TRUST IN GERMAN SICHERHEIT

G DATA

# TechPaper N.º 0273

# Gestión de dispositivos móviles

# Desarrollo de aplicaciones G DATA

# Contenido

# 1. Introducción

Tradicionalmente, los administradores de redes corporativas y sistemas han gestionado grupos homogéneos de dispositivos cliente. El proceso de planificación e implantación de clientes de red se limitaba casi exclusivamente a ordenadores de sobremesa. Esta previsibilidad simplificaba la implementación de la infraestructura de la red, del hardware de los clientes y de las aplicaciones, garantizando la uniformidad de todos los dispositivos de red. Sin embargo, desde que los smartphones y tabletas han irrumpido en la electrónica de consumo, el panorama tecnológico se ha complicado enormemente. Tendencias como Consumerización de TI y Bring your Own Device (BYOD, «trae tu propio dispositivo»), han llevado la diversidad de dispositivos a la empresa. A los administradores les queda la tarea de proporcionar amplio acceso a los recursos sin descuidar la seguridad. El objetivo de este TechPaper es esbozar las tendencias de uso de smartphones y tabletas en redes corporativas (capítulo 2) así como las estrategias prácticas de gestión para administradores que se enfrentan a un uso cada vez mayor de dispositivos móviles (capítulo 3). El capítulo 4 trata del uso de G Data Mobile Device Management.

# 2. Dispositivos móviles en la empresa

En entornos empresariales, la tecnología se adopta de forma considerablemente más lenta que el ritmo al que los consumidores se hacen con nuevos dispositivos. Incluso si un producto se puede incorporar fácilmente en los flujos de trabajo, ha de probarse su compatibilidad con la infraestructura corporativa, un proceso que puede resultar costoso en tiempo y recursos. Desde que Apple popularizó la categoría de dispositivos móviles con el lanzamiento de sus productos iPhone y iPad, cientos de millones de usuarios particulares y corporativos se han enganchado a esa combinación de tecnología avanzada y facilidad de uso. Sin embargo, muchas corporaciones luchan todavía para integrar estos dispositivos adecuadamente en el ámbito empresarial. Este retardo en la adopción genera a menudo tensión entre las expectativas del usuario final y la funcionalidad que pueden ofrecer las soluciones implementadas en la empresa en la actualidad. En la TI empresarial, podemos hablar de dos tendencias principales para salir del laberinto: Consumerización de TI y Bring your Own Device (BYOD, «trae tu propio dispositivo»).

La llamada Consumerización de TI, la influencia de los dispositivos de uso particular en las soluciones de TI de la empresa, ha crecido inmensamente. Los usuarios finales se han acostumbrado a una Internet móvil siempre accesible, correo electrónico y mensajería basados en la nube, así como enormes cantidades de aplicaciones para personalizar su movilidad. Aunque ningún administrador negaría que el uso de estos servicios es muy cómodo, algunas de sus ventajas suponen riesgos para las estructuras empresariales de TI. El ritmo al que aparecen nuevas aplicaciones para plataformas móviles excede con mucho la capacidad de los administradores para probar la compatibilidad y seguridad de cada una de ellas. El uso de servicios en la nube implica con frecuencia almacenar datos en servidores gestionados por terceros. A pesar de que los usuarios finales dan por sentado que dispondrán de dichos servicios en sus dispositivos, no todas las empresas están técnicamente preparadas para ofrecerlos en el marco de las políticas de TI vigentes.

Incluso cuando los dispositivos y servicios móviles no se implementan activamente en un entorno empresarial, no significa que los administradores no vayan a encontrárselos. Esta tendencia se denomina

Bring your Own Device (BYOD, «trae tu propio dispositivo»): los usuarios finales llevan al trabajo sus propios dispositivos y esperan poder usar la infraestructura de la empresa, como acceso a la Wi-Fi y recursos compartidos de la red. Del mismo modo, muchas configuraciones de servidor de correo permiten el acceso remoto mediante dispositivos móviles, independientemente de si ese dispositivo está gestionado o no. BYOD suele provocar exabruptos: para estar seguros de que no se filtran datos confidenciales o de que no penetra software malicioso en la red, se bloquean los dispositivos móviles para que no entren en la infraestructura corporativa en absoluto, o se limita mucho su funcionalidad mediante directivas estrictas.

Pero por extraño que pueda sonar, hay que darse cuenta de que el uso de dispositivos móviles en la empresa no es una cuestión de blanco o negro. Puede parecer que BYOD y Consumerización de TI vienen a desestabilizar un entorno perfectamente organizado, pero implementar dispositivos corporativos o gestionar los privados comporta distintos beneficios. Una solución de gestión de dispositivos puede ayudar a sacar partido de los aspectos positivos del uso de dispositivos móviles limitando el impacto sobre el resto de la infraestructura de la empresa.

## 2.1. Beneficios

La integración de smartphones y tabletas en flujos de trabajo corporativos tiene evidentes ventajas, independientemente de si se trata de una implantación centralizada o de si los traen los empleados. Ofrecer acceso móvil a los recursos de la empresa puede aumentar enormemente la productividad para los trabajadores remotos y autónomos. Una combinación de controles de acceso y gestión de dispositivos posibilita un uso seguro y eficaz de sus dispositivos para acceder a los recursos de la empresa desde fuera de la oficina. Estar de viaje ya no implica pérdida de comunicación: los empleados pueden consultar a distancia el correo electrónico, la agenda y las notificaciones.

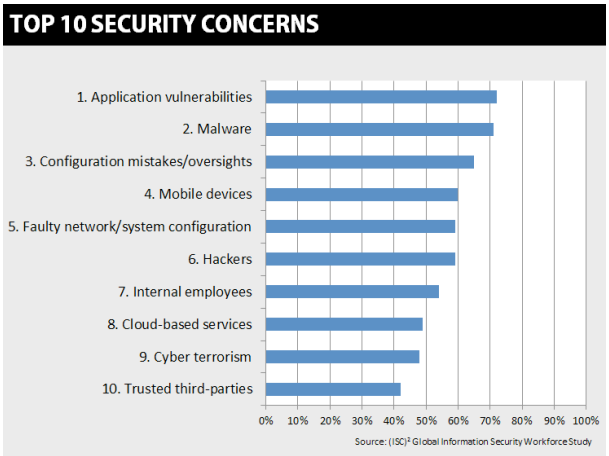
Las aplicaciones y dispositivos corporativos suelen presentar grandes inconvenientes de usabilidad, mientras que la tecnología de consumo está pensada normalmente para que la maneje el usuario final. Esto reduce la curva de aprendizaje para los empleados, que se acostumbrarán enseguida a los dispositivos que suministra la empresa.

Por último, en un entorno BYOD, las empresas ahorran dinero al no tener que invertir mucho en incorporar dispositivos. En lugar de comprar e incorporar nuevos smartphones y tabletas, se puede equipar a los dispositivos de los empleados con software de gestión del dispositivo para su uso corporativo. Así, las empresas dejan de ser responsables de la sustitución de dispositivos cuando los empleados pierden o rompen smartphones o tabletas.

