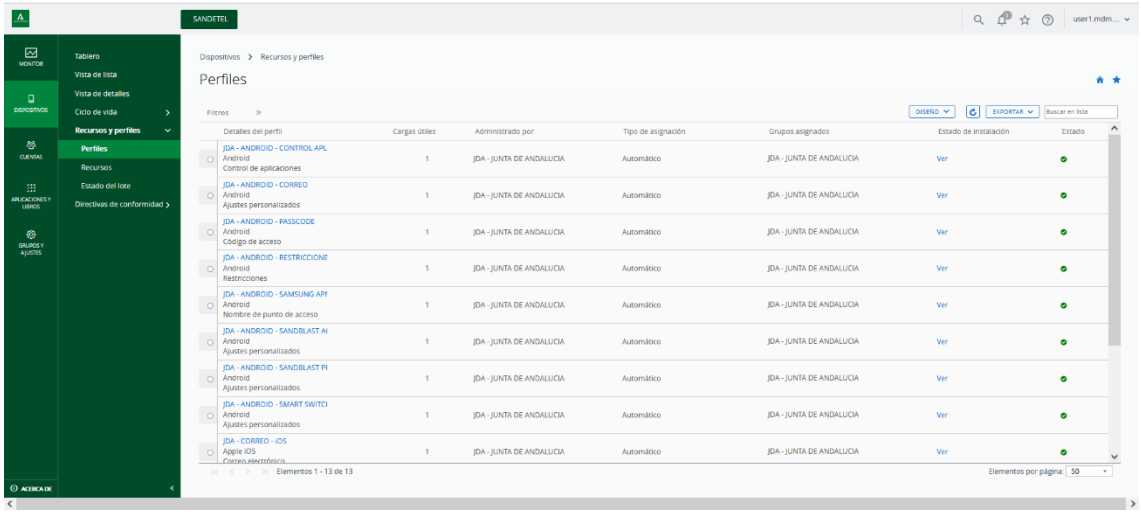
  - **Eliminar dispositivo**. Permite eliminar y anular la inscripción de un dispositivo de la consola. Envía el comando de eliminación total (reset de fábrica) y elimina la representación del dispositivo en la consola. No obstante, el fabricante no recomienda eliminar el dispositivo sin antes haber realizado un reset de fábrica (comando Administración -> ***Eliminación Total***).

- Avanzado:
  - **Iniciar AWCM**. Permite iniciar el servicio AirWatch Cloud Messaging (AWCM) en el dispositivo seleccionado. AirWatch Cloud Messaging (AWCM) permite el envío de políticas y comandos en tiempo real al dispositivo. Con AWCM detenido, el dispositivo sólo recibe las políticas y comandos durante los intervalos de comprobaciones de estado regulares preestablecidos.

  - **Detener AWCM**. Permite detener el servicio AirWatch Cloud Messaging (AWCM) en el dispositivo seleccionado.

5.3. Políticas preconfiguradas (perfiles)

En la página Dispositivos -> Recursos y perfiles -> Perfiles se pueden consultar los perfiles preconfigurados. Los perfiles configuran las políticas de uso establecidas por la organización.



Los perfiles preconfigurados para la Junta de Andalucía son los siguientes:

Perfiles para dispositivos Android:

- JDA - ANDROID - CONTROL APLICACIONES. Perfil que impide la desinstalación de aplicaciones obligatorias y permite la activación de aplicaciones de sistema.
- JDA - ANDROID – PASSCODE. Perfil que obliga al usuario a establecer una contraseña de bloqueo de pantalla (mediante contraseña, PIN de al menos 4 cifras o biométrico).
- JDA - ANDROID – RESTRICCIONES. Perfil que impide que el usuario pueda realizar un reset de fábrica, instalar aplicaciones desde fuentes desconocidas y usar el modo “depuración USB”.
- JDA - ANDROID - SAMSUNG APN. Perfil que configura el APN como secundario en dispositivos Samsung. El usuario deberá introducir su contraseña manualmente en los ajustes del dispositivo.
- JDA - ANDROID – CORREO. Perfil que configura el correo IMAP corporativo de la Junta de Andalucía en el dispositivo.
- JDA - ANDROID - SMART SWITCH. Perfil que permite el uso de la aplicación “Smart Switch”.
- JDA - ANDROID - SANDBLAST PROVISIONADO. Perfil necesario para activar la aplicación Harmony Mobile Protect (anteriormente denominada SandBlast).
- JDA - ANDROID - SANDBLAST ACTIVADO. Perfil necesario para activar la aplicación Harmony Mobile Protect. Cuando este perfil está instalado significa que el antivirus ya está activado en el dispositivo.

