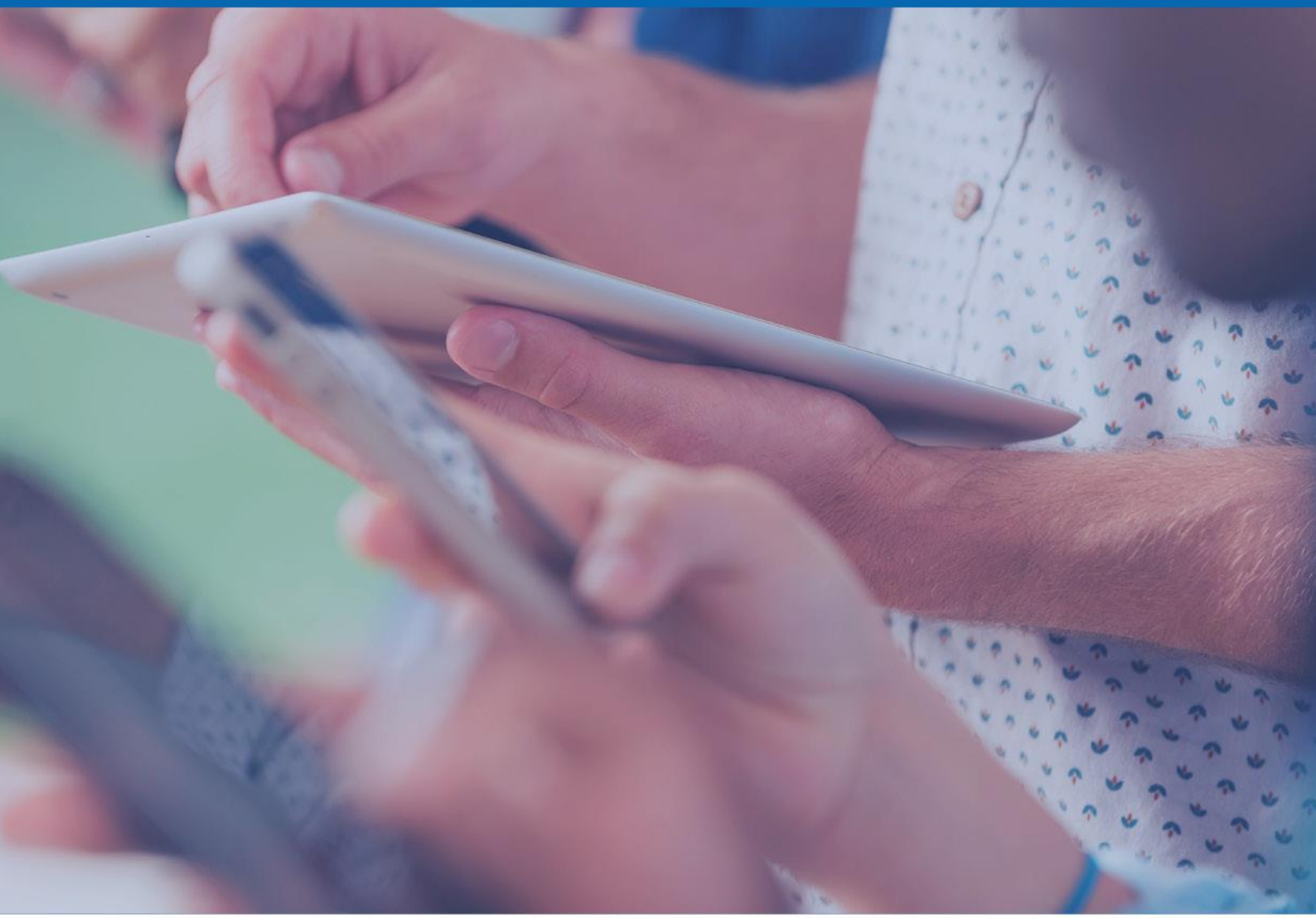
Panda Multidispositivo



Manual de usuario

panda movistar

pandasecurity.com

Indice

1. Introducción

Panda Multidispositivo es una aplicación desarrollada por Panda Security que proporciona una solución completa de seguridad concebida para proteger la red informática y gestionar la seguridad de manera sencilla y en modo online. La protección que proporciona neutraliza spyware, troyanos, virus y cualquier otra amenaza dirigida contra sus equipos.

Sus principales características son:

- Máxima protección para PCs, portátiles y servidores.
- Fácil de instalar, gestionar y mantener a través de su consola Web.
- Gestión y organización basada en perfiles de protección y grupos de equipos.

El centro de gestión de Panda Multidispositivo es la consola Web, desde donde usted podrá:

1. Configurar la protección, distribuirla e instalarla en los equipos.

2. Monitorizar el estado de la protección en los equipos.

3. Extraer informes sobre el estado de la seguridad y las amenazas detectadas.

4. Gestionar las detecciones realizadas y saber en todo momento qué se ha detectado, cuándo y en qué equipo.

5. Configurar la cuarentena de elementos sospechosos.

1.1. La protección

De acuerdo con las necesidades de protección de sus equipos, usted podrá crear perfiles y determinar cuál será el comportamiento de la protección (antivirus, firewall, control de dispositivos, servidores Exchange y control de la navegación) para el perfil que está creando. A continuación, podrá asignar dicho perfil a los grupos de equipos que quiere proteger.

Usted puede configurar la protección instalada en los equipos antes o después de la instalación, pero es recomendable que dedique un tiempo a analizar en profundidad cuáles son las necesidades de protección de su red.

Estas necesidades pueden variar de unos equipos a otros, o también pueden ser las mismas para todos ellos. En función de ello, usted puede necesitar crear perfiles nuevos o le bastará con la configuración por defecto que Panda Multidispositivo proporciona.

2. Requisitos

2.1. Consola web

• Conexión a Internet

• Internet Explorer

• Firefox

• Google Chrome

2.2. Estaciones de trabajo y servidores de ficheros Windows

• Uno de ellos al menos con conexión a Internet.

• Sistemas Operativos (estaciones): Windows 2000 Professional, Windows XP SP0 y SP1 (32 y 64-bits), XP SP2 y superiores, Vista, Windows 7, Window 8.0, Windows 8.1 (32 y 64 bits) y Windows 10.