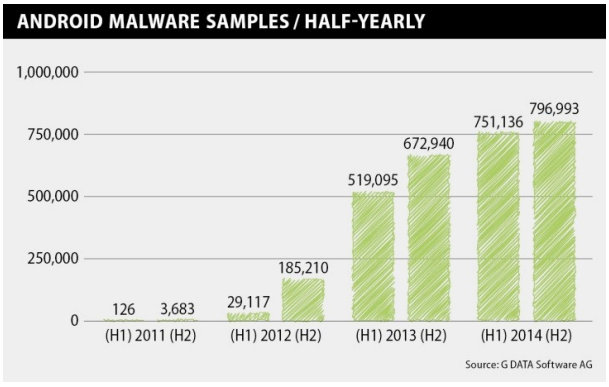
## 2.2. Riesgos

Aunque la adopción de dispositivos móviles puede tener muchos aspectos positivos para la productividad de la empresa, hay ciertos problemas. Los dispositivos móviles figuraban en el cuarto lugar entre las preocupaciones de seguridad en el Estudio global de la fuerza laboral de seguridad de la información 2015 de la Fundación del (ISC)2[1]. Igual que con los PC, los dispositivos móviles se ven afectados por el malware. Android e iOS están especialmente en riesgo: con una cuota conjunta de mercado del 96,3 por ciento[2], son un objetivo predilecto de los delincuentes. En 2014, los expertos de seguridad de G Data investigaron más de 1,5 millones de muestras de malware para Android, un 30% más que en 2013[3]. El malware de Android se usa para múltiples propósitos perversos, entre ellos:

- Robar datos, como correos electrónicos, datos de inicio de sesión y documentos confidenciales.
- Causar costes excesivos enviando mensajes SMS a números de teléfono con recargo (extranjeros)
- Espiar aplicaciones bancarias móviles
- Bloquear dispositivos para conseguir un rescate (ransomware)




Sin embargo, el malware no es la única amenaza para los dispositivos móviles. Al navegar por Internet, los sitios de phishing pueden tratar de convencer al usuario para que introduzca datos personales en un formulario aparentemente inocuo. E incluso si el dispositivo en sí es seguro, esto no significa que se pueda usar con seguridad en un entorno corporativo. Cuando los empleados utilizan dispositivos móviles para acceder a documentos corporativos, hay que asegurarse de que no se filtra la información confidencial, sea por accidente (por ejemplo, subiéndola a un servicio para compartir archivos) o a propósito (alguien infiltrado).




Además de los riesgos de seguridad, los dispositivos móviles pueden mermar la productividad. El uso de aplicaciones se debe restringir para garantizar que los empleados no dedican demasiado tiempo a juegos o pasatiempos. La gestión de contactos puede ayudar a reducir la funcionalidad del teléfono a lo estrictamente necesario, ahorrando tiempo y costes.

Los beneficios del uso del dispositivo móvil en la empresa superan a los riesgos. Sin embargo, estos últimos se deben mitigar. Una política de gestión de dispositivos integrada puede ayudar a controlar los riesgos de seguridad y los problemas de productividad, garantizando un uso seguro y eficiente de smartphones y tabletas.

[1] Fuente: Fundación del (ISC)2, https://www.isc2cares.org/IndustryResearch/GISWS/
[2] CY14. Fuente: IDC, https://www.idc.com/getdoc.jsp?containerId=prUS25450615
[3] Fuente: Informe de malware móvil G DATA 2S/2014

# 3. Gestión de dispositivos móviles

Como administrador, ignorar consumerización y BYOD es casi imposible. Los usuarios finales continuarán pidiendo a la empresa smartphones y tabletas que mantengan la usabilidad a la que están acostumbrados. Si estos dispositivos no se implementan activamente, ellos se traerán los suyos. Teniendo en cuenta las ventajas que los dispositivos móviles pueden suponer para la productividad, el objetivo de la gestión de dispositivos móviles debe ser maximizar la productividad mientras se garantiza la seguridad y se minimizan los costes.

## 3.1. Implementación y administración

Antes de que smartphones y tabletas puedan gestionarse con una solución de gestión de dispositivos móviles, se tienen que implementar. La implementación supone una conexión inicial única entre el dispositivo y el servidor, después de la cual el dispositivo informará periódicamente al servidor y podrá gestionarse remotamente. La comunicación entre el servidor y el dispositivo se produce en forma de tráfico de Internet (cuando se puede establecer una conexión directa con el servidor), mensajes Push (normalmente basados en soluciones de mensajería en la nube propias del vendedor) o mensajes SMS (cuando no hay una conexión móvil a Internet disponible). No es necesaria una comunicación permanente entre el dispositivo y el servidor: el dispositivo puede cumplir con las políticas del servidor incluso si no hay contacto con este. Esto significa que los dispositivos están protegidos en todo momento, incluso fuera del ámbito de la empresa.

La implementación se ha de simplificar al máximo. Los dispositivos nuevos, gestionados por la empresa, deben ir siempre provistos de funciones de gestión de dispositivos móviles antes de que se les entreguen a los empleados. A los dispositivos BYOD se les debe impedir el acceso a la red corporativa y a sus recursos hasta que se les haya equipado con gestión de dispositivos móviles. Opcionalmente, se puede usar una red para invitados para los dispositivos que no cumplan con los requisitos o que usen los visitantes.

Para evitar que aumente la carga de trabajo, los administradores deben escoger una solución de gestión de dispositivos que se integre con las estructuras de gestión de las que ya disponen. Se debe evitar el uso de varios *back-ends*. Idealmente, los dispositivos móviles se pueden gestionar usando el mismo tipo de interfaz y capacidades de generación de informes que ya están disponibles para otros tipos de dispositivos en la red, para que sean compatibles con un flujo de trabajo integrado y una configuración consistente.

Para dispositivos BYOD, hay que tener en cuenta los aspectos legales de la gestión de dispositivos. Como este tipo de dispositivos no es propiedad de la empresa, los administradores no tienen automáticamente derecho a gestionarlos.

Permisos como el de borrado remoto pueden resultar conflictivos. Dependiendo de la situación legal, es posible que las empresas tengan que pedir permiso al usuario final antes de añadir un dispositivo a la gestión de dispositivos móviles. Es recomendable definir un acuerdo de licencia de usuario final (EULA) que explique las acciones que la empresa tiene que ser capaz de realizar sobre el dispositivo. El usuario final puede aceptar o rechazar el acuerdo, pero si no firma el EULA no podrá acceder a los recursos corporativos. El EULA puede ser útil incluso para dispositivos que no sean BYOD.

## 3.2. Antirrobo

Los dispositivos móviles aumentan los niveles de riesgo para la infraestructura física y los flujos de trabajo basados en la información. Entre los empleados que llevan consigo archivos confidenciales mientras están de viaje y los dispositivos móviles que se roban o extravían, nunca ha sido más fácil que se filtre accidentalmente información reservada. Para asegurarse de que no se pueda acceder a los correos, documentación y otra comunicación corporativa cuando se robe o se pierda un dispositivo, se pueden definir varias medidas. Primero, puede ser útil intentar recuperar el dispositivo. Usar la tecnología GPS o activar una alarma puede servir para localizarlo. Si no se puede localizar el dispositivo por cualquier motivo, este puede inutilizarse bloqueándolo. Como última opción, los dispositivos se pueden reiniciar a los valores de fábrica, borrando todos los datos que contengan.

## 3.3. Aplicaciones

Parte del encanto de los dispositivos móviles es que su funcionalidad se puede ampliar instalando aplicaciones. Incluso en el ámbito corporativo, esto puede resultar muy práctico: las herramientas de productividad o las aplicaciones de configuración pueden aumentar considerablemente los usos de los dispositivos móviles.  A la vez, los dispositivos corporativos deben proporcionar un entorno controlado, asegurándose de que las aplicaciones no causan problemas de compatibilidad, filtran información confidencial ni difunden malware. La gestión de aplicaciones es una forma potente de controlar la funcionalidad de un dispositivo móvil, conjugando seguridad y usabilidad.

Separar las aplicaciones buenas de las malas puede ser una tarea complicada. Algunas aplicaciones, como los juegos, resultan claramente inapropiadas para el ámbito corporativo. Otras pueden tener un sentido, pero pueden conllevar riesgos de privacidad, como los servicios para compartir archivos online. Incluso las aplicaciones que parecen inocuas pueden ponerse en peligro después, bien por fallos de seguridad, bien porque están afectados sus servicios *backend*, o porque transmiten información de forma no segura. La productividad también cuenta: por ejemplo, los empleados que solo necesitan un smartphone para hacer llamadas y concertar citas solo deberían tener acceso al teléfono y al calendario, mientras que los empleados que trabajan en ruta con documentos tendrían acceso al navegador, aplicaciones ofimáticas y otros componentes necesarios.