Perfiles para dispositivos iOS:

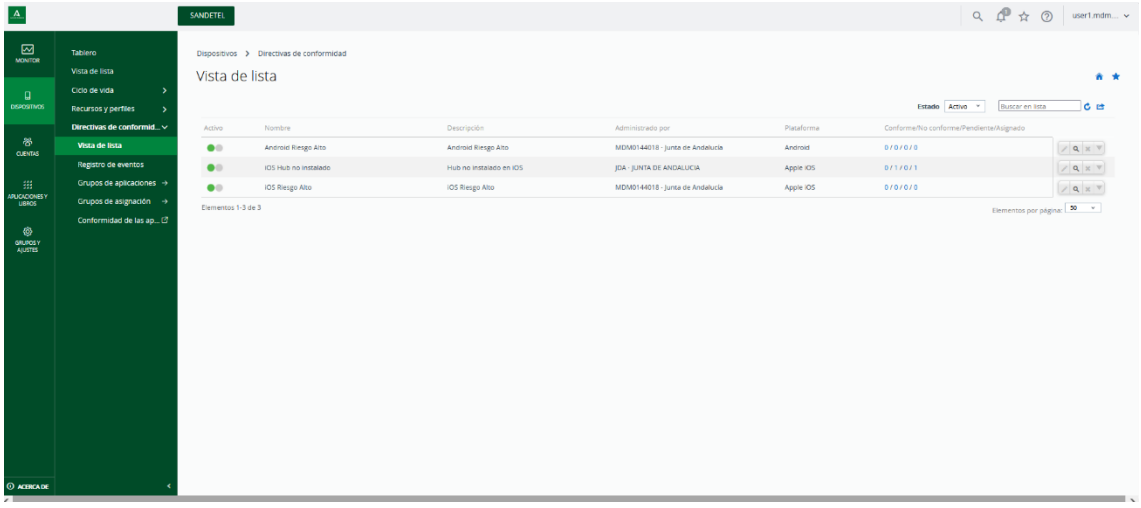
- JDA - iOS – PASSCODE. Perfil que obliga al usuario a establecer una contraseña de bloqueo de pantalla de al menos 4 cifras.
- JDA - CORREO – iOS. Perfil que configura el correo IMAP corporativo de la Junta de Andalucía en el dispositivo.
- JDA - iOS – RESTRICCIONES. Perfil que permite un uso personal del dispositivo.
- JDA - IOS – SANDBLAST. Perfil necesario para activar la aplicación Harmony Mobile Protect (anteriormente denominada SandBlast).
- JDA - IOS - SANDBLAST NO ACTIVADO. Perfil necesario para activar la aplicación Harmony Mobile Protect. Cuando este perfil NO esté asignado al dispositivo significa que el antivirus ya está activado en el dispositivo.

La activación del antivirus Harmony Mobile Protect se hace de forma automática y tarda unas 24 horas desde que el dispositivo se enrola en el MDM.

5.4. Directivas de conformidad

Las políticas de conformidad permiten establecer acciones de forma automática cuando se cumplen una serie de criterios.

En la página Dispositivos -> Directivas de conformidad -> Vista en lista se muestran las directivas de conformidad:



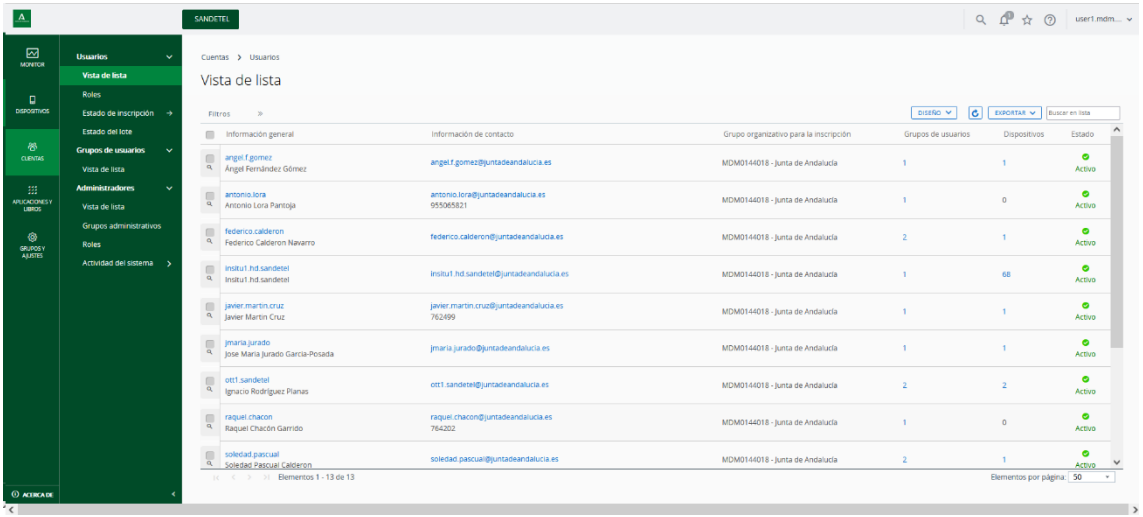
Actualmente las directivas de conformidad no realizan ninguna acción pero podrían configurarse en caso de ser necesario. En concreto:

- Android Riesgo Alto. Esta directriz detecta cuándo el antivirus ha informado a la consola que un dispositivo Android está en riesgo alto. Entre las acciones que podrían configurarse es que desde la plataforma se envíe un email al responsable del organismo informando de tal evento.
- iOS Riesgo Alto. Esta directriz es igual que la anterior pero para dispositivos iOS.
- iOS Hub no instalado. Esta directriz informa que la aplicación Intelligent Hub no está instalada en un dispositivo iOS autoenrolado.

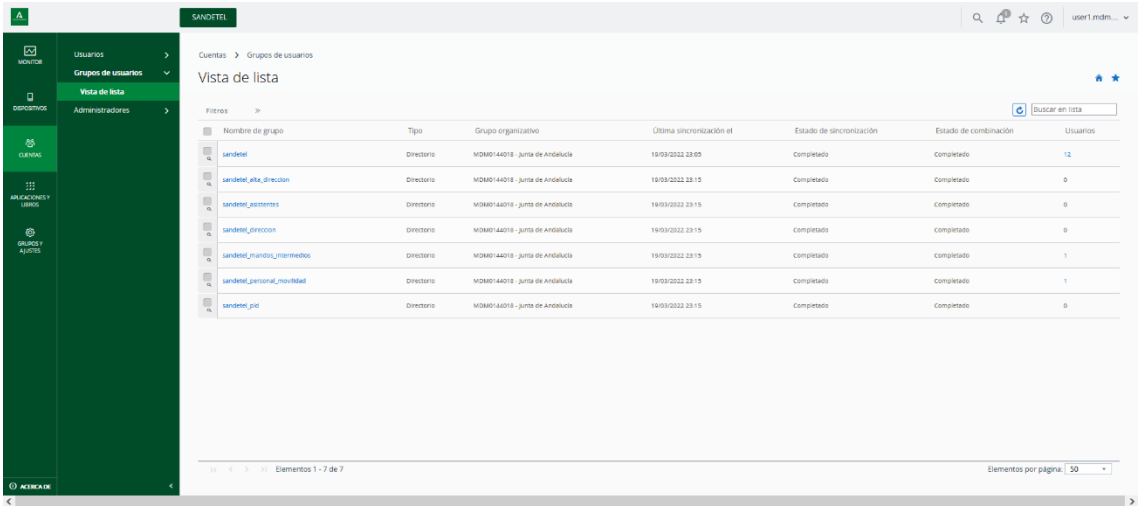
6. Tablero Cuentas

Desde el tablero de cuentas se muestra información de los usuarios, grupos de usuario y usuarios administradores creados en el grupo organizativo.

Los usuarios se muestran en Cuentas -> Usuarios -> Vista en lista.



Los grupos de usuarios se muestran en Cuentas -> Grupos de usuario -> Vista en lista



Los grupos de usuario configurados están integrados con el LDAP corporativo y contienen la siguiente clasificación:

- Grupo “nombre de organismo” (en el ejemplo: “sandetel”). En este grupo está configurada la rama del LDAP asociada al organismo. De esta forma, todos los usuarios que pertenezan a dicha rama del LDAP pertenecerán a este grupo de usuario.

- El resto de grupos configurados: “personal con movilidad”, “asistentes”, “mandos intermedios”, “pld”, “dirección” y “alta dirección” son los grupos asociados a la *Instrucción 1/2014, de la Dirección General de Telecomunicaciones y la Sociedad de la Información, por la que se definen los requisitos y obligaciones para el uso racional de los servicios de telefonía por parte de los organismos de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía* (***Plan RUT***).