• Sistemas Operativos (servidores): Windows 2000 Server, Windows Home Server, Windows 2003 (32, 64 bits y R2) SP1 y superior, Windows 2008 (32 y 64 bits), Windows 2008 R2 (64 bits), Windows Small Business Server 2011, Windows Server 2012 (64 bit y R2).

2.3. Tablets y smartphones

• Android 2.3 (Gingerbread) y superiores.

2.4. Estaciones de trabajo y servidores de ficheros Linux

• Ubuntu 12 32/64 bits y superiores.

• Red Hat Enterprise Linux 6.0 64 bits y superiores.

• CentOS 6.0 64 bits y superiores.

• Debian 6.0 Squeeze y superiores.

• OpenSuse 12 32/64 bits y superiores.

• Suse Enterprise Server 11SP2 64 bits y superiores.

2.5. Certificaciones en entornos de virtualización

• VMWare ESX 3.x,4.x, 5,x

• VMWare Workstation 6.0, 6.5, 7.x, 8.x y 9.x

• Virtual PC 6.x

• Microsoft Hyper-V Server 2008 R2 y 2012 3.0

• Citrix XenDesktop 5.x, XenClient 4.x, XenServer y XenApp 5.x y 6.x

3. Acceso a la consola web

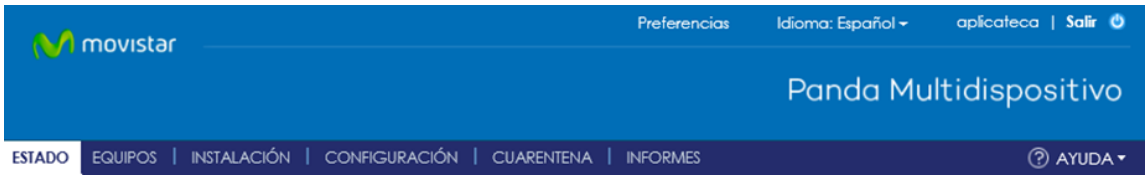
Para acceder a la consola Web:

1. Acceda a través de Aplicateca http://www.aplicateca.es identificándose con su usuario y contraseña.

2. Acceda a Mis Aplicaciones y encontrará un acceso directo a Panda Multidispositivo.

3. Acepte los términos y condiciones del Acuerdo de Licencia (sólo se le solicitará la primera vez que acceda a la aplicación).

Después se mostrará la ventana principal de la consola Web. Desde esa ventana, usted podrá acceder a las áreas de Estado, Equipos, Instalación y configuración, Cuarentena e Informes.



Mediante la opción Salir, usted puede cerrar la sesión. También puede seleccionar el idioma en el que desea visualizar la consola Web, utilizando el desplegable Idioma situado junto al idioma activo.

Para establecer la configuración general de su consola Web, haga clic en Preferencias.

Si desea acceder a la ayuda, o consultar la Guía Básica de Administración, seleccione la opción correspondiente en el menú desplegable Ayuda. Utilice también este menú si lo que desea es acceder al Acuerdo de Licencia.

4. Instalación de la protección

4.1. Cerrar otras aplicaciones durante la instalación.

Es recomendable realizar la instalación manteniendo el resto de aplicaciones cerradas.

4.2. Existencia de otras protecciones instaladas en los dispositivos equipos.

Es muy importante que antes de instalar Panda Multidispositivo en los equipos se asegure usted de que no hay instalado otro antivirus o solución de seguridad. Algunos de ellos serán detectados y desinstalados automáticamente por el instalador de Panda Multidispositivo. Puede consultar una lista actualizada de los antivirus que Panda Multidispositivo desinstala automáticamente en el link:

http://www.pandasecurity.com/spain/enterprise/support/card?id=50021&idIdioma=1.

Mediante la opción Salir, usted puede cerrar la sesión. También puede seleccionar el idioma en el que desea visualizar la consola Web, utilizando el desplegable Idioma situado junto al idioma activo.

Para establecer la configuración general de su consola Web, haga clic en Preferencias.

Si desea acceder a la ayuda, o consultar la Guía Básica de Administración, seleccione la opción correspondiente en el menú desplegable Ayuda. Utilice también este menú si lo que desea es acceder al Acuerdo de Licencia.

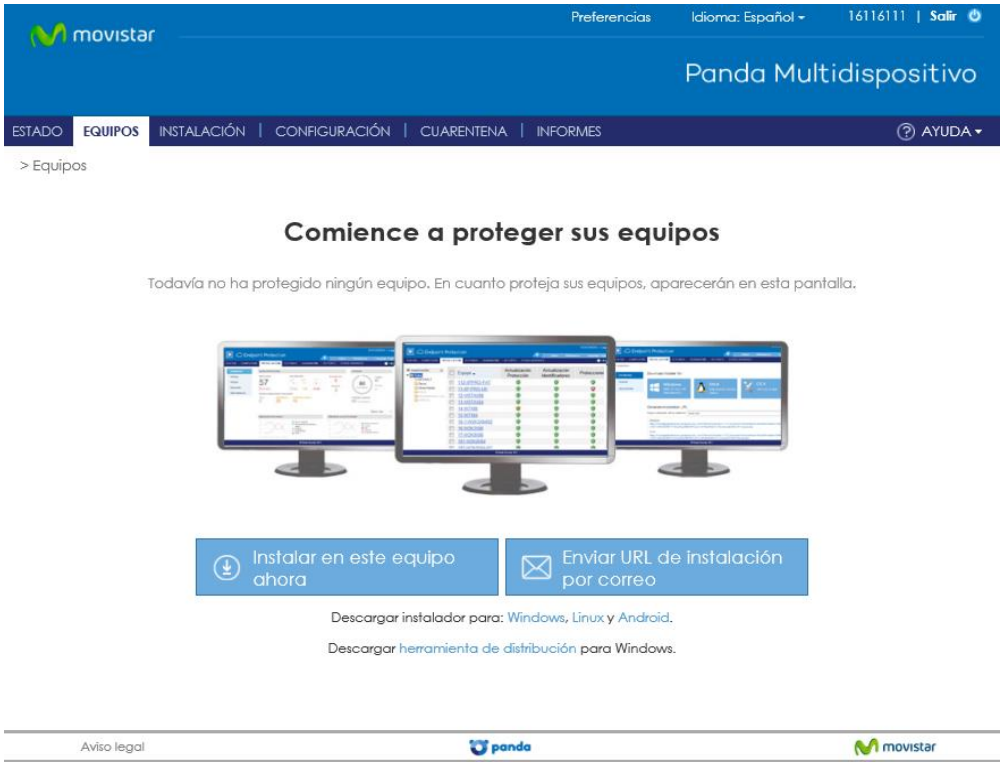
Si el suyo no estuviera en la lista, desinstálelo manualmente:

En Windows XP: Panel de Control > Agregar o quitar programas

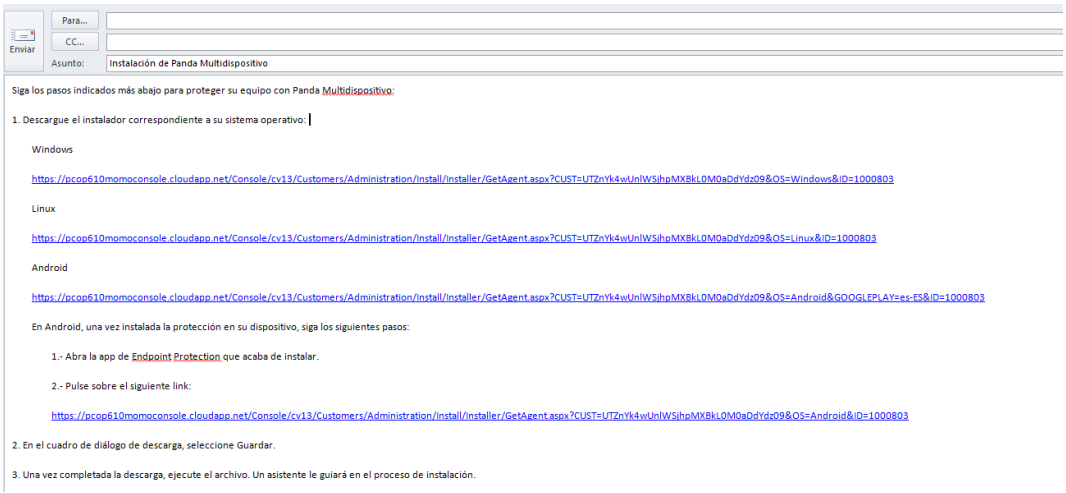
En Windows Vista o Windows 7: Panel de Control > Programas y características > Desinstalar (y el resto de versiones y SO?)

4.3. Instalación rápida

La primera vez que acceda a su consola de gestión verá la siguiente pantalla en la que puede instalar directamente la protección en el dispositivo desde el que accede o bien generar un ejecutable a enviar a los dispositivos donde quiera instalarlo.

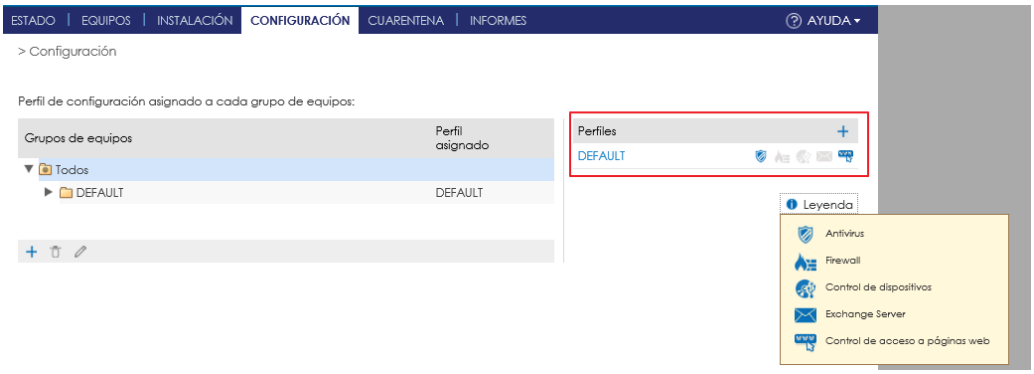


Si elige la opción de enviar URL de instalación por correo se generará el siguiente correo a enviar a todos los usuarios cuyos dispositivos desee proteger.



También podrá realizar esta operación desde la pestaña Instalación.

De esta manera se instalará la protección por defecto. Para ver las características de esta protección puede entrar en la pestaña Configuración y ver el perfil Default.



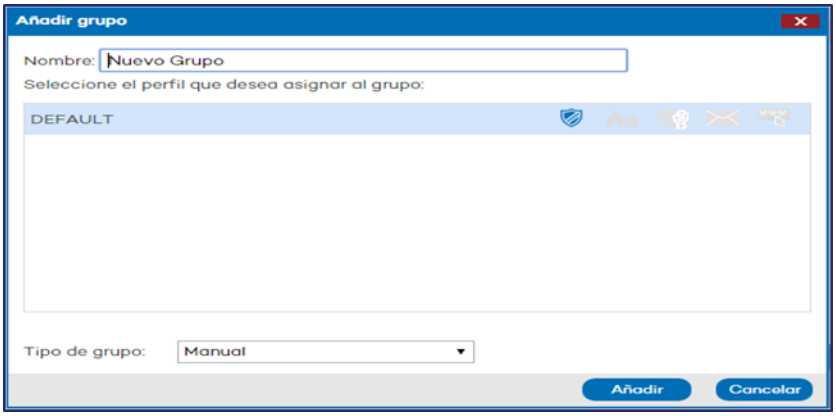
4.4. Configuración

Para hacer configuraciones personalizadas en la solución, acceda al apartado Configuración. Ahí verá dos apartados: Grupos de Equipos y Perfiles.

- **Grupos de equipos:** existe uno por defecto, llamado Default, donde se irán incorporando los equipos sobre los que instale el agente de Panda Multidispositivo, por defecto. La finalidad de los Grupos es que usted unifique máquinas bajo un mismo grupo según un criterio. Por ejemplo: ubicación geográfica, sistema operativo, tipos de dispositivos (portátiles, sobremesa, servidores, móviles, etc). Sobre los grupos de máquinas se aplican los "Perfiles", que se explican más abajo.