## 3.4. Protección en tiempo real y a petición

Igual que los clientes de escritorio y portátiles, los clientes móviles también son vulnerables a los ataques online. En particular, los dispositivos Android con permisos de superusuario no tienen suficientes permisos de protección contra aplicaciones maliciosas de fuentes desconocidas, pero incluso las aplicaciones malintencionadas que consiguen colarse en las tiendas de aplicaciones oficiales pueden ser devastadoras. De la misma forma, los sitios web pueden intentar introducir malware, aprovecharse de vulnerabilidades del sistema operativo o engañar al usuario. Como con los ordenadores de sobremesa, los sitios web de phishing pueden tratar de persuadir a los usuarios para que les faciliten contraseñas u otros datos reservados. Para defenderse de estos ataques, se deben configurar medidas de protección en todos los dispositivos móviles gestionados.

La protección en tiempo real protege los dispositivos en todo momento sin que intervenga el usuario. Incluye tecnologías como protección contra el phishing y comprobación automática de virus. La protección a petición, en cambio, la activa el usuario final o el administrador. Por ejemplo, se puede

iniciar manualmente una comprobación de virus para estar seguros de que no se han instalado previamente aplicaciones maliciosas en el dispositivo.

Las soluciones en tiempo real y a petición dependen en gran medida de la plataforma cliente. Mientras que los clientes Android son especialmente propensos a las aplicaciones maliciosas, los dispositivos iOS son más vulnerables a pérdidas de datos o amenazas de phishing. Las soluciones de gestión de dispositivos móviles deben ofrecer medidas para adaptarse de forma óptima a cada plataforma móvil: un módulo para todo no sirve para las innumerables amenazas a las que se enfrentan los dispositivos.

## 3.5. Filtrado y gestión de contactos

Para los dispositivos que se usan en el ámbito corporativo, puede ser esencial controlar los flujos de comunicación. Puede ser útil bloquear las aplicaciones si la comunicación se debe evitar totalmente, pero en ciertas situaciones se debe implementar un filtro más sutil. En lugar de bloquear completamente la aplicación de teléfono si un dispositivo se va a usar solo para comunicaciones de trabajo, se pueden filtrar las llamadas entrantes y salientes que no cumplan con los criterios corporativos. Por ejemplo, una empresa que proporciona móviles a sus empleados para comunicarse con la oficina mientras están de viaje podría bloquear todas las llamadas excepto las previamente aprobadas como contactos corporativos.

Para la gestión de los contactos es esencial una agenda de contactos gestionada. Los contactos almacenados en el dispositivo se pueden sincronizar con el servidor central y los administradores pueden enviar los nuevos números de teléfono a los dispositivos. Igual que la gestión de aplicaciones, la gestión de contactos se puede usar para dispositivos individuales, pero es mejor combinarla con gestión por grupos. Los números de teléfono individuales se pueden permitir o bloquear para grupos de dispositivos, o se puede enviar una agenda de contactos corporativa completa a todos los dispositivos.

# 4. Utilizar G Data Mobile Device Management

G Data ofrece un módulo de gestión de dispositivos móviles como parte de sus soluciones corporativas. Tanto G Data AntiVirus Business como G Data Client Security Business, G Data Endpoint Protection Business y G Data Managed Endpoint Security incluyen el componente Mobile Device Management, compatible con iOS y Android. Se integra totalmente con otras partes de las soluciones corporativas y se puede gestionar desde la misma aplicación (G Data Administrator). Esto supone una clara ventaja con respecto a las soluciones independientes, que se tienen que administrar aparte y cuya curva de aprendizaje es por lo general más dilatada.

## 4.1. Android

G DATA Mobile Device Management para Android se realiza a través de G Data Internet Security para Android. La funcionalidad de la aplicación se gestiona de forma centralizada a través de G Data Administrator y ofrece todo un conjunto de funciones de seguridad y productividad para todos los dispositivos a partir de Android 2.3.

### 4.1.1. Implementación y administración

El primer paso es implementar G Data Internet Security para Android en todos los dispositivos Android. Para asegurarse de que al servidor solo se pueden conectar clientes de red autorizados, hay que definir una contraseña en el lado del servidor antes de instalar en ningún cliente. Después se tiene que introducir la misma contraseña en la aplicación para permitir la autenticación con G Data ManagementServer. Las instalaciones de los clientes se inician usando G Data Administrator. El proceso de implementación se realiza a través de correo electrónico. Se puede enviar a una o más direcciones un correo electrónico de activación que contiene un enlace al archivo de instalación Después de descargar el archivo en el cliente Android y de confirmar los permisos solicitados, se instalará G Data Internet Security para Android y se podrá iniciar desde el menú de aplicación de Android. La implementación se completa conectando la aplicación Android con ManagementServer, después de lo cual se conectará al servidor para inmediatamente descargar la configuración de gestión de dispositivos móviles.

Tan pronto como se conecte a ManagementServer, el dispositivo aparecerá automáticamente en G Data Administrator. Como los dispositivos Android aparecen como clientes en la lista normal de clientes, se pueden mover a grupos. Es aconsejable crear un grupo dedicado, con subgrupos para los distintos tipos de acceso de dispositivo (corporativo, privado o mixto), para los distintos departamentos que usan Android o con cualquier otro criterio. Esto permite una administración eficiente y así el dispositivo hereda automáticamente la configuración correcta.