La adhesión de los usuarios a uno de estos grupos depende de lo que se haya configurado en el Gestor de Líneas de la RCJA. La información que se configura en dicha herramienta se vuelca en el LDAP corporativo de la RCJA, que es de donde el MDM toma los datos.

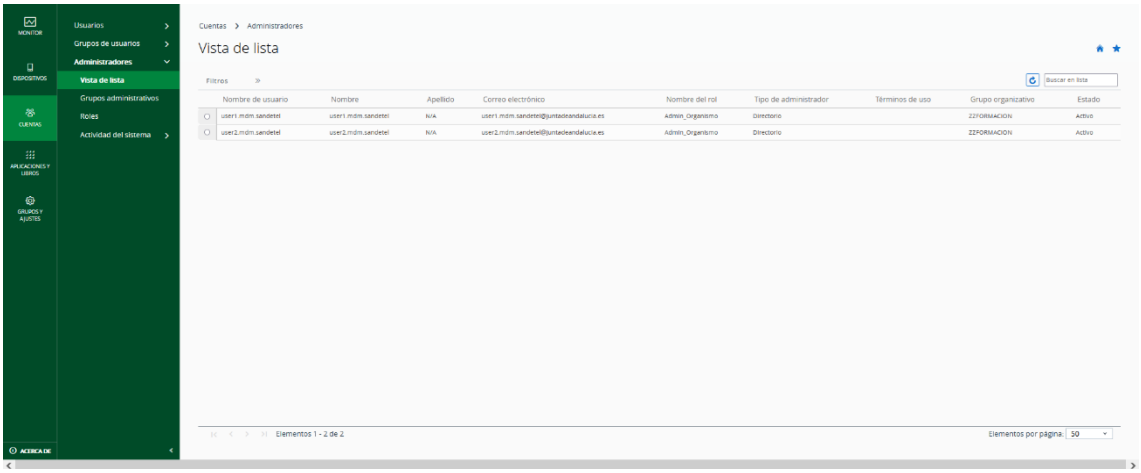
Asociados a estos grupos existe una restricción en el número de dispositivos que cada usuario puede inscribir en la herramienta, conforme a lo establecido en el mencionado Plan RUT. Concretamente:

- Los usuarios pertenecientes al grupo de usuarios “Dirección” y “Alta Dirección” pueden tener un máximo de 4 dispositivos inscritos simultáneamente. Según se establece en el Plan RUT, los usuarios que pertenecen a dichos grupos pueden tener un máximo de 2 dispositivos simultáneos, pero se permite el doble para el momento en el que el usuario realice una renovación de terminal y pueda pasar la información del dispositivo antiguo al nuevo.

- De la misma forma, los usuarios pertenecientes al grupo de usuarios “personal con movilidad”, “asistentes”, “mandos intermedios” y “pld”, tienen la limitación de poder inscribir un máximo de 2 dispositivos simultáneamente.

El resto de usuarios no tienen limitaciones para enrolar un número máximo de dispositivos.

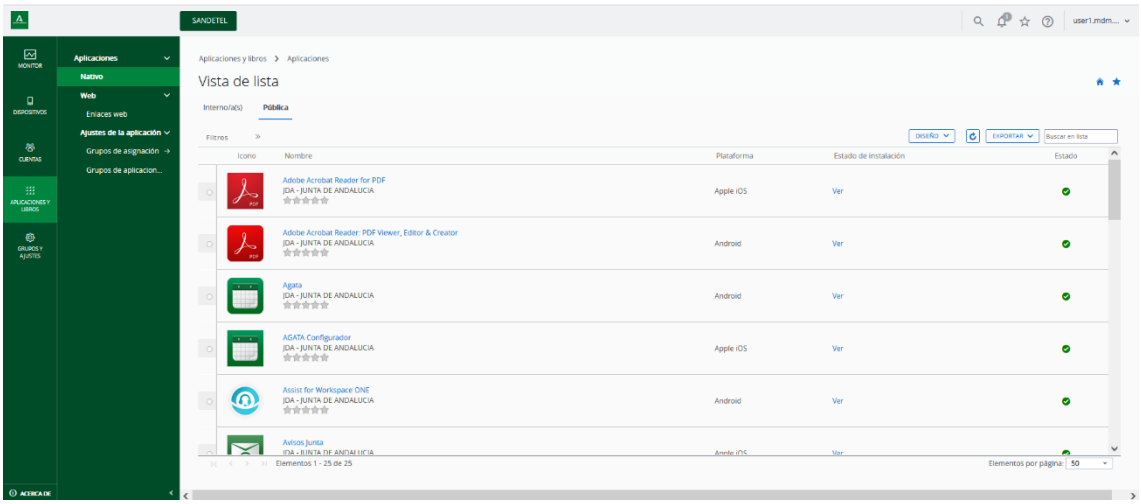
Por último, los usuarios administradores configurados en el grupo organizativo pueden visualizarse en Cuentas -> Administradores -> Vista en lista.