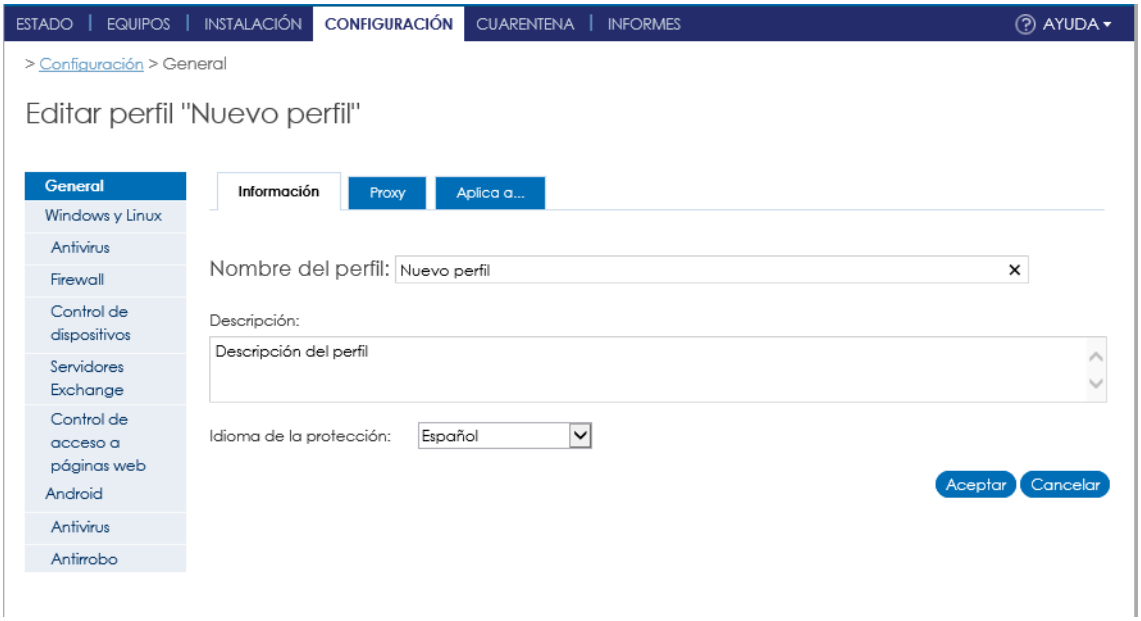
Para crear grupos de máquinas tiene que pulsar el botón "+" que aparece en la parte inferior del apartado "Grupos":

Y una vez hecho esto, aparecerá un popup en el que tiene que indicar el nombre del grupo y pulsar el botón "Añadir"



- **Perfiles:** Son configuraciones que se aplican a los Grupos de equipos creados en el punto anterior. Para cada perfil se puede configurar: antimalware, firewall, control de dispositivos, protección para servidor Exchange, Control de acceso a páginas web y antirrobo en Android. Existe un perfil por defecto, llamado "Default ", que tiene configurado sólo antimalware y filtrado web. Para añadir un nuevo Perfil al que configurar el resto de las opciones disponibles, puede acceder al apartado Configuración y en la parte derecha de la pantalla, pulsar el botón "+" que hay en el apartado Perfiles.

Aparecerá una pantalla como la que figura a continuación:



Para más información sobre cada uno de los apartados puede pulsar AYUDA en el menú superior al entrar en cualquiera de las opciones del menú lateral.

4.5. Vista de la instalación y de la protección en el PC del usuario

Una vez instalada la protección aparecerá un icono en la barra del reloj con el símbolo de un escudo.

Haciendo clic en dicho símbolo con el botón derecho del ratón sobre el icono, se mostrará al usuario el estado de protección y fecha de la última actualización con la nube.

Se puede hacer un análisis bajo demanda pinchando en el recuadro correspondiente a Antivirus.

5. Estado de la protección

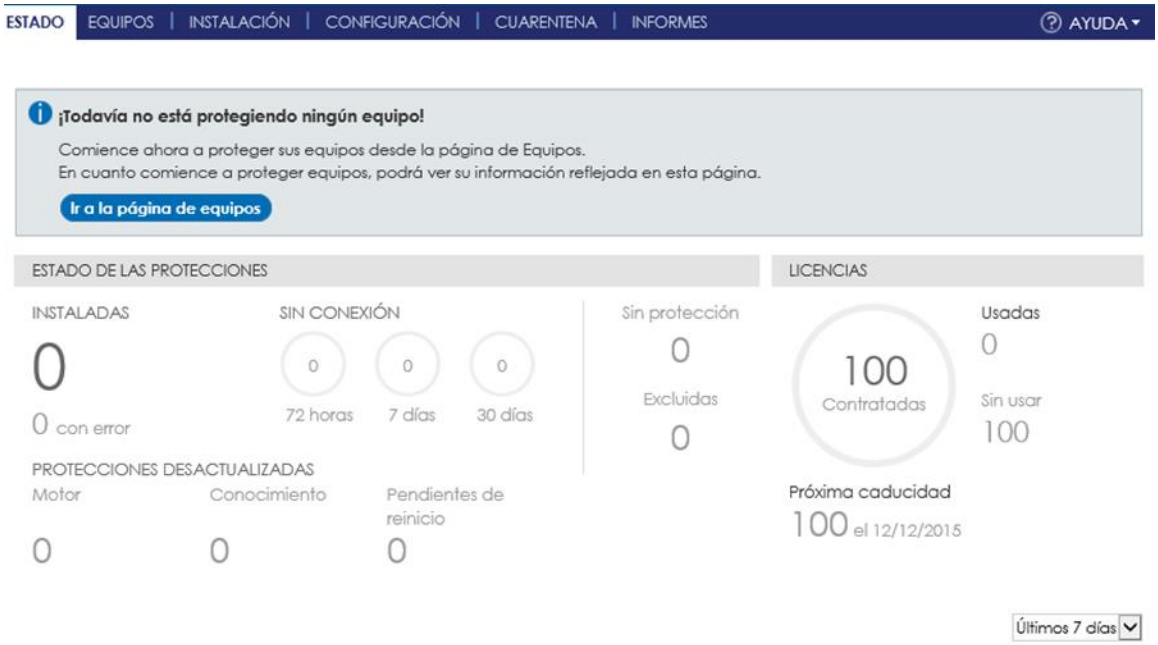
Una vez instalada la protección en los dispositivos podemos ver toda la información en la pestaña Estado del menú superior, el cual se estructura en tres secciones: Notificaciones, Licencias y Detecciones.