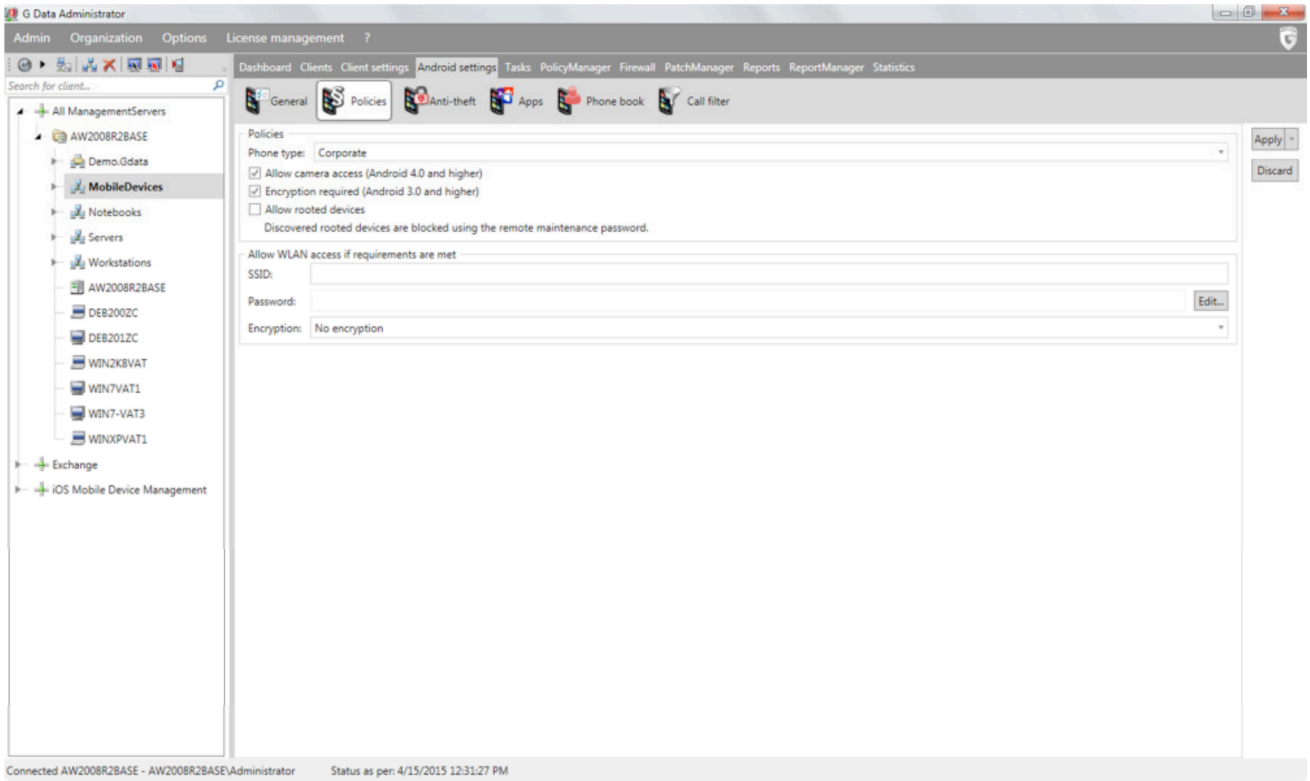



*Imagen 1: G Data Administrator, Ajustes Android, Políticas*

Para cada dispositivo o grupo, se puede definir un tipo de teléfono en AJUSTES ANDROID > POLÍTICAS. Para dispositivos entregados por la empresa y que sean solo para uso corporativo, se recomienda el tipo de teléfono CORPORATIVO. Esto bloqueará los menús de ajustes de la parte del cliente de Internet Security para Android, con lo que los usuarios no pueden cambiar involuntariamente los ajustes

gestionados de forma remota al conectarse a la red de la empresa. Los teléfonos de tipo PRIVADO se pueden utilizar para dispositivos que no haya entregado la empresa. Esto posibilita que el usuario final tenga acceso total a los ajustes de Internet Security para Android. El tipo de teléfono MIXTO sirve para los dispositivos entregados por la empresa que se usan tanto con fines corporativos como para la comunicación privada.

Algunos ajustes básicos se deben configurar directamente después de implementar un dispositivo nuevo. Se deben definir siempre una programación de actualizaciones y la sincronización. Ambos ajustes dependen del uso habitual del dispositivo. Los dispositivos que se conecten a menudo a una red inalámbrica (WLAN) se pueden configurar para que actualicen sus firmas de virus automáticamente y para que sincronicen sus datos con ManagementServer cada pocas horas. Los dispositivos que se usan principalmente fuera de la red de la empresa o que se conectan a Internet con la conexión de datos móvil, se pueden configurar para que se actualicen con menos frecuencia, o manualmente, o solo cuando se conecten por Wi-Fi. Esto mismo se aplica a la sincronización: se pueden configurar distintos ajustes para Wi-Fi o conexión de datos móvil. Si es necesario, a los dispositivos se les puede asignar un acuerdo de licencia de usuario final. Por imperativo legal, es posible que las empresas tengan que informar a sus usuarios finales de que su dispositivo se puede gestionar remotamente.

### 4.1.2. Antirrobo

Las medidas antirrobo se pueden activar tanto automática como manualmente. Algunas se pueden configurar para que se ejecuten si le sucede algo al dispositivo (como un cambio de tarjeta SIM). Otras se pueden activar mediante G Data Administrator para que envíen un comando a través de Google Cloud Messaging. Por último, los comandos se pueden enviar por SMS.

Para habilitar todas las medidas se tienen que configurar varios ajustes en AJUSTES ANDROID > ANTIRROBO. Para usar comandos SMS es necesario introducir una contraseña de mantenimiento remoto (un código PIN numérico). También funcionará como contraseña de bloqueo de pantalla si esta no se ha definido explícitamente. Se necesita configurar un número de teléfono de confianza para estar seguros de que el comando de reinicio de la contraseña de mantenimiento remoto no lo puede enviar cualquiera: solo funcionará si se envía desde el teléfono de confianza. Finalmente, se debe introducir una dirección de correo electrónico para recibir información de las acciones.

Cuando un dispositivo se roba o se pierde, el procedimiento más rápido para ejecutar una acción es enviarle un SMS. Los administradores pueden seleccionar individualmente los comandos que se pueden enviar al dispositivo. Están disponibles las siguientes medidas:

- Enviar al administrador un correo electrónico con los datos de la ubicación.
- Reiniciar el dispositivo a los valores de fábrica. Se borrarán todos los datos personales.
- Activar un sonido de alarma.
- Silenciar todos los tonos de llamada, excepto el activado por la opción de sonido de alarma.
- Activar el bloqueo de pantalla utilizando la contraseña de bloqueo de pantalla.
- Establecer la contraseña de bloqueo de pantalla.

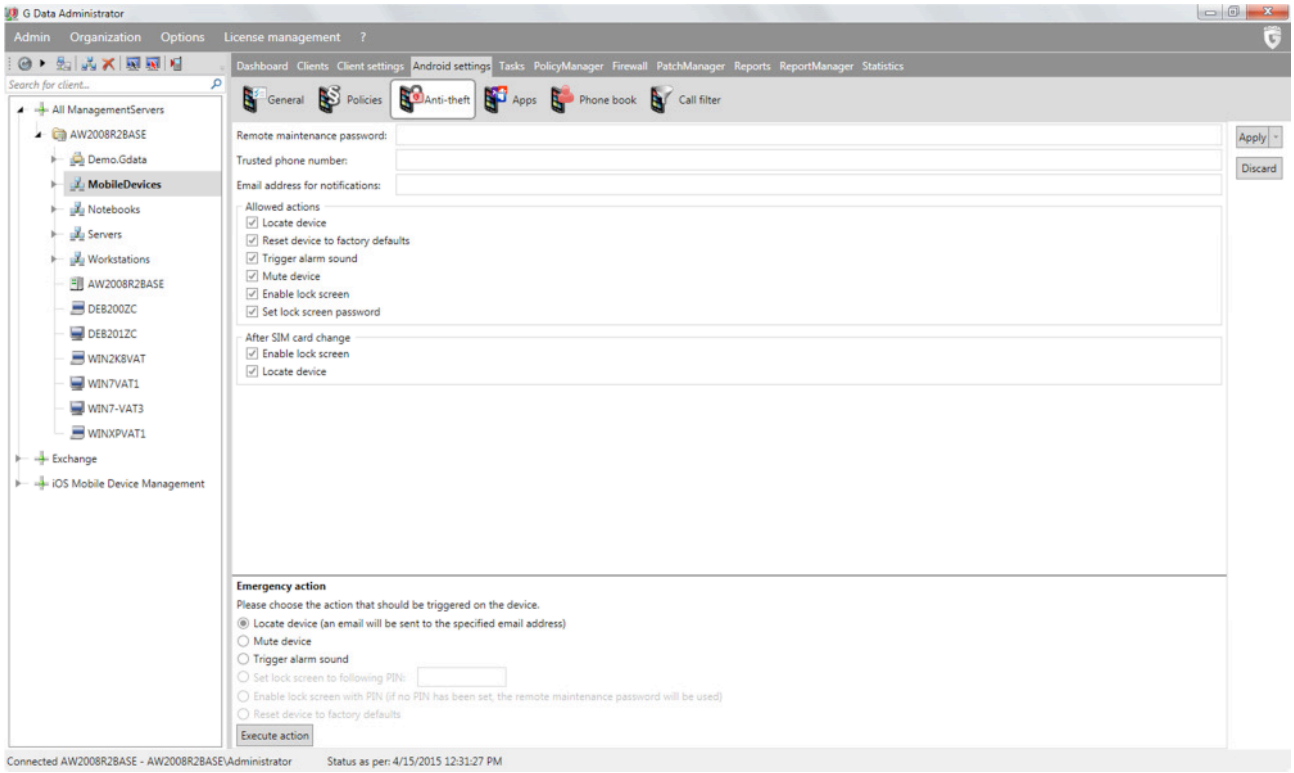



*Imagen 2: G Data Administrator, Ajustes Android, Antirrobo*

Si se roba un dispositivo, por lo común se le quita la tarjeta SIM para evitar que el dueño contacte con el dispositivo a través del número de teléfono. Esto significa que los SMS no llegarán al dispositivo. Como contramedida, se pueden definir acciones automáticas en caso de que se cambie la tarjeta SIM. Se puede habilitar el bloqueo de pantalla del teléfono, volviendo el dispositivo inaccesible, y el dispositivo se puede localizar. Además de las medidas basadas en SIM y SMS, se puede iniciar varias acciones a través de G Data Administrator. El dispositivo no tiene que estar conectado a la red del ManagementServer para que funcionen: utilizan Google Cloud Messaging, un servicio online de Google que permite enviar comandos a dispositivos Android[4].

Como las acciones antirrobo pueden afectar mucho la usabilidad del teléfono (p. ej., borrando sus datos), es recomendable informar al usuario final a través del EULA.

### 4.1.3. Aplicaciones

G Data Mobile Device Management para Android ofrece posibilidades de gestión de aplicaciones muy elaboradas. Como primer paso, se puede usar para hacer inventario de las aplicaciones en uso en los dispositivos móviles de la red. Cada aplicación instalada figura con su nombre, versión y tamaño. Para cada aplicación, los administradores obtendrán información del vendedor, funciones e historial de versiones, siempre que dicha información esté disponible. Para muchas aplicaciones las tiendas oficiales proporcionan detalles suficientes, mientras que para otras será necesario acudir a la página del vendedor. A partir de esta información y por el uso previsto del dispositivo (basándose en el grupo y tipo de dispositivo y en la zona de red), las aplicaciones se pueden añadir a la lista negra o a la lista blanca.

[4] Es preciso disponer de una cuenta de Google Cloud Messaging, cuyo registro es gratuito con Google en https://code.google.com/apis/console/.

Esto permitirá o bloqueará las aplicaciones de la lista que corresponda. Mediante la contraseña definida, se puede bloquear la ejecución de las aplicaciones.

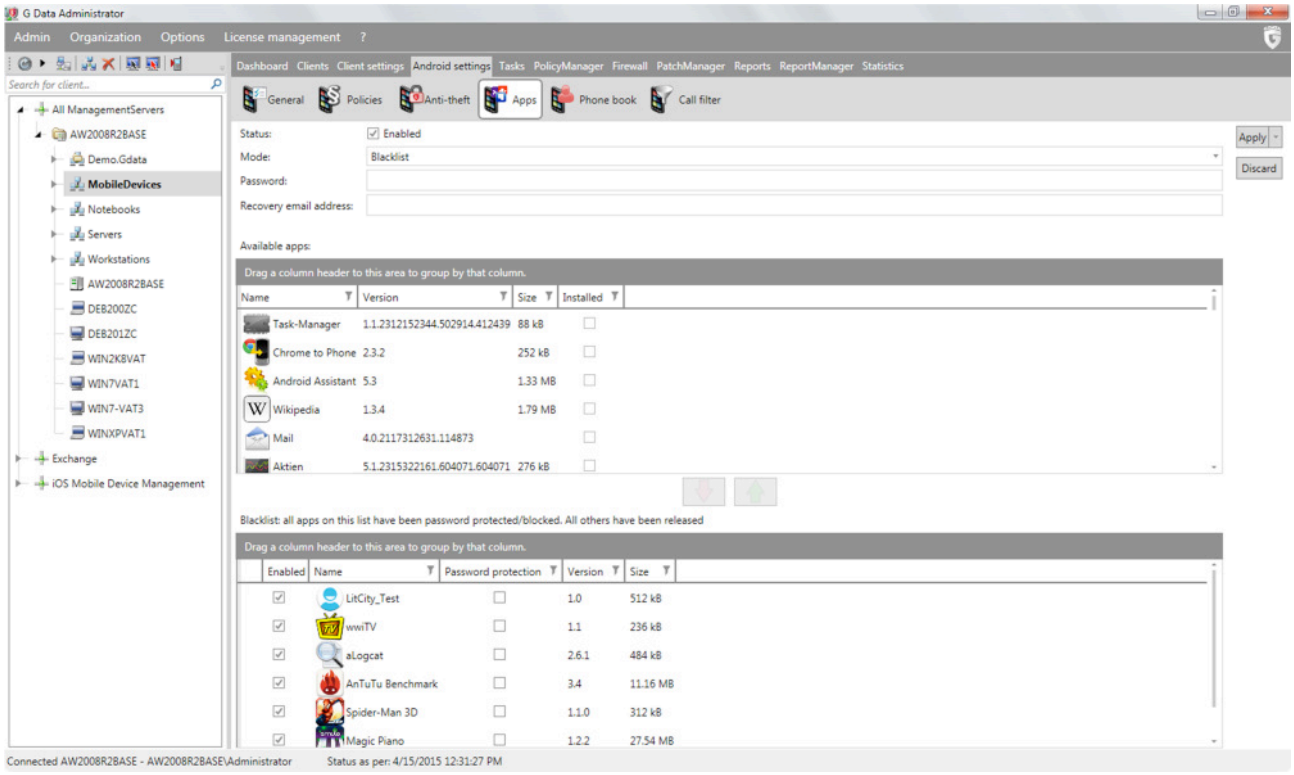



*Imagen 3: G Data Administrator, Ajustes Android, Aplicaciones*

La estrategia de usar la lista blanca o la lista negra depende del grado de bloqueo deseado para el dispositivo. Cuando la gestión de aplicaciones se usa en modo de lista negra, se puede configurar fácilmente para dispositivos multiusos en los que el usuario final debe poder instalar aplicaciones nuevas sin autorización previa. El riesgo consiste en que se puede instalar y ejecutar básicamente cualquier aplicación. Solo después de que un administrador la bloquee manualmente los usuarios tendrán prohibido el acceso. Un método más seguro, pero más restrictivo, es el de lista blanca: no se puede instalar ninguna aplicación en el dispositivo a menos que se haya añadido a la lista blanca. Esto es particularmente útil en casos en los que un dispositivo se configure para un único uso. Los administradores pueden preinstalar las aplicaciones necesarias, incluirlas en la lista blanca, e impedir el acceso a todas las demás.

Si el objetivo es solamente bloquear unas cuantas aplicaciones perjudiciales sin coartar una relativa libertad del usuario, una lista negra basta. Como mínimo, la aplicación Ajustes de Android y la propia Internet Security se deben proteger con contraseña. Esto impedirá que el usuario final modifique ningún ajuste. Si se pone en la lista negra la tienda de aplicaciones oficial, se puede estar seguro de que no se van a instalar otras aplicaciones. Para controlar completamente el manejo de las aplicaciones del dispositivo, la estrategia de la lista blanca es la opción más fiable. Las aplicaciones en la lista blanca se pueden usar sin limitaciones, pero cualquier otra aplicación se bloquea. La principal utilidad de esto es para dispositivos configurados con la máxima seguridad o para un único flujo de trabajo. Por ejemplo, un dispositivo que solamente van a usar los representantes de ventas puede funcionar en el modo de lista blanca, permitiendo que se usen tan solo el componente de teléfono y la interfaz de la base de datos de ventas.

### 4.1.4. Protección en tiempo real y a petición

La protección contra el malware en tiempo real está disponible a través de los módulos WEB PROTECTION y VIRUS CHECK. Además, se puede restringir la funcionalidad a través de la pestaña POLÍTICAS de G Data Administrator.

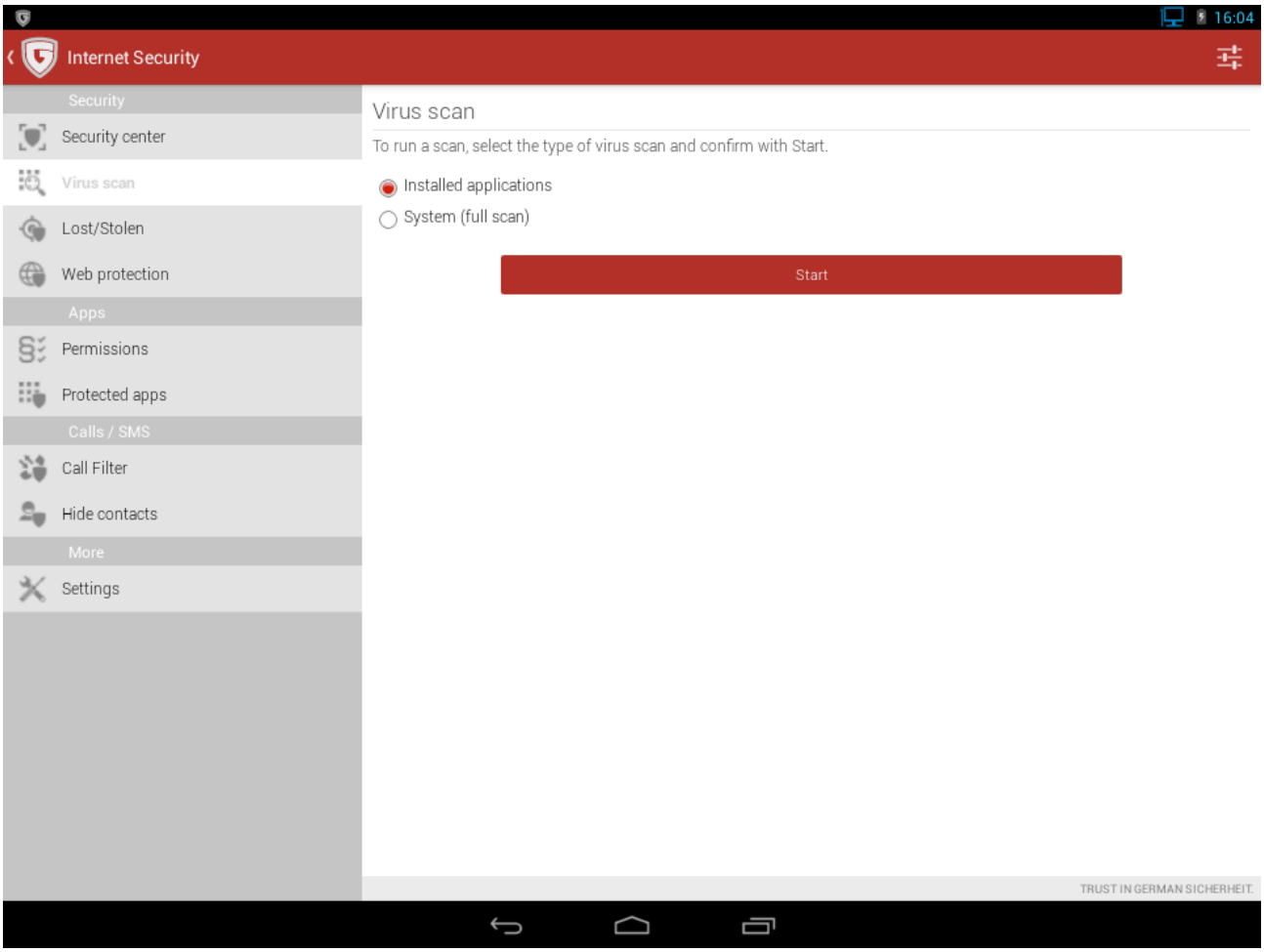



*Imagen 4: G Data Internet Security para Android, Seguridad, Exploración de virus*

La protección web proporciona protección en tiempo real cuando se utiliza el navegador de Android. Como la protección web puede producir una pequeña cantidad de tráfico de datos, se puede configurar para que funcione solamente cuando el dispositivo esté conectado por Wi-Fi. La comprobación de virus comprueba de forma transparente las aplicaciones descargadas en busca de malware y bloquea la instalación si encuentra que es maliciosa.

La protección contra malware a petición está disponible en forma de una comprobación de virus completa para todo el dispositivo. Es aconsejable comprobar periódicamente todas las aplicaciones para estar seguro de que no queda malware en los medios de almacenamiento (como una tarjeta SD). Dependiendo de la frecuencia de uso del dispositivo y con qué frecuencia se instale o se guarde software nuevo en él, el intervalo se puede establecer en 1 día, 3 días, 7 días, 14 días o 30 días. En la mayoría de los casos, se recomienda realizar una comprobación diaria: la exploración no causa una ralentización perceptible y proporciona la máxima seguridad. Para asegurarse de que la comprobación de virus no agota la batería del dispositivo, se puede configurar para que se efectúe solamente cuando el dispositivo se está cargando.

En dispositivos Android, la mayor amenaza viene de dispositivos con derechos de superusuario. Si el usuario final ha obtenido derechos de superusuario para el dispositivo, cualquier seguridad que se implante en el sistema operativo y a nivel de aplicación se puede venir abajo si el malware se las arregla para infectar el dispositivo, ya que gana acceso prácticamente ilimitado a las funciones del sistema operativo. Con el fin de mantener el control sobre los dispositivos móviles gestionados, es aconsejable por tanto usar la pestaña POLÍTICAS para impedir el acceso a la red de los dispositivos con derechos de superusuario. Además, el administrador puede activar o desactivar el acceso a la cámara (para los dispositivos a partir de Android 4.0) y/o ordenar la codificación para proteger los datos almacenados en el dispositivo.

### 4.1.5. Filtrado y gestión de contactos

Para gestionar los contactos en los dispositivos Android, se puede usar la agenda de contactos corporativa. Incluso sin usar ninguna de las opciones de filtrado, bloquear la agenda de contactos integrada del dispositivo y rellenar la agenda de contactos corporativa de Internet Security para Android puede ser una forma efectiva de controlar la información de los contactos. Unido al módulo de filtro de llamadas, dispondremos de una amplia gestión de contactos y de opciones de filtrado.

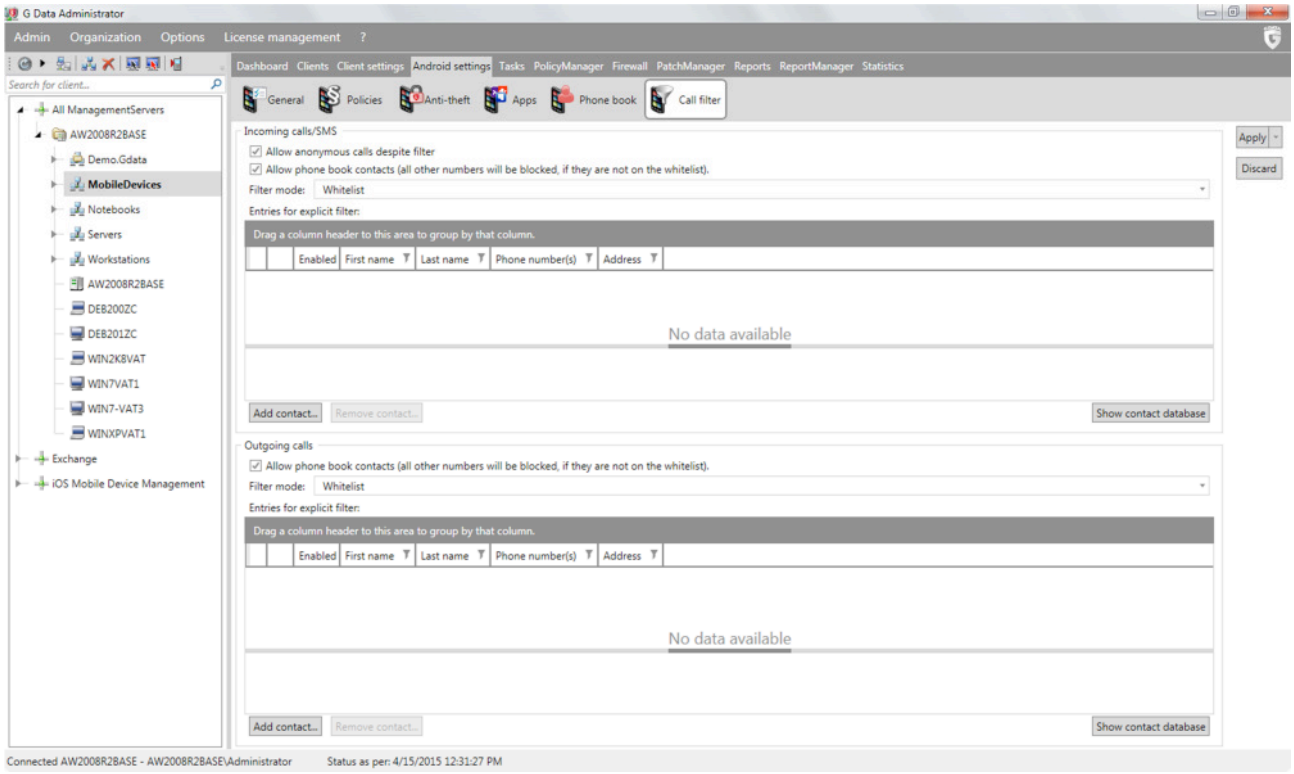



*Imagen 5: G Data Administrator, Ajustes Android, Filtro de llamadas*

La base de toda la funcionalidad es la base de datos de contactos. Funciona como una central para todos los contactos corporativos, a partir de la cual se pueden crear agendas de contactos para distintos dispositivos, así como filtros para llamadas y SMS. Para organizaciones con un número de contactos limitado o para agendas de contactos gestionadas de tamaño reducido, puede ser práctico y más rápido introducir los contactos manualmente en la base de datos de contactos. Si la red utiliza Active Directory, se pueden importar los contactos. Con todos los contactos definidos, estos se pueden distribuir a los

dispositivos oportunos. Por ejemplo, a todos los dispositivos se les puede equipar con una lista completa de las extensiones directas de los compañeros. Alternativamente, en combinación con el bloqueo de la aplicación de la agenda de contactos estándar y el uso del filtro de llamadas, se puede permitir solo a ciertos grupos de dispositivos el acceso a números de teléfono concretos de la agenda.

El filtro de llamadas se puede usar también para un filtrado exhaustivo de las comunicaciones entrantes y salientes. Funciona como un filtro sobre la agenda de contactos integrada del dispositivo. En lugar de bloquear completamente la aplicación de agenda de contactos de Android, el filtro permite un control más preciso de los flujos de comunicación. Por ejemplo, habilitando el modo de lista blanca no se permitirán llamadas entrantes ni salientes excepto para los números incluidos en la lista blanca. En el modo de lista negra, se permite la comunicación en general, pero se pueden bloquear números de teléfono específicos. Un filtro adicional permite la comunicación con los contactos de Android y de la agenda de contactos de Internet Security mientras se bloquean todos los demás (a excepción de los contactos en la lista blanca).

## 4.2. iOS

G Data Mobile Device Management para dispositivos iOS se ha diseñado como una solución sin agente para iOS 7.0 y superior. Utilizando G Data Administrator, los perfiles de la política se pueden implementar en uno o más dispositivos iOS. Esto permite a los administradores gestionar los dispositivos con flexibilidad manteniendo el máximo control sobre su uso.

### 4.2.1. Implementación y administración

La implementación en clientes iOS se puede iniciar desde G Data Administrator. El proceso de implementación se realiza a través de correo electrónico. En la zona de gestión de clientes, seleccione cualquier nodo bajo MOBILE DEVICE MANAGEMENT PARA IOS, haga clic en el botón de la barra de herramientas ENVIAR ENLACE DE INSTALACIÓN A CLIENTES MÓVILES e introduzca una lista de direcciones de correo electrónico. Se pueden introducir algunos parámetros para personalizar la apariencia de la solicitud de MDM en el dispositivo. NOMBRE, DESCRIPCIÓN y ORGANIZACIÓN aparecerán en la solicitud de MDM, así como después en la pestaña GENERAL de AJUSTES IOS. El ACUERDO DE LICENCIA DE USUARIO FINAL se puede usar para informar al usuario final de que el dispositivo se gestionará de forma remota.

Cuando el usuario abre el enlace desde el correo electrónico de instalación en un dispositivo iOS, el dispositivo aparece inmediatamente en G Data Administrator, (con el ESTADO DE SEGURIDAD en la pestaña CLIENTES detallando el estado pendiente). En cuanto el usuario acepte la solicitud de MDM, el dispositivo iOS se puede gestionar completamente a través de G Data Administrator.

Cuando un dispositivo iOS se selecciona en G Data Administrator, queda disponible una serie de módulos de MDM de iOS. En la pestaña CLIENTES (IOS) aparece un resumen de todos los dispositivos iOS gestionados. Para cada cliente se visualizan varias propiedades específicas del dispositivo, como el número IMEI, la versión de iOS y el nombre del producto. La columna ESTADO DE SEGURIDAD muestra advertencias para los dispositivos sin perfil de política, así como alertas de estado de la instalación de MDM. Utilizando el módulo AJUSTES IOS, los administradores pueden configurar las medidas antirrobo (véase el capítulo 4.2.2) además de los perfiles de política (véase el capítulo 4.2.3). El módulo INFORMES (IOS) se puede usar para hacer un seguimiento del estado de varios mensajes Push, el método principal

de comunicación entre G Data ActionCenter y los dispositivos iOS. Los informes incluyen el estado de implementación del perfil y las confirmaciones de la función antirrobo.

### 4.2.2. Antirrobo

Cuando se roba o se pierde un dispositivo, la primera acción que hay que emprender es asegurarse de que nadie acceda a los datos del dispositivo. Después, se puede localizar usando GPS (para encontrar y recuperar el dispositivo) o, como medida más drástica, borrar el dispositivo (en caso que no haya forma de encontrar y recuperar el dispositivo). Apple ofrece a los usuarios registrados en iCloud la función Buscar mi iPhone. Permite a los usuarios iniciar sesión en un sitio web dedicado y bloquear, seguir el rastro o borrar un dispositivo.

