Comunicación TECNIMAP 2010

Implicaciones económicas y mercado único
Dispositivos móviles.
Plataforma Corporativa de Gestión de Dispositivos Móviles

José Antonio Perea Yustres
Jefe de la unidad de Innovación Tecnológica (I+D+i)
Instituto Nacional de Estadística

1 La movilidad como impulso para modernizar la Función Pública y mejorar la calidad del servicio a la ciudadanía

"Aquí hay que correr mucho para poder seguir en el mismo sitio". La Reina de corazones en Alicia en el País de las Maravillas

Lewis Carroll (1832-1898)

La movilidad es ya una realidad en nuestra sociedad, y los ciudadanos la utilizan como herramienta de comunicación personal pero también como herramienta profesional, gracias a que las empresas han empezado a apostar por la innovación que representa poder disponer de toda la información de la empresa en cualquier lugar y momento para mejorar la productividad de sus empleados.

La administración pública no puede quedar al margen de estas innovaciones en las formas de interacción de los ciudadanos, y por ello debe plantearse el salto a la movilidad ofreciendo dos categorías principales de servicios:

- Los servicios orientados al ciudadano que mejoren su interacción con la administración.
- Los servicios orientados a los empleados para aumentar su productividad.

La movilidad contribuye a mejorar la competitividad de las organizaciones en un entorno más global y dinámico, en el que la empresa u organismo público de hoy en día ha de ser cada vez más una empresa que gestiona la información en tiempo real.

Dos de los principales motores de la Sociedad de la Información han sido, sin duda, Internet y las comunicaciones móviles. Dejando a un lado la evidente influencia de Internet en la Sociedad de la Información, el cambio que ha producido en el sector de las telecomunicaciones la introducción de la movilidad ha sido crítico, no sólo por la extensión de la posibilidad de la comunicación en cualquier momento y en cualquier lugar, sino por la propia personalización en la naturaleza de la comunicación entre individuos.

Algunos analistas consideran a la movilidad como la tercera revolución tecnológica, siguiendo al nacimiento de la informática y la popularización de Internet. No es para menos, ya que ha conseguido asentar sus bases tanto en el segmento residencial como en el corporativo; y en un tiempo récord.

Por otro lado, la evolución tecnológica y de servicios está conduciendo a una progresiva integración de plataformas, servicios y operadores, de tal manera que muchos productos audiovisuales transitan sobre las redes de banda ancha como servicios avanzados de la SI.

2 Evolución de las aplicaciones y servicios en movilidad

Ubicuo: *Dicho de una persona: Que todo lo quiere presenciar y vive en continuo movimiento. Se dice de quien vive en continuo movimiento para no perderse nada:.* **Diccionario de la lengua española**

La información siempre debe estar disponible independientemente de donde esté el usuario aprovechando las oportunidades que ofrece la movilidad en la transmisión de voz y en la transferencia de datos con funcionalidades como el intercambio de ficheros, el acceso remoto a aplicaciones específicas, la ejecución de aplicaciones en movilidad, la conexión remota a las intranets corporativas o la conexión a Internet.

Hay que dotar al sistema de información de las organizaciones de ubicuidad, posibilitando el acceso de forma remota desde cualquier sitio y a cualquier hora (anywhere, anytime). La información debe estar allí donde se necesite con el fin de mejorar la productividad, el funcionamiento de los servicios y agilizar la toma de decisiones,

Hoy en día, la movilidad se busca para aumentar la productividad de las organizaciones. En la actualidad, un 30% de las empresas españolas está abordando ya estrategias en movilidad, y alrededor de un 62% es consciente de la necesidad de las mismas, según recientes estudios del sector. Actualmente, existe una clara tendencia hacia la flexibilidad, y las soluciones móviles constituyen las principales herramientas para ofrecer una respuesta ágil y flexible a las organizaciones.

El cambio tecnológico también se manifiesta en la creciente oferta de contenidos, servicios y aplicaciones para usuarios móviles. Al mismo tiempo, la convergencia con el mundo Internet facilita la accesibilidad a sus servicios, lo que demuestra que el negocio de los móviles evoluciona hacia un paradigma donde los servicios de datos tendrán una gran importancia y generarán un porcentaje importante de los ingresos.

La carrera por ofrecer contenidos personalizados, adaptados a las necesidades de las comunidades de usuarios, no ha hecho más que comenzar. Dentro de poco, quien utilice su móvil sólo para hablar será tan 'raro' como quien hoy día ya no dispone de uno de estos dispositivos.