5.1. Notificaciones

Esta área se mostrará sólo cuando existan cuestiones que pueden ser de su interés, tales como la existencia de versiones nuevas del producto o avisos sobre incidencias técnicas, mensajes informativos acerca del estado de sus licencias, o cuestiones críticas que requieran especialmente su atención.

5.2. Licencias

Aquí podrá usted ver el número de licencias de Panda Multidispositivo que haya contratado.



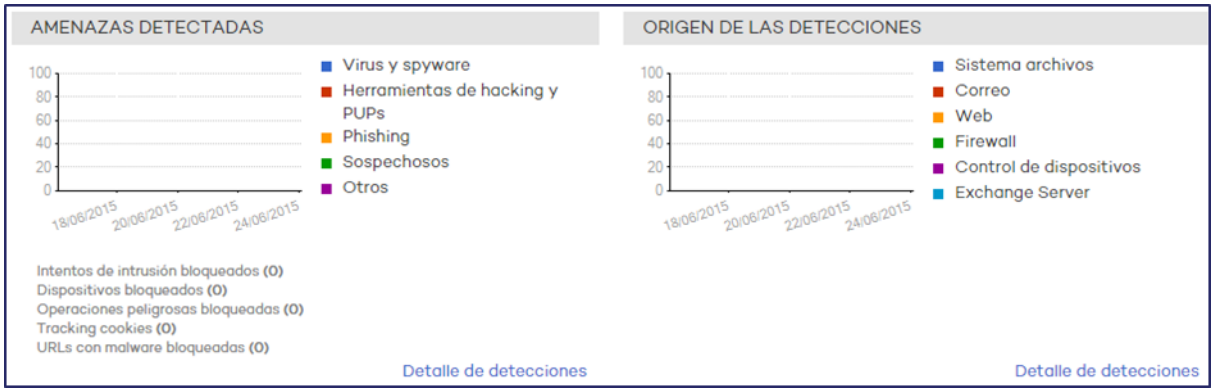
5.3. Detecciones

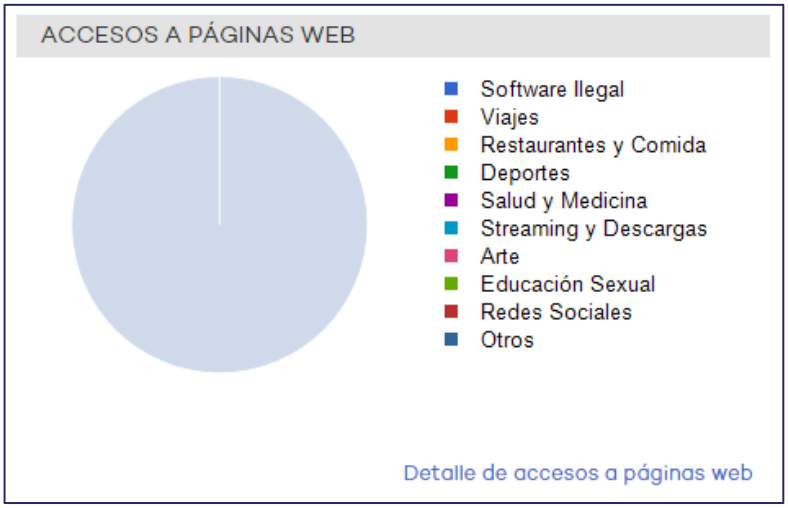
En el apartado "Estado", tenemos tres gráficas que nos muestran listados de las detecciones que Panda Multidispositivo ha hecho en las máquinas a través de los agentes.

Podemos visualizar "Listado de detecciones" por tipo de malware, donde para cada malware encontrado, se detallará el dispositivo donde se localizó, la ruta donde fue localizado, la acción ejecutada sobre dicho malware y otros datos de interés.

También podemos ver un "Listado de detecciones" por origen. Este listado muestra qué sección de la herramienta ha detectado el malware y también ofrece detalles sobre dichas detecciones.

Y por último, también se ofrece un listado de los "detalles de accesos a páginas web". Este listado está asociado al apartado de Control de acceso a páginas web que se configura para los perfiles. Aparecerán reflejados los accesos que los usuarios han hecho a distintas categorías de navegación definidas.

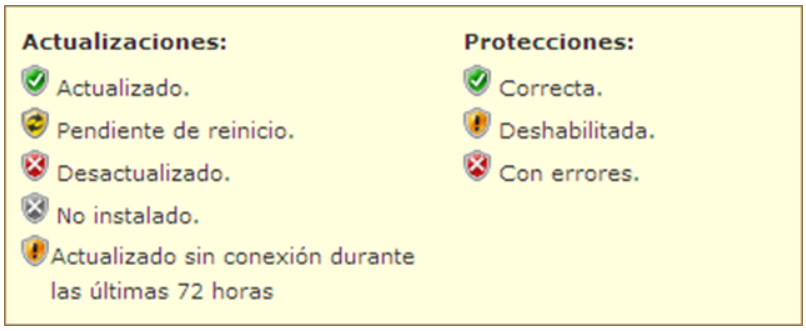

AMENAZAS DETECTADAS
100
80
60
40
20
0
18/06/2015
20/06/2015
22/06/2015
24/06/2015
Virus y spyware
Herramientas de hacking y PUPs
Phishing
Sospechosos
Otros
Intentos de intrusión bloqueados (0)
Dispositivos bloqueados (0)
Operaciones peligrosas bloqueadas (0)
Tracking cookies (0)
URLs con malware bloqueadas (0)
Detalle de detecciones
ORIGEN DE LAS DETECCIONES
100
80
60
40
20
0
18/06/2015
20/06/2015
22/06/2015
24/06/2015
Sistema archivos
Correo
Web
Firewall
Control de dispositivos
Exchange Server
Detalle de detecciones


ACCESOS A PÁGINAS WEB
Software Ilegal
Viajes
Restaurantes y Comida
Deportes
Salud y Medicina
Streaming y Descargas
Arte
Educación Sexual
Redes Sociales
Otros
Detalle de accesos a páginas web

6. Monitorización de los equipos

El área de Equipos ofrece una visión general del estado de la protección en los equipos que la integran, pero además también permiten conocer al detalle si la protección se ha instalado correctamente, si se ha producido algún error durante el proceso de instalación, si se encuentra a la espera de reinicio y cuál es su nivel de actualización.