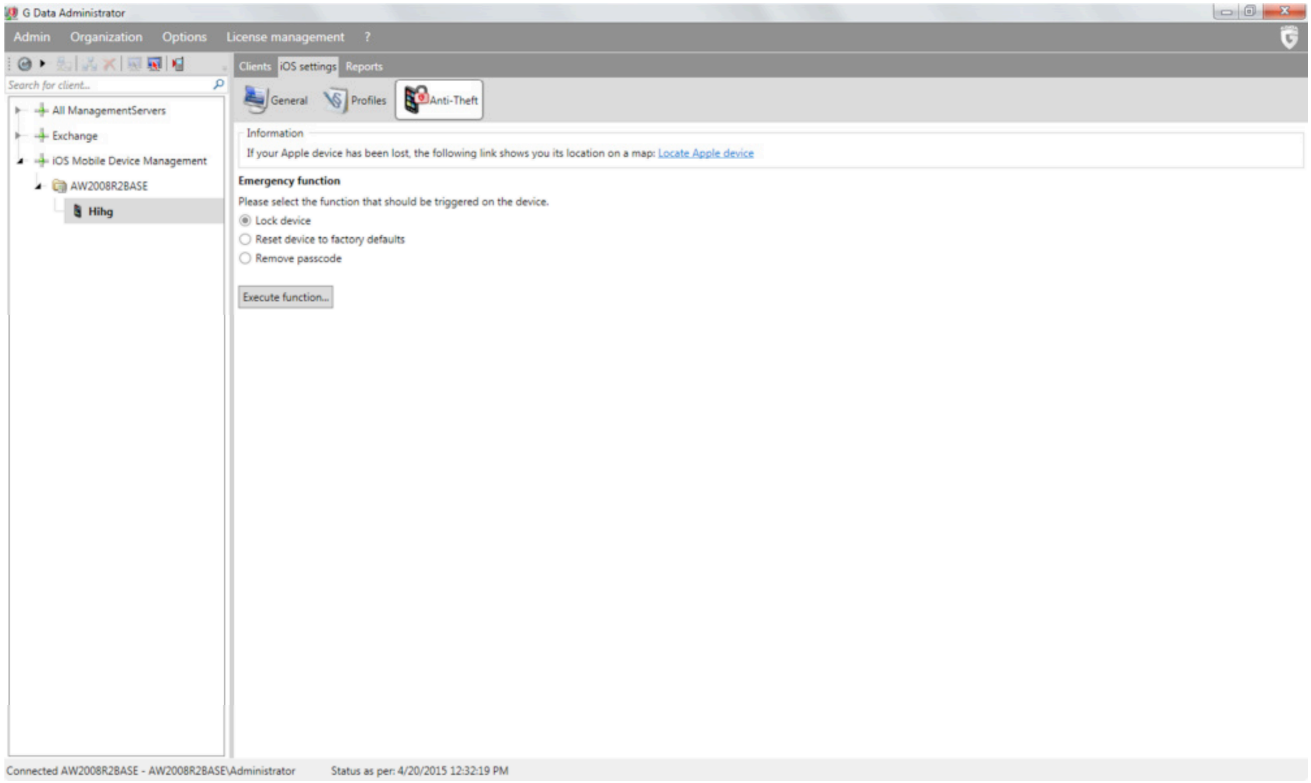



*Imagen 6: G Data Administrator, Ajustes iOS, Antirrobo*

Como alternativa a las funciones de Buscar mi iPhone, el módulo AJUSTES IOS permite a los administradores activar las funciones antirrobo de la pestaña ANTIRROBO sin necesidad de iniciar sesión en un sitio web externo. El bloqueo del dispositivo y las funciones de reinicio se pueden activar seleccionando la opción correspondiente y haciendo clic en EJECUTAR FUNCIÓN. Para los dispositivos que se hayan bloqueado usando un código desconocido, utilice la opción ELIMINAR CÓDIGO.

### 4.2.3. Gestión de aplicaciones, protección y contactos

A diferencia de los dispositivos Android, iOS tiene un concepto de gestión de la seguridad unificado, que permite a los administradores reunir los ajustes de seguridad para cubrir una amplia gama de módulos en un solo perfil. Estos perfiles se pueden aplicar a varios dispositivos, reduciendo el tiempo necesario para asegurar todos los dispositivos iOS de la red. La pestaña PERFILES de G Data Administrator se puede usar para crear y editar perfiles.

Cada perfil puede contener hasta cinco políticas, cada una de las cuales se centra en un tipo específico de ajustes de seguridad:

- RESTRICCIONES DE FUNCIONALIDAD: restringir el uso de iCloud, garantizar un uso seguro de la pantalla de bloqueo, controlar varias funciones más.
- AJUSTES DE CÓDIGO DE ACCESO: obligar a que se cumplan las condiciones para el uso de códigos de acceso, como un número mínimo de caracteres complejos, una longitud mínima y un periodo de gracia después del bloqueo del dispositivo.
- RESTRICCIONES DE APLICACIÓN: bloquear o permitir Safari (incluyendo funciones como cookies, elementos emergentes y JavaScript) y iTunes Store.
- RESTRICCIONES DE CONTENIDO DE MEDIOS: controlar qué tipo de contenidos de medios se permite (aplicaciones, películas, programas de TV).
- WI-FI: introducir información sobre la red Wi-Fi, permitiendo a los dispositivos iOS que se conecten automáticamente a una red Wi-Fi en particular.

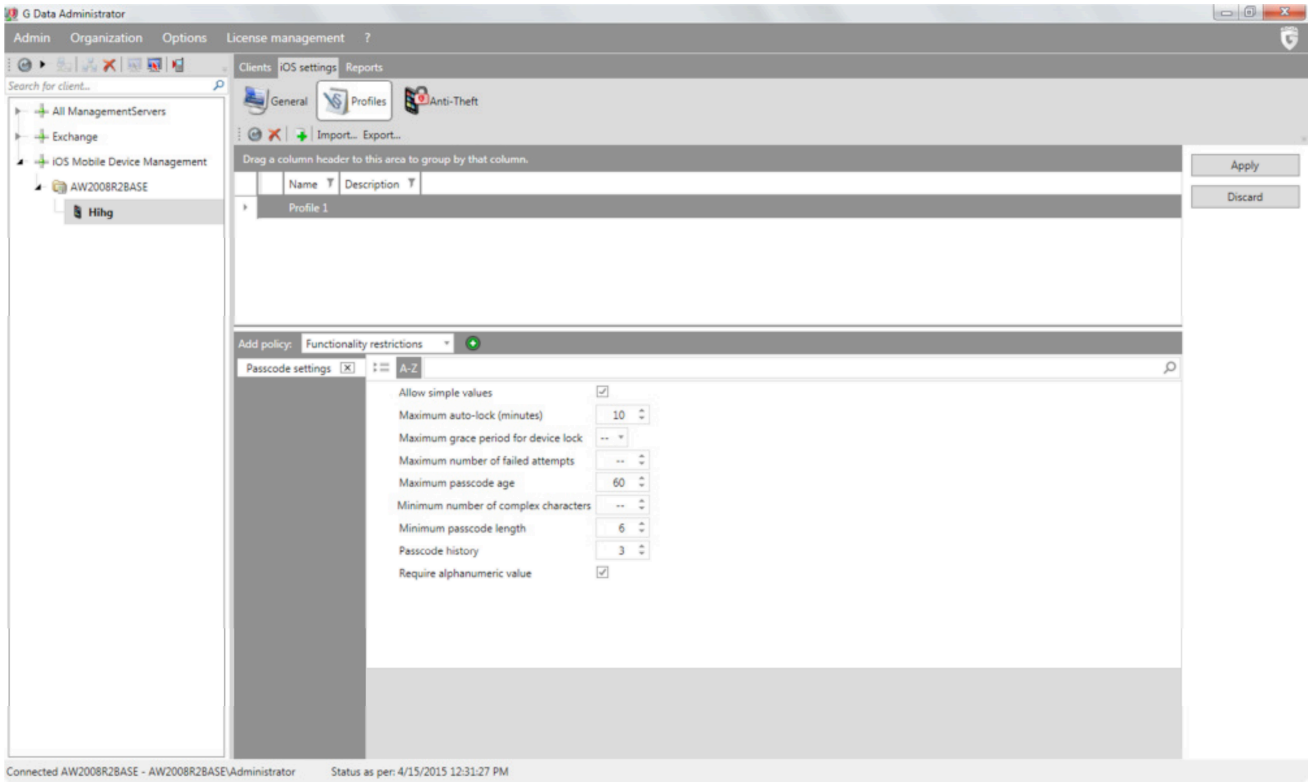



*Imagen 7: G Data Administrator, Ajustes iOS, Perfiles*

Como Apple permite a los usuarios eliminar los perfiles MDM de sus dispositivos en cualquier momento, los administradores tienen que asegurarse de que los perfiles de seguridad contienen una razón de peso para no hacerlo. Se recomienda añadir la política Wi-Fi en todos los perfiles. Esto permite que el dispositivo se conecte a la red Wi-Fi especificada (protegida). Cuando un usuario final trata de esquivar partes de la política de seguridad eliminando el perfil MDM de un dispositivo iOS, se elimina automáticamente el acceso Wi-Fi, limitando en gran medida el acceso del dispositivo a los recursos corporativos. Esto garantiza que los dispositivos inseguros no tengan acceso a recursos de red compartidos reservados ni a otros datos confidenciales.