7. Tablero Aplicaciones y libros

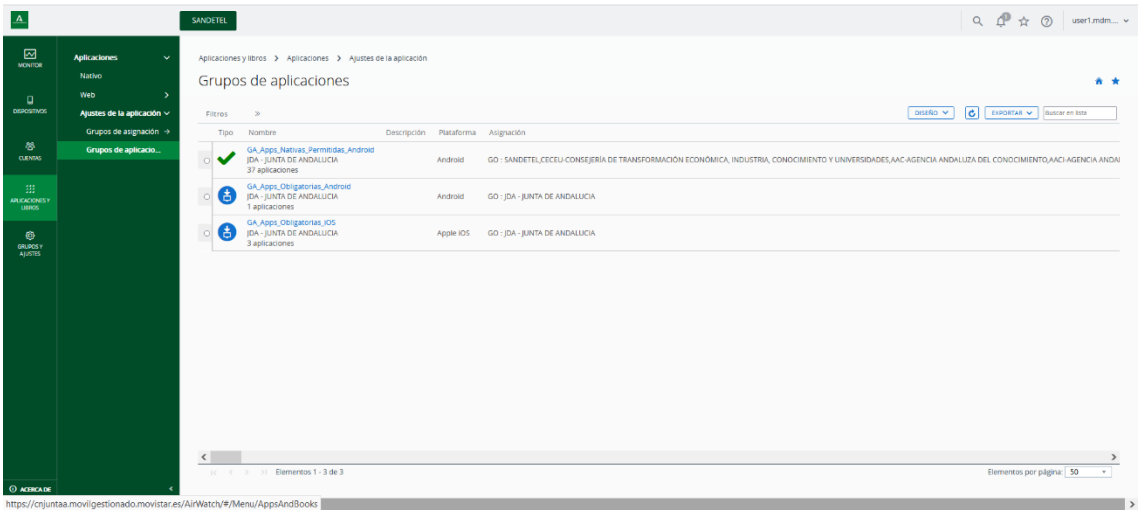
Desde el tablero de “Aplicaciones y Libros” se muestran las aplicaciones asignadas al grupo organizativo.

En la página “Aplicaciones y Libros” -> Aplicaciones -> Nativo pueden visualizarse las aplicaciones internas (apk que se distribuyen desde el MDM) y las públicas (aplicaciones que se distribuyen desde Google Play / Apple Store).



Entre las aplicaciones existentes, Harmony Mobile Protect está configurada para que se instale automáticamente y de forma obligatoria en los dispositivos Android e iOS.

En la página “Aplicaciones y Libros” -> ajustes de la aplicación -> Grupos de aplicaciones se muestran las políticas establecidas para el uso de las aplicaciones:



Los grupos de aplicaciones configurados son:

- GA_Apps_Obligatorias_Android. Contiene el listado de aplicaciones obligatorias para Android. Sólo aparece configurada Harmony Mobile Protect. Los usuarios no podrán desinstalar esta aplicación debido al tener también configurado el perfil “JDA - ANDROID - CONTROL APLICACIONES” (ver apartado *5.3 Políticas preconfiguradas (perfiles)*).
- GA_Apps_Obligatorias_iOS. Al igual que en el anterior caso para Android, también tiene configurada únicamente Harmony Mobile Protect para iOS.

- GA_Apps_Nativas_Permitidas_Android. Contiene un listado de aplicaciones permitidas para dispositivos Android. Contiene el listado de aplicaciones de fábrica de dispositivos Samsung y Huawei.

8. Tablero Grupos y ajustes

Desde el tablero de “Grupos y ajustes” se accede a los ajustes de la consola. El administrador de organismo no tiene acceso al mismo. Tan sólo podrá ver información del grupo organizativo de su organismo desde Grupos y ajustes -> Grupos -> Grupos organizativos -> Vista en lista.