Las columnas Actualización Protección, Actualización Identificadores, y Protecciones utilizan una serie de iconos para indicar el estado de actualización de las protecciones y la situación general de la protección en sí. La Leyenda utilizada es la siguiente:



7. Cuarentena

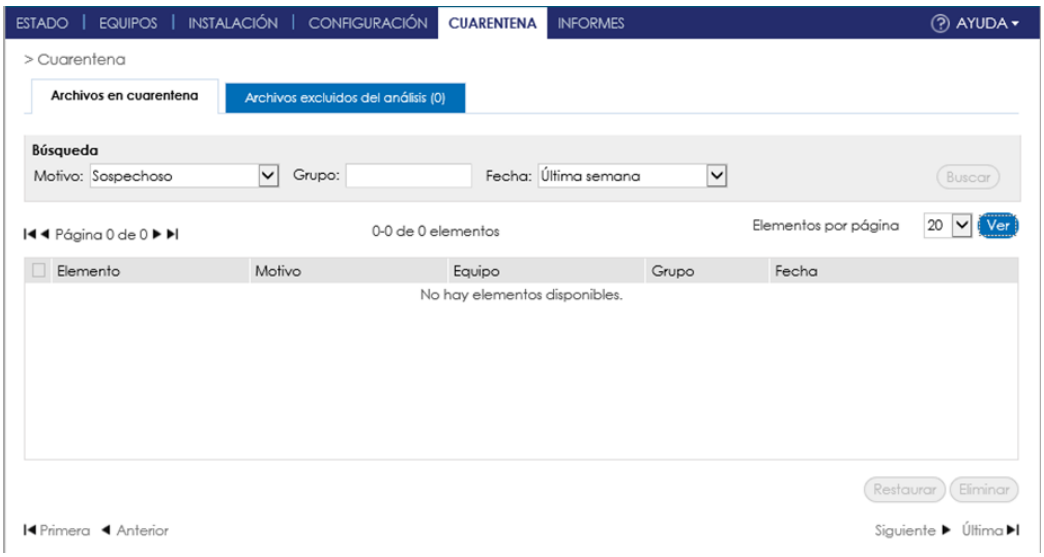
Panda Multidispositivo almacena en situación de cuarentena aquellos contenidos sospechosos de ser maliciosos o aquéllos no desinfectables, así como el spyware y herramientas de hacking detectadas. Una vez que los elementos sospechosos han sido enviados para su análisis, se pueden producir tres situaciones:

- Si se comprueba que los elementos son maliciosos, son desinfectados y posteriormente restaurados a su ubicación original, siempre y cuando exista desinfección para ello.
- Si se comprueba que los elementos son maliciosos y no existe manera de desinfectarlos, son eliminados.
- Si se comprueba que no se trata de elementos perjudiciales, son restaurados directamente a su ubicación.

En la ventana principal de la consola web, haga clic en Cuarentena para abrir la ventana del mismo nombre. La ventana se estructura en dos secciones: una zona de búsqueda y otra para mostrar el listado de elementos resultantes de dicha búsqueda.

Si desea restaurar algún elemento, marque la casilla correspondiente, haga clic en Restaurar y responda afirmativamente al mensaje de confirmación. A continuación, el elemento desaparecerá del listado de búsqueda y podrá usted encontrarlo en la pestaña Archivos excluidos del análisis.

Si lo que quiere es eliminar alguno de los elementos encontrados, seleccione la casilla correspondiente, haga clic en Eliminar y responda afirmativamente al mensaje de confirmación.



En el caso de que existan varios elementos que contengan el mismo tipo de malware, al restaurar o eliminar uno de ellos se restaurarán o eliminarán todos. Al situar el cursor sobre cualquiera de los elementos del listado de búsqueda, aparece una etiqueta amarilla con información sobre dicho elemento.

8. Informes

Con Panda Multidispositivo puede obtener informes sobre el estado de la seguridad en su red informática y las detecciones realizadas en un determinado periodo de tiempo. Además, puede también seleccionar el contenido que aparecerá en el informe, si quiere que la información sea detallada, y si desea acompañarla de gráficas. Todo ello de manera rápida y sencilla.

En la ventana principal de la consola web, haga clic en Informes. Podrá seleccionar entre tres tipos de informes, el período de tiempo y los perfiles sobre los que desea la información. Una vez seleccionadas las opciones haga click en el botón Generar informe al final de la pantalla.

8.1. Informe ejecutivo

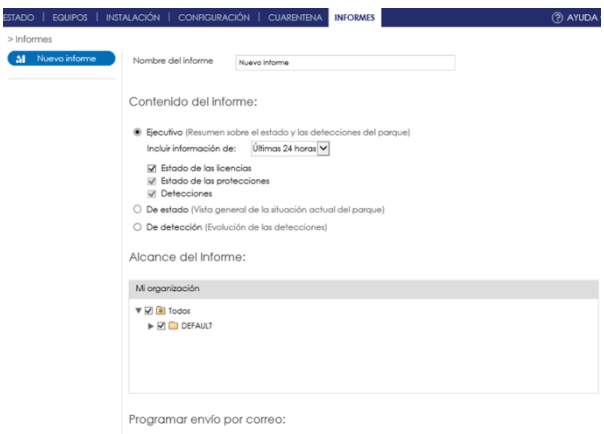
- Resumen del estado de las protecciones instaladas y las detecciones realizadas en las últimas 24 horas, últimos 7 días, o último mes.
- Listas top 10 de equipos con malware detectado y ataques bloqueados, respectivamente.
- Listas top 10 de equipos con dispositivos bloqueados. Información sobre el estado de las licencias contratadas.
- Detalle del número de equipos que se encuentran en proceso de instalación de la protección en el momento de generar el informe (se incluyen los equipos con error en la instalación).
- Informes sobre la cifra de spam detectado.