Las generaciones de infraestructuras de comunicaciones móviles se han presentado en el pasado de forma secuencial, empezando con las soluciones analógicas de la primera generación de principios de los ochenta. En los años 90, las primeras soluciones digitales sustituyeron a las soluciones analógicas, llamadas más tarde soluciones 2G, y a continuación aparecieron las soluciones 3G. En la carrera por el liderazgo en las tecnologías de cuarta generación (4G), la vanguardia la enarbolan participantes asiáticos y estadounidenses.

Los servicios TIC se orientar a satisfacer las nuevas necesidades a las personas que integran las organizaciones. El trabajo rompe con las barreras físicas y se convierte en una mezcla de elementos físicos, sociales, lógicos y electrónicos.

Las comunicaciones se transforman con una orientación hacia la persona con acceso a la información y a contenidos de forma personalizada. El usuario transporta su entorno de comunicaciones completo e integrado allá donde va, independientemente de su ubicación geográfica y de la naturaleza del servicio que requiere, compatibilizando su ámbito personal y privado

Aumenta, por tanto, la necesidad de crear infraestructuras más orientadas, ágiles y eficientes que doten a los empleados de un soporte a las diferentes formas de trabajar "en el momento y lugar necesario, con quien sea adecuado"

3 ¿Qué son los sistemas de Gestión de Dispositivos Móviles?

La movilidad se ha mostrado en el actual entorno económico como una herramienta particularmente interesante para mejorar la productividad y generar ahorros de costes. Sin embargo, también es cierto, que una correcta gestión de los dispositivos y su entorno no es nada sencilla, básicamente por la enorme diversidad de dispositivos, sistemas operativos y software que debe ser administrado.

Los dispositivos móviles son elementos cruciales que aumentan la productividad y el intercambio rápido de información en las empresas contemporáneas. Esto conlleva que los gastos de consumo, de adquisición, gestión y mantenimiento sean uno de los componentes principales de gastos operativos de las organizaciones.

La gestión diaria de dispositivos móviles y la información relacionada es un cometido desafiante en las empresas modernas que disponen de una cantidad importante de recursos móviles.

La movilidad trae consigo nuevos retos en las organizaciones:

- Incidencias y averías continuas
- Problemas de seguridad

- Hay que solucionar los problemas en remoto
- Ancho de banda limitado
- Se necesita viabilidad de los activos y su uso
- Dificultad para conocer el TCO.
- No podemos prever el gasto
- Servicios complejo
- Gran diversidad de: marcas y fabricantes, fechas de compra, vigencia de garantías, usos y tecnologías
- Múltiples tareas repetitivas de operación en la gestión de equipos
- Reubicaciones, nuevas compras, contratación mantenimiento o reparaciones, gestión de averías...
- Todas las tareas relativas a movilidad consumen una enorme cantidad de recursos y pueden retrasar o entorpecer la adopción de soluciones móviles

Ante estos nuevos retos nos planteamos las siguientes cuestiones:

- ¿Cuánto me cuesta la movilidad?
- ¿Puedo prever averías y reducir el coste de su gestión?
- ¿Tengo el control adecuado de inventario y de stocks?
- ¿Soy capaz de medir la calidad de servicio ofrecida a mis usuarios?
- ¿Estoy realmente securizando mis sistemas en movilidad?
- ¿Tienen mis usuarios un único canal de entrada de incidencias y peticiones?
- ¿Dispongo de las herramientas adecuadas que optimicen la gestión?, ¿y el coste?
- ¿Me interesa invertir en estas herramientas?
- ¿Estamos aplicando las mejores prácticas del mercado?

En definitiva necesito gestionar y securizar mis sistemas en movilidad, pero, ¿qué significa Gestionar y Securizar?:

- Gestionar
  - Distribuir programas remotamente
  - Distribuir información y contenidos remotamente
  - Listar los activos físicos y lógicos (software) remotamente
  - Parchear el sistema operativo y el software remotamente
  - Determinar el estado de las licencias de los programas remotamente
  - Ajustar las configuraciones a la política de la empresa
  - Hacer copias de respaldo y restaurarlas remotamente
- Securizar
  - Cifrar todas las comunicaciones
  - Obligar a los usuarios a políticas de contraseñas
  - Obligar a encriptar toda la información almacenada en el dispositivo
  - Matar el dispositivo remotamente si es robado o perdido
  - Instalar parches de seguridad de Win32 remotamente

- Asegurarse de que los dispositivos perdidos o robados no son utilizables Debe proporcionar una completa serie de funciones de administración y seguridad a fin de garantizar que los datos y dispositivos móviles estén actualizados y sean fiables y seguros.

La idiosincrasia de los proyectos de movilidad, que engloba potentes terminales con configuraciones cambiantes y ejecutando software de gestión crítico para el negocio, usados a su vez por perfiles con poca experiencia en tecnología PC (al fin y al cabo son personal desplazado cuya labor se realiza a pie de campo), convierte a las plataformas de gestión de dispositivos en piezas clave para el éxito de los proyectos.

Una solución corporativa de gestión de dispositivos debe proporcionar al menos:

- La gestión remota de las configuraciones o cómo cambiar configuraciones en terminales que pueden estar a centenares de kilómetros de distancia.
- La instalación de software en terminales a distancia. gestionar el intercambio de datos y ejecutar comandos en clientes y servidores
- El inventario de hardware y software instalado en terminales y el control en instalación de herramientas no permitidas.
- La recuperación ante desastres de los terminales (backup, reinstalación, etc.) móviles de forma remota, y a poder ser, desatendida.
- Establecer control remoto para diagnosis de problemas, escaneo de ficheros con antivirus …
- Optimizar las transmisiones mediante checkpoint / restart y mediante compresión
- Ejecución de políticas en Background
- Reducción automática de tiempos de conexión
- Backup específicos (del todo o parte del sistema)
- Integración con LDAP
- Seguridad móvil (cifrados, autenticación, claves, etc.).
- Soportar un amplio abanico de sistemas móviles.

4 Ejemplos de sistemas de Gestión de Dispositivos móviles

Como ejemplos de sistemas en este ámbito destacaríamos las siguientes:

- MSP (Mobility Services Platform) de la empresa Symbol. Esta aplicación de uso web, incorpora tanto la monitorización, la distribución / actualización de software para PDAs, como la gestión de la infraestructura Wireless.
- AirBeam Smart: Otro ejemplo de aplicación de distribución / actualización de software de la empresa Symbol.
- Afaria de la empresa iAnywhere (Sybase). A modo de Gestor de Sistemas, esta aplicación permite el cambio de versiones, el control en los fallos de las aplicaciones instaladas, monitorización de uso y el control de seguridad de datos residentes en los dispositivos. Permite, así mismo, la monitorización de las comunicaciones.
- SOTI Pocket Controller Enterprise de la empresa SOTI Inc: Esta aplicación permite que las organizaciones gestionen remotamente los dispositivos móviles desde una localización central.
- Mobile Director: Esta herramienta desarrollada por Datalogic permite configurar los terminales por cable o por radio frecuencia de manera remota.
- Wavelink AVALANCHE de la empresa Wavelink: Con esta aplicación es posible la gestión de manera centralizada de los terminales móviles, permitiendo, así mismo, la aplicación de políticas de seguridad.

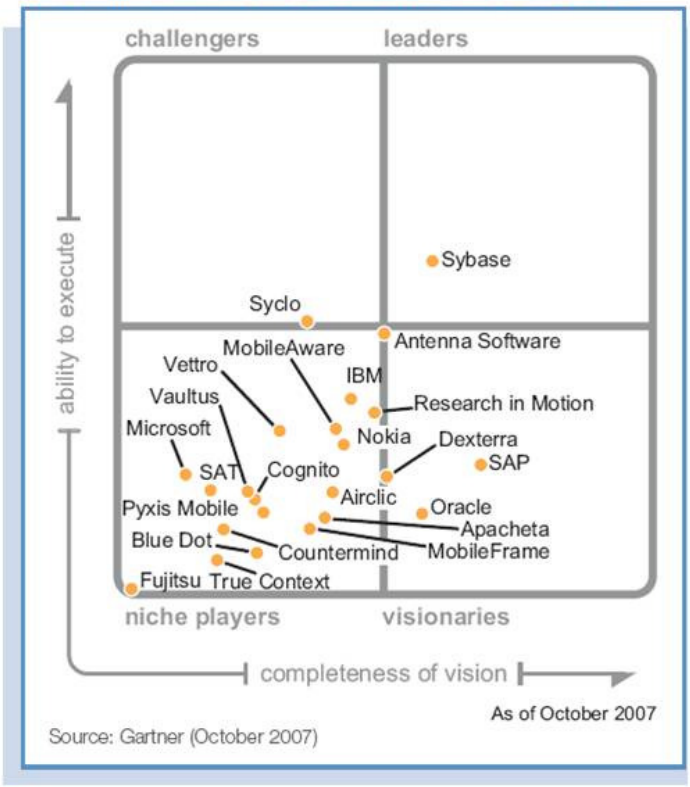
- MDM (Mobile Device Management) de Tamagos Engineering Creativity S.L., es un sistema de gestión integral de dispositivos móviles, líneas y todos los gastos relacionados. Permite llevar el control de gastos y gestionar eficientemente todos los recursos relacionados con los dispositivos móviles.

Este cuadro de IDC y Gartner proporcionan una comparación cualitativa de los proveedores de gestión de dispositivos móviles. Representa una posición en el mercado basado en dos aspectos:

- Capacidad de ganar mercado
- Posicionamiento frente a futuras oportunidades de mercado

Source: IDC, October 2007

Figure 1. Magic Quadrant for Multichannel Access Gateways, 2007



5 Guía para la realización de un pliego de contratación de una plataforma corporativa de gestión de dispositivos móviles.

El objeto del contrato es poder gestionar y securizar el parque de dispositivos móviles con alguna herramienta que posibilite su control remoto.

La solución debe constar de las licencias, elementos software, y adaptaciones necesarias para la gestión de los dispositivos móviles, de acuerdo con el inventario de cada organización, con capacidad de acceso total a los mismos para su gestión remota.

El producto o productos suministrados en la solución, deberán cubrir la totalidad de las necesidades planteados en las funcionalidades indicadas en el pliego, de forma nativa. No se recomienda admitir módulos de desarrollo a medida para cubrir dichas funcionalidades.

El adjudicatario deberá realizar las tareas de soporte técnico y desarrollo que sean necesarias para la correcta implantación de la solución de movilidad, cumpliendo los requisitos técnicos y funcionales detallados en el pliego, hasta la obtención de la aprobación final por parte del organismo.

El adjudicatario deberá realizar junto con el organismo la definición de las políticas de gestión que deberán ser aplicadas. Esta definición incluirá un diseño de las políticas, la definición de los grupos de usuarios, los tipos de dispositivos que se utilizarán, los procedimientos para renovar los dispositivos, los procedimientos de actuación ante incidencias como robos, pérdidas, fallos de hardware etc.

El adjudicatario deberá instalar la solución en modo ASP o en la ubicación donde solicite el organismo.

Debe especificar detalladamente la arquitectura que propone, describiendo la operativa, cómo funciona la escalabilidad y la redundancia, el equipo que se utilizará, cómo se integrarán y los puertos y protocolos utilizados en las comunicaciones.

La solución presentada por el adjudicatario estará basada en productos software estándar de mercado con implantación acreditada. Se requiere como mínimo disponer de dos referencias de implantación en territorio Nacional de cada una de las herramientas que conforman la solución ofertada y que tengan como mínimo 100 usuarios en entornos similares al expuesto en el pliego durante un periodo mínimo de un año (a la fecha de publicación del concurso). No se podrá presentar como referencia la implantación de la solución en la propia empresa.

El sistema propuesto debe permitir su administración y gestión distribuida mediante la utilización de perfiles que independicen su utilización por parte de las diferentes unidades que existan garantizando, en todo momento, la identidad y confidencialidad de la información de los dispositivos móviles.

El sistema propuesto debe tener alta capacidad transaccional y fácil escalabilidad, disponibilidad, nivel de seguridad, rendimiento y gran capacidad de interconexión con sistemas heterogéneos de comunicaciones.

El sistema propuesto debe incluir todas las licencias necesarias y las actualizaciones que se vayan produciendo a lo largo del periodo de validez del concurso.

El sistema de gestión de dispositivos y el cliente que se instale en el dispositivo así como los manuales de formación, de operación y de administración, debe estar en castellano.

Formación sobre el uso de la plataforma al personal del organismo encargado de la gestión de la misma.

El coste de todo el sistema (equipos físicos, lógicos, comunicaciones, licencias, soporte, formación, actualizaciones, etc.) debe estar incluido en el presupuesto de licitación del concurso. En el catálogo de precios adjunto a la oferta debe aparecer un apartado dónde se indique de forma detallada el coste de esta plataforma, cuotas de alta, cuotas mensuales, licencias, etc.

El adjudicatario deberá indicar las optimizaciones que la solución aporta para las comunicaciones inalámbricas y celulares y cómo éstas impactan en el rendimiento o la calidad del servicio prestado por la solución propuesta.

El adjudicatario deberá incluir una herramienta de gestión remota de dispositivos móviles heterogéneos con las siguientes funcionalidades (deberá indicar para cada función de las requeridas a continuación los sistemas operativos móviles sobre los que está disponible dicha función):

- **Inventario**

La solución debe ser capaz de inventariar los dispositivos corporativos (teléfonos, PDAs, equipos con dispositivos de comunicaciones…), recogiendo informaciones sobre el hardware y los programas instalados en el dispositivo de una forma automática y transparente para el usuario.

El inventario debe ser capaz de detectar cambios en las propiedades del dispositivo y debe ser capaz de notificarlo a los administradores.

Debe recoger el número de teléfono, IMEI, IMSI, operador móvil, red actual, WiFi información como (WiFi activo o inactivo, dirección MAC, red actual), estado del Bluetooth, nombre y dirección Bluetooth, estado IR, aplicaciones instaladas, versión de las aplicaciones y directorio en el que están situadas.

La solución propuesta debe permitir utilizar herramientas estándar de informes para crear informes a medida sobre la información recogida de los dispositivos. Éstos deben ser accesibles desde la consola de administración.

Debe ser posible para la solución leer informaciones específicas de los dispositivos para incluirlas en los informes como Claves de registro…

Acceso al estado del dispositivo: batería, memoria disponible,…

- **Configuración de dispositivos**

La solución debe ser capaz de configurar los dispositivos. Se debe indicar qué parámetros del dispositivo son configurables.

Debe indicarse qué tipos de dispositivos puede gestionar.

La solución propuesta debe permitir gestionar desde conexiones móviles 3G, dispositivos con sistema operativo Windows 32 (Tablet PCs, Netbooks, Portátiles…). Es decir, debe implementar la gestión sobre redes inalámbricas como WiFi, o 3G y debe implementar las optimizaciones de comunicación que se requieren para el mundo móvil.

Igualmente la solución debe ser capaz de aplicar parches al sistema Windows 32 utilizando las optimizaciones de comunicación para redes inalámbricas como 3G. Los parches que se apliquen deben haber sido aprobados por el administrador.

Deben indicar qué aplicaciones estándar (correo electrónico, agenda…) son configurables.

Creación y mantenimiento de las conexiones de red. La solución debe permitir que el administrador realice un mantenimiento (creación y / o modificación) de las conexiones de red que se han definido en el dispositivo.

Control de configuración de aplicaciones. La solución debe permitir la configuración de aquellas características de las aplicaciones que están funcionando en el dispositivo móvil y que puedan ser modificadas desde fuera de la propia aplicación.

- **Despliegue de aplicaciones**

El sistema de gestión debe ser capaz de distribuir software ya sea distribuyendo los archivos uno a uno o instalando paquetes cab, etc.

La distribución de software debe poder hacerse según criterios que se comprueban con cada terminal como versión de su sistema operativo, memoria disponible, otras aplicaciones instaladas, etc.

La instalación debe poder hacerse en diferentes puntos como memoria del dispositivo o tarjeta en función de criterios similares a los anteriores.

Debe ser capaz de detectar si a una aplicación le falta algún archivo y debe ser capaz de reponerlo automáticamente.

Debe ser capaz de ofrecer un informe del estado de un despliegue. Por ejemplo indicar el número de dispositivos en los que se ha instalado con éxito y el número de los que faltan.

Debe ser capaz de diferenciar a nivel de byte en los ficheros. El replicado de información debe ser diferencial, descargando únicamente las diferencias de los ficheros a distribuir.

Reinstalación de software si resulta eliminado, así como la desinstalación de software no autorizado.

Posibilidad de distribución de ficheros y documentos, previa selección de los usuarios a los que están destinados dichos contenidos.

El sistema debe poseer un lenguaje de creación de Scripts en el dispositivo móvil para la ejecución de cualquier tipo de proceso sobre el propio dispositivo.

Configuración del tamaño del paquete de la información a remitir, para la adecuación con respecto al ancho de banda disponible en la comunicación.

- **Control Remoto**

El inicio de la sesión debe poder hacerse desde el servidor o desde el cliente por parte del usuario. En este último caso la conexión será distribuida por el sistema a una de las consolas abiertas por el personal de atención a usuarios.

El control remoto debe estar disponible para el sistema/s deseados y debe soportar conexiones inalámbricas.

El licitador indicará claramente las capacidades del sistema de control remoto. Debe al menos permitir transferir archivos, acceder al registro, y parar o arrancar procesos.

La comunicación debe poder cifrarse.

Debe ser posible hacer la conexión entre el administrador y el dispositivo usando un servidor puente que recibe las conexiones de ambos, para evitar problemas con traducciones de direcciones.

Debe ser posible grabar las sesiones en video

Debe disponer de Chat, conexión de Audio, y video conferencia.

- **Gestión de Seguridad**

Cumplimiento obligatorio de políticas de seguridad corporativas definidas por los administradores de manera centralizada, y despliegue de las mismas de manera automática en la conexión del dispositivo.

Posibilidad de definir políticas de seguridad sobre la información residente en el dispositivo, en modo totalmente local sin necesidad de conexión:

- Posibilidad de bloqueo del dispositivo.
- Posibilidad *de Hard Reset* del dispositivo. Borrado de la información residente en el dispositivo y vuelta a la configuración original de fábrica y / o la configuración determinada por los administradores.

Protección por contraseña:

- Contraseñas de múltiples niveles y formatos. La solución debe permitir definir los formatos de contraseña que los usuarios utilizan para el acceso al dispositivo.
- Control de la frecuencia de cambio de contraseñas. La solución debe permitir la configuración del tiempo máximo de vida de las contraseñas utilizadas por los usuarios.
- La solución debe permitir poder bloquear el dispositivo, después de la introducción incorrecta de contraseña, pérdida del dispositivo o robo.
- Asimismo debe permitir acceder a los administradores con una contraseña de acceso que sólo conozcan éstos, para facilitar la administración del dispositivo en casos de bloqueo.
- La solución debe ofertar como mínimo una protección del dispositivo mediante contraseña. Debe ofrecer un método para que el usuario pueda solicitar por teléfono una contraseña nueva en caso de que olvide la que tiene asignada.
- La protección por contraseña debe deshabilitar las comunicaciones Bluetooth, WiFi, o USB del dispositivo, aunque no necesariamente la posibilidad de realizar llamadas.

Cifrado de datos:

- Cifrado de ficheros y directorios en dispositivo móvil. La solución debe permitir cifrar los datos residentes en el dispositivo móvil para accesos no deseados.
- La solución debe permitir cifrar el tráfico entre el cliente y el servidor utilizando protocolos estándar.

- La solución debe ser capaz de cifrar todos los archivos del dispositivo o sólo los de ciertas carpetas. El algoritmo de cifrado debe ser estándar y la solución debe ofrecer al menos dos algoritmos diferentes (Blowfish, AES, 3DES, RC2…).
- Indicar si el sistema de cifrado ha pasado normas de certificación.

Cifrado de medios

- Indique si la solución puede cifrar también el contenido de las memorias y medios conectados al dispositivo como tarjetas SD en el caso de teléfonos móviles o memorias USB o unidades Firewire en caso de portátiles con Windows 32.
- Indique otras facilidades para controlar la información de memorias y medios extraibles.

Identificación de los usuarios

- Debe ser posible identificar los nombres y contraseñas de los usuarios de los dispositivos frente a un servidor de identidades LDAP.

Logs para auditorías de seguridad

- Indique si la solución realiza logs para auditorías de seguridad como por ejemplo logs de los archivos copiados a memorias USB.

Borrado del dispositivo desde el servidor

- Debe ser posible ordenar desde el servidor el borrado completo de las aplicaciones y datos del dispositivo. Este borrado debe poder iniciarse:
  - Cuando el dispositivo se conecta con el servidor para una sesión de gestión.
  - Desde el servidor mediante comunicación IP (en el caso de que el dispositivo esté accesible).
  - Borrado total mediante SMS.

Borrado del dispositivo desde el propio dispositivo

- La solución deberá poder borrar todos los datos cifrados y aplicaciones en caso de que:
  - Se introduzca mal la contraseña más de un número configurable de veces.
  - Si el dispositivo no se conecta con el servidor en un tiempo determinado.

Antivirus/Antispam móvil:

El adjudicatario deberá llevar a cabo las restricciones pertinentes y proveer las herramientas necesarias para proteger de código malicioso y también evitar la recepción de Spam, suscripción a servicios (incluso a través de la web) y publicidad a los terminales y dispositivos móviles.

Debe ofrecer para móviles protección frente a código malicioso como virus, troyanos etc en los dispositivos móviles ya venga este código vía archivos adjuntos al correo, Bluetooth, infrarrojos, USB, transferencias de archivos, enlaces en SMS o MMA. Entre ellos:

- Malware - FlexiSpy/MobiSpy
- Agujeros en el Bluetooth - Cabir/Bluesnarfing
- Troyanos - Brador/BBProxy…
- Uso de de la sincronización de PC - Crossover/Mobler…
- Malware que cuelgue el dispositivo- Skulls, Fontal…
- Gusanos Mobile IP - P2P SMS y MMS dialer
- Troyanos como -CommWarrior/RedBrowser…

Debe permitir barridos de comprobación ordenados desde el servidor.

La herramienta ha de poder:

- Realizar limpiezas periódicas del sistema del terminal móvil, así como de los ficheros, correos, descargas, documentos, etc., contenidos en el terminal, tanto memoria interna del propio terminal, como los ubicados en la tarjeta de expansión (si la hubiera).
- Tendrá que usar pocos recursos de memoria en el terminal, para que el terminal siga funcionando correctamente, sin detectar una ralentización del mismo.
- Deberá detectar envíos malintencionados desde o hacia los contactos contenidos en el terminal, y eliminar dicho SPAM, o de crear listas negras o blancas.
- También deberá proteger de accesos malintencionados mediante Bluetooth o WiFi.
- El listado de virus a detectar será actualizable en la medida que el usuario de terminal lo precise (WiFi, 3G, GPRS,…).
- Sería aconsejable que la gestión de la instalación, mantenimiento y monitorización de la herramienta sea administrable desde el gestor de dispositivos móviles que se oferte.

Cortafuegos:

Debe permitir filtrar conexiones IP salientes y entrantes del dispositivo móvil para, por ejemplo, permitir sólo la conexión a ciertos servicios.

Debe filtrar las llamadas y SMS salientes según el rango numérico al que van dirigidas.

Debe realizar un registro (log) de las acciones realizadas.

- **Copias de Respaldo**

La solución propuesta debe ser capaz de hacer copias de seguridad de archivos y carpetas. Esta información debe poder guardarse en un servidor de archivos localizado en instalaciones del organiusmo. El administrador debe poder ser capaz de restaurar archivos concretos o todos los archivos copiados así como crear actividades automáticas de restauración pero no debe ser capaz de poder leer el contenido de los archivos de los que el sistema ha hecho copia de seguridad.

El licitante debe detallar en la oferta:

- Funcionalidad de planificación de backup: dónde, cuándo y cómo realizar los backups de los dispositivos móviles.
- Funcionalidad de selección por parte del usuario de la información residente en su dispositivo móvil a salvar y / o restaurar.

- **Control de licencias**

La solución debe permitir llevar un control de la caducidad de las licencias de software instalado en los dispositivos. Debe ser capaz de mostrar informes de próximas caducidades y estado de las licencias, así como el número de licencias desplegadas de cada tipo. Debe permitir generar alertas ante próximas expiraciones de licencias y llevar un control de las licencias desplegadas frente a las adquiridas.

- **Métodos de inicio de la conexión**

La solución propuesta debe permitir al cliente de gestión conectarse con el servidor:

- Utilizando la conexión TCP / IP por defecto.
- Abriendo un punto de acceso específico por ejemplo llamando al punto de acceso nombre_empresa.es, o una conexión Dial up de módem específica.
- Utilizando una conexión que haya abierto el usuario. Debe ser posible indicar al cliente de gestión que se conecte en el momento en el que el usuario o el dispositivo abra una conexión para cualquier propósito, como navegar o descargar correo.

- La solución propuesta debe permitir al cliente de gestión reintentar la conexión en caso de fallo un número de veces programable y en un tiempo de reintento también configurable.

- **Otros requisitos**
  - Monitores para Windows Mobile. Para dispositivos Windows Mobile debe ser posible lanzar actividades de gestión de forma asíncrona ante eventos en el dispositivo gestionado. Estos eventos deben ser cambios en claves de registro, creación o borrado de archivos, puesta en marcha o parada de procesos, o que la memoria o batería alcancen ciertos niveles. Debe ser posible lanzar alguna aplicación en local ante estos eventos.
  - La solución propuesta debe guardar un registro de todas las acciones realizadas con cada dispositivo, tanto si tienen éxito como si no. En caso de que no tengan éxito el registro (log) debe indicar claramente las acciones individuales que no se han podido realizar y el tipo de error que ha sucedido. En el log debe ser fácil localizar un dispositivo, las sesiones que ha ejecutado el servidor sobre él y qué acciones se han realizado en cada sesión y cuál ha sido su resultado. Los logs deben ser accesibles a través de una interfaz de BBDD relacional.
  - Escalabilidad. La solución debe poder escalarse fácilmente hasta al menos 10.000 dispositivos. Deben explicar cómo se logra la escalabilidad.
  - Redundancia. La solución debe ofrecer redundancia de forma que un fallo puntual no pare el sistema de gestión. Explique cómo se logra esta redundancia.
  - Multiempresa. Debe ser posible crear en un mismo servidor espacios separados de gestión. De manera que el administrador o administradores de cada espacio sólo pueda actuar y obtener información de los dispositivos gestionados dentro de su espacio. Un administrador global debe tener acceso a todos los espacios de gestión.
  - Múltiples administradores, identificación y granularidad en los permisos. Debe ser posible definir múltiples administradores y también definir para cada uno de ellos qué permisos tiene. En particular qué acciones puede realizar, y cuáles no. Debe ser posible integrar la definición de los administradores con un sistema LDAP de gestión de identidades. La comunicación con el servidor LDAP debe poder ir sobre SSL caso necesario.
  - Administración. Asignación, aplicación de políticas
    - A dispositivos y grupos
    - Por fechas
    - Aplicación una sola vez o cada vez que se conecte
  - Capacidad para crear scripts. Debe ser posible crear scripts que permitan automatizar tareas de gestión. Por ejemplo parar una aplicación, comprobar la existencia de archivos, enviar o recibir archivos y poner aplicaciones en marcha. Debe disponer de lógica condicional (IF, Then, o While, Else). Debe permitir leer y escribir en el registro. Detectar la velocidad de conexión para decidir qué acciones hacer con esa conexión y cuáles no. Generar alertas y mensajes. Capacidad para integrarse con otras aplicaciones.
  - Facilidades para el despliegue. Instalación vía aire. El cliente de gestión debe poder ser instalable vía aire, es decir debe poder enviarse al dispositivo sin necesidad de realizar una instalación mediante un cable. Algunas opciones son: Un SMS con una URL para descarga u OMA. El texto del mensaje SMS debe ser configurable. Debe haber una interfaz SMPP o módem para el envío de los SMS.
  - Cliente instalado en la EPROM o BIOS de los terminales. Se valorará esta posibilidad.
  - Soporte de protocolos estándar de gestión:

- OMA CP. Debe soportar la creación de un punto de acceso en un dispositivo mediante OMA CP.
- OMA DM. La solución de gestión debe permitir utilizar OMA DM en los dispositivos que cumplan esta norma.

- Grupos Dinámicos. La solución debe permitir crear grupos de dispositivos en función de características de los dispositivos.
- Integración con otras aplicaciones. API Cliente y Servidor.
- Alarmas configurables. La solución propuesta debe ser capaz de generar alarmas ante eventos específicos en los terminales y en el servidor. Las alarmas deben ser configurables. La solución propuesta debe permitir ver las alarmas en la consola de gestión y debe ser posible exportar las alarmas como "traps" SNMP a otros sistemas y notificarlas a los administradores vía correo electrónico usando SMTP.
- Integración con sistemas de Informes. La información recabada de los dispositivos por la solución deben estar disponibles en una base de datos relacional para poder ser utilizadas con sistemas de informes estándar.
- BBDD Abierta. Para la integración con otras aplicaciones se solicita que la información de gestión pueda guardarse en una base de datos relacional. El esquema de esta base debe estar documentado.

- **Puesta en marcha e integración**

El adjudicatario será responsable de la puesta en funcionamiento del hardware y software en colaboración con el personal del organismo. Comprenderá:

- Instalación del Sistema.
- Configuración del Sistema y del software de base (sistemas de ficheros, bases de datos, etc.).
- Instalación y configuración de producto/s, herramienta/s, etc., necesarias para proveer de toda la funcionalidad requerida en este pliego de prescripciones técnicas.
- Automatización e integración con los sistemas existentes según las condiciones de este pliego de prescripciones técnicas.
- Pruebas, ajustes de rendimiento y reconfiguración del Sistema.
- Despliegue de la solución de gestión de dispositivos móviles para los elementos determinados por el organismo.
- Creación de la base de datos de inventario de dispositivos sobre los que se haya desplegado la solución de gestión.

- **Formación y documentación**

El adjudicatario deberá dejar constancia escrita de todos los procesos seguidos para la instalación, configuración y adaptación requeridos por la solución, de manera que puedan ser reproducidos en el futuro. Este requerimiento se hace extensivo a la configuración del hardware y software de base que resulte necesario para el funcionamiento de la instalación. También deberá dejar constancia escrita de los trabajos realizados y soluciones aportadas en el marco de apoyo técnico.

Sin perjuicio de lo anterior, y en el caso de requerir desarrollo de código fuente para la adaptación de posteriores funcionalidades, el adjudicatario deberá hacer entrega de toda la documentación de diseño técnico y funcional, así como elaborar un manual de referencia en castellano para cada biblioteca de código desarrollada, describiendo todas las funciones, procedimientos o métodos que la componen.