8.2. Informe de estado

- Proporciona una visión general del estado de las protecciones y sus actualizaciones en el momento de solicitar el informe.
- Detalle del número de equipos que se encuentran en proceso de instalación de la protección en el momento de generar el informe (se incluyen los equipos con error en la instalación).

8.3. Informe de detección

- Ofrece la evolución de las detecciones realizadas en las últimas 24 horas, últimos 7 días, o último mes.
- Detalla el equipo, grupo, tipo de detección, número de veces



9. Protección Android

9.1. Instalación

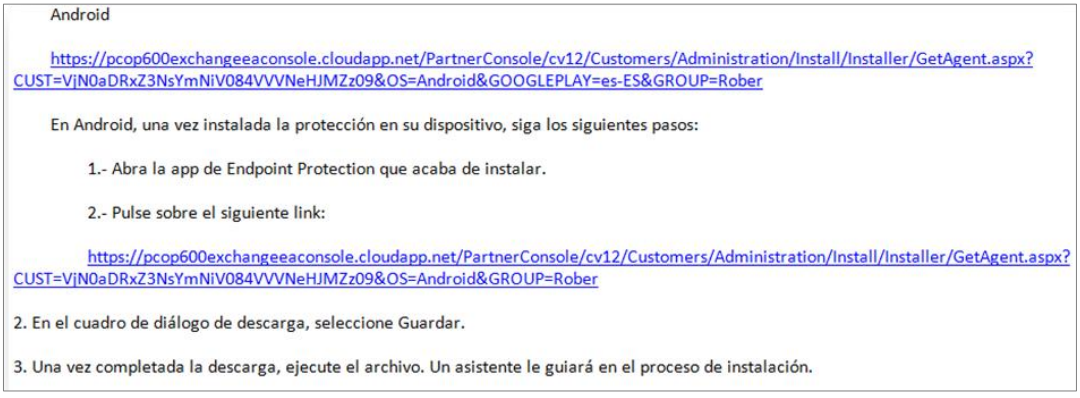
La instalación de la protección para Android consta de dos pasos:

1. Instalación de la APK en el dispositivo

2. Integración del dispositivo en el grupo deseado

Para ello, se podrán utilizar bien la descarga directa, la generación de la URL de instalación y el envío de email.

En cualquiera de los casos, tanto el link de descarga como en el de envío de email, una vez descargada e instalada la APK a través del primer link, habrá que integrarla utilizando el segundo link recibido:



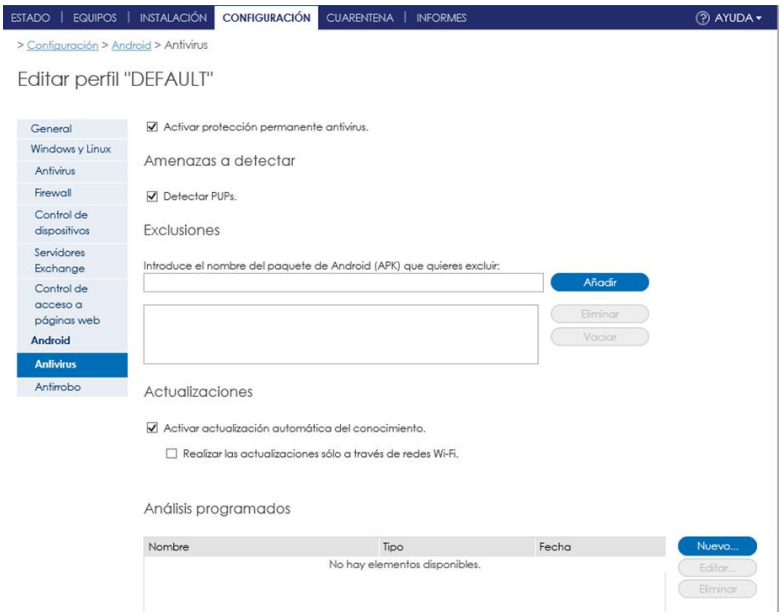
En el caso de seleccionar descarga del instalador Android, se mostrará la siguiente página con instrucciones. En este caso, se podrá utilizar un código QR para integrar el dispositivo en el grupo deseado.

9.2. Protección Antivirus

La protección antivirus para sistemas Android protege frente a malware y programas no deseados (PUPs). Cuenta con la posibilidad de excluir del análisis aquellas aplicaciones que no deseemos que sean analizadas.

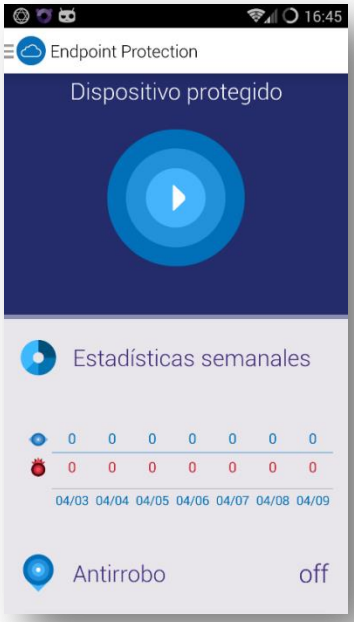
Además, se podrán lanzar análisis desde consola:

- Análisis inmediatos.
- Análisis programados.
- Análisis periódicos.



Localmente, la protección antivirus permite lanzar análisis inmediatos.

Cuenta con un historial de eventos y estadísticas semanales donde veremos los resultados de los análisis, actualizaciones etc.



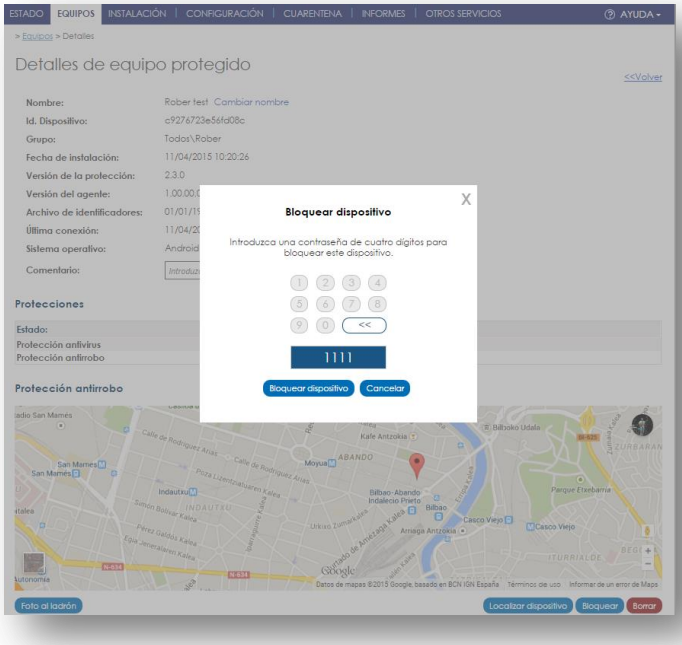
9.3. Protección antirrobo

Esta protección cuenta con las siguientes opciones:

- Bloqueo remoto
- Borrado remoto
- Geolocalización
- Foto al ladrón

9.4. Bloqueo remoto

Podemos enviar bajo demanda una orden de bloqueo del dispositivo desde los detalles del equipo. Se nos pedirá un PIN de cuatro dígitos que habrá que introducir en el dispositivo móvil para desbloquearlo.



9.5. Borrado remoto

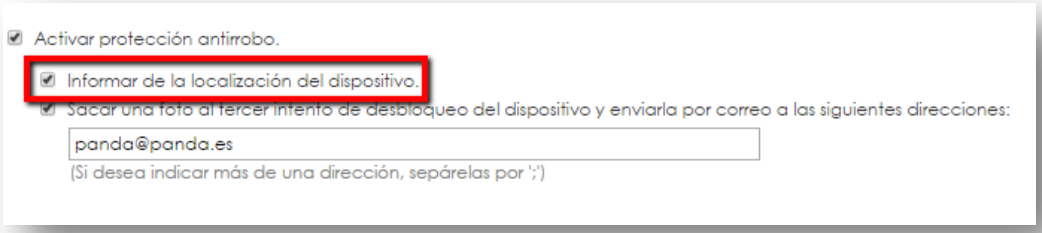
Del mismo modo, podemos borrar bajo demanda, los datos del dispositivo, así como los de la memoria externa, clicando al botón de Borrar en los detalles del equipo.

9.6. Geolocalización

También disponemos de la posibilidad de geo-localizar el dispositivo. Para ello, deberán estar activados los servicios de localización del dispositivo.

Podemos configurar en el perfil la opción de informar automáticamente de la localización del dispositivo. Teniendo esta opción activada, se enviará la ubicación a la consola

- Cuando el dispositivo se esté quedando sin batería.
- Cuando se pide una foto al ladrón
- Cuando se solicita una localización del dispositivo desde la pantalla de equipos.



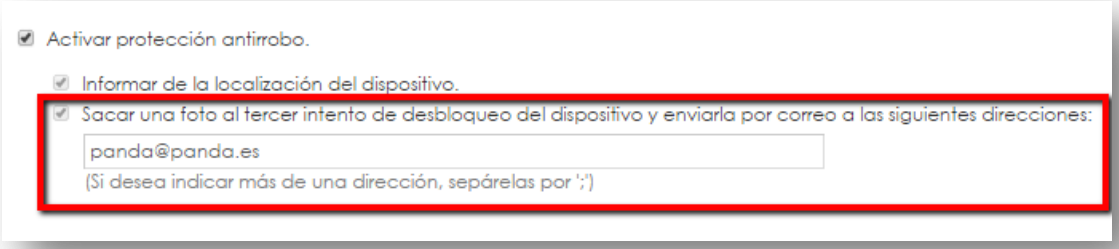
Adicionalmente podremos solicitar la localización del dispositivo en cualquier momento desde el detalle del equipo.

9.7. Foto al ladrón

Esta funcionalidad nos permitirá obtener una fotografía a través de la cámara frontal (o trasera si el dispositivo no dispone de cámara frontal) y enviarla a la dirección o direcciones de correo configuradas. El objetivo es poder identificar al ladrón en el caso de que el dispositivo haya sido sustraído.

Al igual que la funcionalidad de localización, esta funcionalidad dispone de dos modos, automático y bajo demanda.

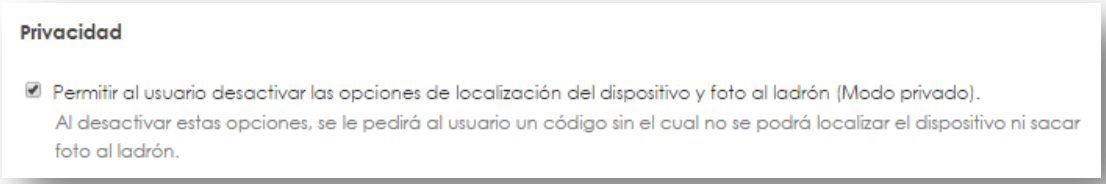
El modo automático es configurado desde el perfil que se aplica al dispositivo y tomará una foto siempre que se intente desbloquear el dispositivo tres veces consecutivas de manera incorrecta, y enviará la foto a la o las direcciones de correo configuradas.



Al igual que las otras opciones, se podrá lanzar la petición de foto bajo demanda desde la consola de gestión, en el detalle del equipo. En este caso se solicitará la dirección a la que enviar la foto.

9.8. Modo privado

En la configuración del perfil se puede activar la posibilidad de permitir al usuario del dispositivo móvil desactivar las opciones de localización y foto al ladrón.



Al activar el modo privado en el móvil, el usuario deberá configurar en el dispositivo un código de cuatro caracteres o más, que será necesario posteriormente para poder localizar o sacar una foto al ladrón en caso de pérdida o robo.

En colaboración con: