EXPDTE: SFC/2019/00011

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES QUE HA DE REGIR LA CONTRATACIÓN DE LOS SERVICIOS DE EQUIPAMIENTO Y LICENCIAS DE USUARIO O PUESTO DE TRABAJO DE LA EMPRESA MUNICIPAL DE SERVICIOS FUNERARIOS Y CEMENTERIOS DE MADRID, S.A.

Madrid, 4 de marzo de 2019

ÍNDICE

1ª. OBJETO DEL CONTRATO

El objeto de este contrato es contratación de los servicios de implantación de los servicios de "Puesto de trabajo" que incluye la correspondiente migración desde la situación actual e integración de los mismos dentro de la nueva red privada virtual de la Empresa Municipal de Servicios Funerarios y Cementerios de Madrid S.A. (en adelante SFMADRID)

Se entiende como "Puesto de trabajo" el servicio que permita dotar a los usuarios de la SFMADRID de todo el equipamiento y licencias de ámbito ofimático, así como los sistemas on-line de los mismos (Office 365) así como cualquier otro equipamiento o software necesario para la conexión y gestión de los mismos, todo ello dentro de este servicio global y con un coste fijo.

Detalle de la contratación:

Proyecto de Implantación "Puesto de Trabajo"
SITUACIÓN ACTUAL
Análisis de SITUACIÓN ACTUAL. Equipamiento, licencias, herramientas de usuario, antivirus, etc.
IMPLANTACIÓN Y TRANSICIÓN (PMO)
DISEÑO / IMPLANTACIÓN
TRANSICIÓN y GESTIÓN DEL CAMBIO
Desactivación y destrucción **equipamiento actual**
PMO: Gestión global del proyecto, plazos, entregas, calidades, etc.
Servicios Recurrentes
1. Servicio de Plataformado o replataformado de equipos Y MENSUALIDAD de equipamiento/licencias en uso.
2. Servicio de Incidencias 24x7
3. Servicios de Peticiones de Servicio, Operación/Explotación
4. Servicios de Gestión de Cambio
5. Servicios de Monitorización y disponibilidad: Equipamiento, Antivirus, Exchange, OneDrive, SharePoint, Skype for business/Microsoft Teams, etc.
6. Servicios de Administración: Equipamiento, Antivirus, Exchange, Onedrive, Sharepoint, Skype for business/Microsoft Teams, etc.
7. Servicios de Back-up: Equipamiento, Exchange, Onedrive, Sharepoint, Skype for business/Microsoft Teams, etc.
8. Servicios de Recuperación y Continuidad de negocio
9. Servicios de Seguridad
10. Servicios de Seguimiento del Servicio y Mejora Continua
Documentación de estos servicios, así como el plan de transición y devolución del servicio.
1. Documentación de estos servicios, así como el plan de transición y devolución del servicio.

2ª. CARACTERÍSTICAS DEL MATERIAL Y SERVICIO

Introducción, datos de contexto:

Distribución de las **sedes** (a efectos de posibles cálculos de desplazamientos en trabajos de campo u on-site):

Nombre sede	Dirección
Tanatorio M30	Calle Salvador de Madariaga 11, 28027 Madrid
Cementerio la Almudena	Avenida de Daroca 90, 28017 Madrid
Crematorio Almudena	Avenida de Daroca 90, 28017 Madrid
Oficina de barrio 1	Pza. de Cristo Rey 4 1-D, 28040 Madrid
Oficina de barrio 2	Calle Doctor Castelo 52, 28009 Madrid
Oficina de barrio 3	Calle San Modesto 42, 28034 Madrid
Cementerio Sur	Calle Ildefonso González Valencia 6, 28054 Madrid
Tanatorio Sur	Calle Ildefonso González Valencia 6, 28054 Madrid
Crematorio Sur	Calle Ildefonso González Valencia 6, 28054 Madrid

Las sedes secundarias que pudieran existir están al lado de estas consideradas como principales y se puede llegar a ellas sin necesidad de vehículo.

A lo largo de este pliego se menciona en varias ocasiones la necesidad de conexión a Red Privada Virtual (RPV) de la SFMADRID, DA y ADFS (Directorio Activo y Servicios de federación), el licitante de esta implantación debe considerar que estos servicios e infraestructuras ya estarán implantados, y que sólo debe hacer el esfuerzo de entender la forma establecida y segura para conectar con ellos aportando desde su parte de la implantación lo que sea necesario en términos de equipamiento, licencias y/o cualquier otro concepto para su conexión y/o haciendo peticiones al proveedor de servicios de dicha plataforma y servicios de RPV, DA y ADFS para el resto, todo ello dentro de los costes fijos de esta licitación.

Las incidencias y/o peticiones que se generen en el transcurso de la implantación, pero también durante la prestación de estos servicios serán aperturadas dentro de la plataforma de incidencias y solicitudes de la SFMADRID SA y serán tramitadas allí pudiendo tener el licitante acceso a la misma mediante recepción de notificaciones de correo electrónico y acceso directo a la plataforma por WEB, salvo acuerdo justificado no se aceptarán otras plataformas externas a la mencionada para esta gestión.

Finalmente, también como comentario global se indica que la SFMADRID contrata esta implantación en modalidad de derechos de uso, plataforma y servicios gestionados siendo el licitante el que adquiera todo lo necesario para cubrir los requisitos mínimos aquí descritos, mantenerlos en garantía y correcto estado de uso.

Proyecto de Implantación "Puesto de Trabajo"

1.- Análisis de SITUACIÓN ACTUAL.

Revisión de la situación actual de cara a plantear su migración y aplicable al siguiente equipamiento/licencias/plataforma:

- Equipos PC y portátiles

- Tablets
- Office 365 + Software en propiedad
- Servidor de archivos y archivos en local
- Seguridad y Accesos a Red SFMADRID y configuración ADFS (datos de usuario y SSO)

Es importante resaltar que de cara a transición/re-plataformado sólo se tendrán en cuenta equipos y software en garantía de fabricante, el resto de equipamiento se tendrá en cuenta de cara a "hard-reset" con opción de reacondicionado o destrucción, de este último equipamiento el que tenga una segunda vida útil se pondrá a disposición de la SFMADRID una vez realizado el formateo de fábrica.

Alcance, detalle de elementos actuales a tener en cuenta en este análisis:

Equipamiento Actual	
PC Base	134
Portátil Base	10
PC +	0
Tablets	99
Portatil +	2
	245

(*) + 1 Docking y 1 Pantalla de un segundo equipamiento

Licenciamiento **Actual**	
Empresa Essentials (On.line)	86
Empresa Premium (Instalable)	39
Sólo correo (On.Line)	95
Exchange Online Plan 1	31
Project Essentials	0
Project Professional	2
Antivirus (**por dispositivo**)	
	253

- Servidor de archivos y archivos en local: 800 GBs
- Requisitos mínimos de seguridad y plataformado (normas de la SFMADRID a cumplir durante el proceso de instalación de equipos/software/usuarios, etc.).

Entregables mínimos:

- Lista de maquetas necesarias a realizar por tipo de equipamiento (pc, portátil, Tablet, etc.).
- Inventario de equipos/usuarios/licencias actualizado (contando con la colaboración del equipo SFMADRID para ello) y estrategia de migración.
- Estructura y estrategia de implantación servicios On-line y Antivirus para equipos y tablets.

- Estudio del impacto y soluciones para el uso del software en propiedad de la SFMADRID en el equipamiento y software base a implantar, en especial las conexiones a la Aplicación CORE mediante SSH y Genero.
- Estudio de cómo conectar con Red SFMADRID y ADFS.

2.- DISEÑO E IMPLANTACIÓN

Se entiende por diseño e implantación el plataformado de equipos según tipo de equipamiento y usuario (creación de las maquetas).

Se adjunta la definición inicial/mínima de plataformado a nivel de **PC y portátil**: (Anexo I)

Checklist Plataformado PC.xls:

Por su especial configuración y necesidad se adjunta la definición inicial/mínima de plataformado a nivel de **Tablets**: (Anexos II y III)

Tablets 30 Tablets Nota Tecnica Config

Tablets 30 Protocolo de Puesta

Para aquellos dispositivos que tengan movilidad (tablets y/o portátiles, por ejemplo) el plataformado asegurará que su salida a internet se haga accediendo a la RPV de la SFMADRID y por lo tanto con la seguridad y filtrados corporativos para al menos el acceso a los servicios corporativos, así como cualquier almacenamiento interno de todos ellos deberá configurarse como cifrado.

Igualmente, incluido en este punto, tenemos:

- la conexión con ADFS para usuarios y SSO,
- configuración Exchange O365, incluye al menos lo siguiente:
  - cambio de login a nuevo dominio sfmadrid.es,
  - cuentas individuales con firma corporativa (en algunas de ellas se necesita configuración de alias),
    Migración desde cuentas POP3 para consulta del histórico de comunicaciones.
  - cuentas de administración o aplicación,
  - cuentas compartidas o de uso por varias personas (con creación de firma de todos los usuarios que la usan),
  - cuentas de solo entrada o solo salida incluyendo la limitación de que no se pueda recibir o enviar según sea el caso,
  - grupos de correo (hasta 40 grupos),
  - salas de reuniones (hasta 40 salas),
  - recursos compartidos (hasta 40 recursos), etc.,
- configuración Skype for business/Microsoft Teams (incluye grupos, salas virtuales para SFMADRID y externos, teléfonos de conexión con configuración/integración centralita IP, etc.).
- OneDrive (para uso individual y landing zone digitalización).
- SharePoint (para uso departamental, landing zone para digitalización, IN/OUT departamental, etc.)

- Plataforma/Sistema/Software antivirus por usuario (no por dispositivo) y sistema central de monitorización.
- Plataforma/Sistema/Software de inventario, monitorización y control del equipamiento, así como control remoto de los dispositivos y despliegue de parcheados y upgrades.
- Conexión segura desde el CPD/oficinas del proveedor a la red de la SFMADRID para actuaciones en remoto y creación de los usuarios de administración de toda la solución y/o de auditoría para la SFMADRID.

IMPORTANTE: esta arquitectura de solución global tanto de elementos centrales como de dispositivos finales y todos sus componentes debe servir como uno de los principales elementos de cara a el diseño de los servicios recurrentes y entre ellos especialmente los servicios de monitorización, back-up y recuperación.

Alcance:

- N.° de maquetas diferentes: hasta 10 diferentes (siguiendo normas de seguridad y plataformado de SFMADRID compatibles con la situación actual, así como conexiones a aplicaciones a medida SFMADRID, impresoras, etc.)
- Usuarios: 350 aprox.
- Departamentos: 22
- Espacio de servidor de ficheros: 420 GBs
- Conexión segura a la RPV de la SFMADRID a través de solicitud al proveedor externo a cargo de este servicio, conexiones a ADFS para gestión de identidades y SSO.

Entregables mínimos:

- Creación de las maquetas por tipo de equipamiento:
  - Se debe prestar especial atención al uso del software en propiedad o específico de la SFMADRID como por ejemplo las conexiones a la Aplicación CORE mediante SSH y Genero.
  - Igualmente será necesario garantizar que estas maquetas son compatibles con el resto de los dispositivos de usuario como impresoras (tanto aquellas de impresión mediante aplicaciones de terceros o conectadas a sistema Windows como aquellas que sirven para imprimir desde la aplicación CORE de la SFMADRID basada en Informix, i-4GL y GENERO), faxes o sistemas de digitalización o cualquier otro.
  - Se incluye en este apartado las configuraciones por imagen corporativa de la SFMADRID como fuente predeterminada y fondo de pantalla o cualquier otro similar y aplicadas a todas las aplicaciones del equipamiento. (Anexos IV y V)


FONDODEPANTALLA.jpg


Futura Std.zip

  - Para la creación de las maquetas el licitante contará con la colaboración del personal de la SFMADRID y/o de los proveedores responsables de los servicios externos necesarios en las primeras instalaciones (área piloto) siendo 100% autónomo en el resto del despliegue.
- Conexión segura a la RPV de la SFMADRID. Así mismo, conexión a ADFS para usuarios y SSO. Creación de los usuarios de administración de toda la solución y/o de auditoría para la SFMADRID (solo se admitirán conexiones desde la RPV de la SFMADRID y/o desde dispositivos móviles o personales autorizados).
- Creación de la estructura de Exchange, Skype, OneDrive, SharePoint.

- configuración Exchange O365, incluye al menos lo siguiente:
    - cambio de login a nuevo dominio sfmadrid.es,
    - cuentas individuales con firma corporativa (en algunas de ellas se necesita configuración de alias),
      Migración desde cuentas POP3 para consulta del histórico de comunicaciones.

    - cuentas de administración o aplicación,
    - cuentas compartidas o de uso por varias personas (con creación de firma de todos los usuarios que la usan),
    - cuentas de solo entrada o solo salida incluyendo la limitación de que no se pueda recibir o enviar según sea el caso,
    - grupos de correo (hasta 40 grupos),
    - salas de reuniones (hasta 40 salas),
    - recursos compartidos (hasta 40 recursos), etc.,
- Configuración Skype for business/Microsoft Teams: incluye grupos, salas virtuales para SFMADRID y externos, teléfonos de conexión con configuración/integración centralita IP, conexión desde teléfonos móviles y tablets, etc.
- OneDrive: para uso individual incluyendo tablets y teléfonos y landing zone digitalización.
  Se creará en el PC del usuario un directorio local sincronizado y se moverán todos los archivos locales a él permitiéndole acceder a los archivos en local y en la nube (en la configuración por defecto de los usuarios no se permitirá que graben archivos en directorios locales salvo en este para asegurar el back-up en O365).
  Igualmente se habilitará la conexión y uso especializado para tablets de asistentes comerciales.
- SharePoint: para uso departamental incluyendo tablets y teléfonos, landing zone para digitalización, IN/OUT departamental, etc.
  Se parte de la idea de una implantación de SharePoint básica con la creación de una estructura por departamentos (20 departamentos aproximadamente en SFMADRID) y la migración de los ficheros en servidor de archivos a esta estructura, adicionalmente en cada estructura de departamento se creará un directorio IN y otro OUT público para permitir intercambios, igualmente la creación de un directorio de entrada para el envío de digitalización de documentos desde los servicios de impresión.
  Para el mantenimiento de esta estructura y la creación de directorios y subdirectorios dentro de cada sección departamental se formará a un administrador de esa área.
  Igualmente se habilitará la conexión y uso especializado para tablets de asistentes comerciales.

- Configuración de la consola central de monitorización antivirus (por dispositivo).
- Plataforma de inventario y mantenimiento de equipamiento y licencias.
- Manual de usuario para la configuración de los servicios O365 en sus teléfonos móviles y/o tablets de la SFMADRID (para la parte de teléfonos sólo manual, quedará fuera de este alcance la realización de configuración alguna a este respecto en teléfonos móviles al pertenecer estos a otro servicio).

Para la creación de usuarios finales, de software base y/o administración se seguirán las normas establecidas a nivel de seguridad de la información en la SFMADRID, las Políticas a configurar serán:

Los usuarios finales estarán vinculados al directorio activo (ADFS) y con SSO.

Nomenclatura de usuarios de servicios, sistema operativo y admin que no usen en modo operativo el sistema

Para estos usuarios estamos siguiendo la siguiente nomenclatura;

admin_emsfweb_ftp

siendo Admin la función, en este caso administrador
emsfweb la solución/entorno/aplicación
ftp el servicio dentro de esa solución/entorno/aplicación

Caducidad o renovación de contraseña de usuarios de administración y sistema operativo de 12 meses a realizar de forma controlada/planificada.
La contraseña generada inicialmente en la creación o reseteo forzado de la misma debe ser cambiada por el usuario por una que sólo conozca él en su primer acceso.
Complejidad de la contraseña:

CARACTERES -> 8
MAYS. -> 1 carácter al menos obligatorio
MINS. -> 1 carácter al menos obligatorio
NÚMS. -> 1 carácter al menos obligatorio
CARACTERES ESPECIALES {[(¡!”·$€%&/=¿?Ñ* -> SI

3 INTENTOS hasta bloqueo
DURACIÓN DEL BLOQUEO -> INDEFINIDO

3.- TRANSICIÓN Y GESTIÓN DEL CAMBIO.

Se incluye en este apartado:

- Re-plataformado de PCs, Portátiles y Tablets todavía en garantía/vida útil (de aquellos equipos indicados en "SITUACIÓN ACTUAL").
- Plataformado de equipos nuevos (diferencia entre necesidad y aquellos que se re-plataforman de "SITUACIÓN ACTUAL").
- Licencias Office 365 (migración y activación de nuevas).
- Antivirus de usuario por dispositivo.
- Cuentas de correo (incluye migración de las cuentas actuales accedidas por LiveMail y/o cualquier otro sistema POP3 con todo su histórico).
- Migración de ficheros en local a OneDrive.
- Migración de ficheros en servidor de archivos y/o sistema de carpetas compartidas en Exchange interno a SharePoint.
- Instalación de Software en propiedad, antivirus, etc.
- Inventario inicial y activación del MDM / SCCM (o equivalente).
- Configuración de la Seguridad a los servicios On-line desde todos los dispositivos.
- Formación a usuarios y gestión del cambio (sistema operativo, Office 365, antivirus).
- Conexión segura a la RPV de la SFMADRID a través de solicitud al proveedor externo a cargo de este servicio. Así mismo, conexión a ADFS para usuarios y SSO.
- Configuración de la consola central de monitorización antivirus (por dispositivo).
- Plataforma de inventario y mantenimiento de equipamiento y licencias.

Alcance:

Datos para reacondicionado/migración (del equipamiento actual SFMADRID):

Equipamiento Actual a RE-PLATAFORMAR	
PC Base	37
Portátil Base	9
PC +	0
Tablets	66
Portatil +	2
	114

Licenciamiento **Actual**	
Empresa Essentials (On.line)	86
Empresa Premium (Instalable)	39
Sólo correo (On.Line)	95
Exchange Online Plan 1	31
Project Essentials	0
Project Professional	2
Antivirus (**por dispositivo**)	
	253

En esta estadísticas las licencias que estén en uso será necesario cambiarlas de titularidad en el distribuidor sin necesidad de hacer nada a nivel del usuario (salvo el cambio de login por el nuevo dominio sfmadrid.es) que las continuará usando de forma transparente en su nuevo equipamiento o equipamiento replataformado.

Equipamiento/Licencias NUEVO (a aportar por el adjudicatario):

Equipamiento Nuevo	
PC Base	85
Portátil Base	0
PC +	15
Tablets	42
Portatil +	18
	160

Licenciamiento Nuevo	
Empresa Essentials (On.line)	2
Empresa Premium (Instalable)	15
Sólo correo (On.Line)	13
Exchange Online Plan 1	4
Project Essentials	2
Project Professional	0
Antivirus (**por dispositivo**)	274
	310

Resto de información de contexto:
- Departamentos: 22
- Espacio de ficheros OneDrive: 1 TB por usuario
- Espacio de ficheros SharePoint: 1 TB en total

Equipamiento TOTAL	
PC Base	122
Portátil Base	9
PC +	15
Tablets	108
Portatil +	20
	274

- <u>Pantalla</u>
  10 modelos 28" 4K 3840 x 2160 o superior para comité de dirección y responsables de departamento.
  123 modelos 1920 x 1080 FHD 24" pulgadas o superior LED.
  43 monitores de reciente adquisición se mantienen en el mismo usuario.

- <u>Teclado + Ratón</u>
  20 modelos inalámbricos para comité de dirección y responsables de departamento.
  146 de puestos modelo por cable.

Licenciamiento TOTAL	
Empresa Essentials (On.line)	88
Empresa Premium (Instalable)	54
Sólo correo (On.Line)	108
Exchange Online Plan 1	35
Project Essentials	2
Project Professional	2
Antivirus (**por dispositivo**)	274
	289

Entregables mínimos:

- Re-plataformado de equipamiento antiguo o entrega del nuevo, etiquetado, transporte y puesta en marcha en puesto de usuario incluyendo la colaboración con equipo SFMADRID para instalación del software no maquetado o configuraciones finales en puesto de usuario (*). El licitante contará con la colaboración del personal de la SFMADRID y/o de los proveedores responsables de los servicios externos necesarios en las primeras instalaciones (área piloto) siendo 100% autónomo en el resto del despliegue.

  (*) todos los equipos que se conecten a red sean nuevos o antiguos necesitarán latiguillo de conexión a punto de red y tipo CAT6A 1 mts Netconnect Commscope.

- Se entiende por sustitución de equipamiento previo, la retirada del mismo para su re-plataformado o destrucción (ver punto a este efecto) previa migración de la información del equipo al nuevo. Los equipos retirados quedarán al menos 2 semanas a la espera y confirmación del usuario que ha salvado toda la información que necesita hacia el nuevo equipamiento. El licitante contará con la colaboración del personal de la SFMADRID y/o de los proveedores responsables de los servicios externos necesarios en las primeras instalaciones (área piloto) siendo 100% autónomo en el resto del despliegue.

- Solicitud alta a equipo administrador DA, conexión a ADFS, configuración DHCP, DNS, certificación de cumplimiento de políticas de seguridad global de equipamiento y específicas de usuario, etc.

- Conexiones seguras y filtradas sólo a dispositivos de red SFMADRID o a tablets SFMADRID a los servicios on-line.

- Migración de licenciamiento Office 365 en global.

- Migraciones de ficheros a OneDrive y SharePoint.

- Vinculación con Impresoras / escáneres para que OneDrive y SharePoint permitan la recepción de digitalización de documentos.

- Inventario actualizado MDM / SCCM o similar.

- Conexión segura a la RPV de la SFMADRID a través de solicitud al proveedor externo a cargo de este servicio. Así mismo, conexión a ADFS para usuarios y SSO.

- Configuración de la consola central de monitorización antivirus (por dispositivo).

- Plataforma de inventario y mantenimiento de equipamiento y licencias.

- Formación a usuarios (**): a desarrollar por el licitante teniendo en cuenta los siguientes requisitos mínimos (que aplica todos los dispositivos incluido tablets):

- existirá una formación inicial de todo O365 y lo relativo al antivirus en la entrega del equipamiento al usuario,
- existirán formaciones "de aula" semanales a las que los usuarios podrán apuntarse libremente llevado registro de las mismas,
- la documentación de formación se entregará en formato electrónico y se publicará en SharePoint en lugar público para consulta y sesiones de refuerzo.
- Finalmente se desarrollarán pequeños documentos o "píldoras" formativas con las que se recordarán a los usuarios las principales funcionalidades de O365 y del antivirus, de cara a ser usadas por la SFMADRID en el plan de comunicación y como refuerzo de conocimientos.

(**) Requisitos de cara al registro y control de la formación:
Las definiciones de las diferentes iniciativas formativas se determinarán al menos con el siguiente detalle:

- CIF, Teléfono, dirección de la empresa que imparte la formación
- título de la formación,
- colectivo a la que va destinada,
- objetivos principales de la formación,
- detalle concreto de días,
- número de horas de cada día, temario,
- DNI, nombre y contacto (email y teléfono) del formador

los contenidos se trasladarán con 2 semanas de anticipación a la SFMADRID para su revisión y posibles mejoras/ajustes, una vez estos contenidos sean validados
todas las formaciones deberán tener al menos dos sistemas de medición:

- una encuesta final en la que se valore la formación en sí, conocimientos del formador, medios, etc.
- un examen en el que valorar la eficiencia de la formación, siendo este un examen individual por asistente que permita ver el progreso de conocimientos, en el caso de que haya asistentes que no hayan superado los conocimientos mínimos del examen se les deberá incluir en otra convocatoria hasta logarlo o trabajar con ellos en el refuerzo de conocimientos que lo consiga.

Los materiales de formación (documentos, presentaciones, documentos de reciclaje, encuestas, etc.) se entregarán en formato electrónico para su publicación en postales de formación on-line.

- Será requisito mínimo la realización de un PILOTO con cada uno de los equipamientos a desplegar y en cada una de las sedes para confirmar que todo funciona y/o ajustar conectividades, maquetas, etc. no se realizará el despliegue final al resto de usuarios hasta la confirmación del PILOTO.

- Planificación de despliegue teniendo en cuenta los horarios y servicios y tiempos de actividad o momentos críticos de cada área y/o usuario pudiendo contactar con ellos directamente para agendar el mejor momento, el licitante estudiará la situación actual y propondrá un plan de despliegue que implique el menor impacto en la actividad de la SFMADRID, para lograr este plan se tendrán en cuenta trabajos fuera de horario e incluso fines de semana o festivos si es necesario.

Una vez cerrado el plan se entregará un seguimiento periódico (mínimo cada 3 días del mismo) con planes de remediación para cualquier desfase que se vea no se puede compensar.

Para este plan se tendrá en cuenta una estrategia diferente para renovaciones que para re-plataformados, así como tiempos suficientes de soporte post-entrega para resolución de dudas e incidencias al usuario, no se dará por finalizada la entrega de un equipamiento hasta conseguir la validación expresa del usuario receptor del mismo.

El proceso final de migrado de un equipo a otro siempre se realizará en el propio sitio del usuario con una mínima explicación de lo que se entrega y la validación inicial por su parte, así como la confirmación de que todo queda funcionando.

4.- Desactivación y destrucción del equipamiento actual

Restauración de fábrica de aquellos que, pese a estar fuera de garantía estén aún en buen estado y puesta a disposición de los empleados de la SFMADRID, resto hard-reset y destrucción (ISO 14001).

Alcance (como mínimo lo siguiente):

- PC / Portátiles: 140 (de los cuales 70 a restaurar de fábrica)
- Tablets: 38 (todas a restaurar de fábrica)
- 1 servidor de ficheros (se confirmará que no quedan ficheros sin migrar a SharePoint y se re-plataformará el equipo dejándolo a disposición de la SFMADRID).

Entregables mínimos:

- certificado de destrucción siguiendo normativa 27001 y 14001 para aquellos equipos que finalmente se destruyan.

Esta volumetría podrá variar en un +/- 5% durante el proceso de implantación sin incremento de coste.

5.- El resto de información necesaria y a tener en cuenta en este proyecto/servicio.

Tipos de Equipamiento (requisitos mínimos Hardware para equipamiento de gama profesional):

- PC Base
  Procesador: Intel Core i5 8ª generación
  Memoria RAM: 8 GB DDR4
  Almacenamiento: 500 GB SSD
  Windows 10 PRO 64bits

- PC PLUS (con capacidades extra, por ejemplo, diseño gráfico):
  Procesador: Intel Core i5 8ª generación
  Memoria RAM: 16 GB DDR4
  Tarjeta Video Nvidia / Radeon 2GB / 4GB GDDR5 o similar
  Almacenamiento: 500 GB SSD
  Windows 10 PRO 64bits

- Portátil:
  Convertible 2 en 1
  Pantalla táctil de 12,5" o superior (1920x1080 FHD o superior)

Procesador: Intel Core i7 8ª generación
Memoria RAM: 8 GB DDR4
Almacenamiento: 500 GB SSD
Windows 10 PRO 64bits
Dock station
Funda protectora de transporte
Dispositivo de anclaje y/o antirrobo

Opcional lápiz óptico.

- <u>Tablet (*)</u>:
  Pantalla 9" o superior
  1920x1080 FHD o superior
  Lápiz óptico
  CPU Octa-core o superior
  64GB memoria interna y 4GB de RAM
  Android 8.0 (Oreo) o superior
  GPS, Cámara de 13MP
  4G o superior + WIFI ac
  Funda protectora con teclado incorporado

  (*) Alternativa

  Convertible 2 en 1
  Modelo de procesador: Intel Cherrytrail Atom X5-Z8350 4 núcleos o superior
  Memoria RAM:2 GB o superior
  Tipo de Disco duro: eMMC o superior
  Capacidad de Disco Duro: 32GB o superior
  Tamaño de Pantalla mímino: 25,10 cm -10"
  Versión del Sistema Operativo: Windows 10 PRO

  Con altavoces incorporados
  Puertos de micrófono y auricular externo
  Cámara de mínimo 2MP
  Batería 5400mAh , Polímero de litio
  Tipo de pantalla mínima IPS de 1200x1920
  CONEXIONES: PUERTOS HDMI 1, Wifi 802. 11b/g/n, USB 1, BLUETOOTH 4.0, LECTOR TARJETAS DE MEMORIA
  Tarjeta de telefonía SIM para conexión de datos

  En el caso de ser esta la alternativa se sustituirán todos los dispositivos tipo Tablet por este y no se incluirán servicios de MDM ya que este dispositivo se plataformará como un PC o portátil normal.

- <u>Pantalla</u> (para equipo base, base plus y portátil con dock station):
  Display port / dvi / hdmi / vga

  10 modelos 28" 4K 3840 x 2160 o superior para comité de dirección y responsables de departamento.

123 1920 x 1080 FHD 24" pulgadas o superior LED.

43 monitores de reciente adquisición se mantienen en el mismo usuario.

- <u>Teclado + Ratón</u> (para equipo base, base plus y portátil con dock station):
  Conjunto de teclado + ratón:
  20 modelos inalámbricos para comité de dirección y responsables de departamento.
  146 de puestos modelo por cable.

  Teclado mecánico Español QWERTY
  Compatible Windows 10

El equipamiento será de **categoría profesional** y siempre se mantendrá dentro de garantía de fabricante con sustitución en caso de superarla.

Tipos de <u>combinaciones de licenciamiento</u>:

- O365 Empresa Essentials (On.line)
- O365 Empresa Premium (Instalable)
- O365 Quiosco (On.Line)
- O365 Exchange Plan 1 (On.line)
- O365 Project Essentials
- O365 Project Professional
- Antivirus (por dispositivo a sugerir por licitante)

<u>Otros requisitos</u> a tener en cuenta:

Se requiere una solución para <u>usuarios que COMPARTEN el mismo equipo</u> durante el mismo turno: 8 equipos y 70 usuarios.

La solución reside en instalar en el equipo alguna facilidad para que permita rápidamente a la persona que va a trabajar en ese momento en el equipo identificarse (biométrico, tarjeta, etc.), así como que el equipo tenga suficiente capacidad para admitir sesiones simultáneas de varios usuarios sin bloquearse o ralentizarse (PC +).

<u>Sistema de inventario</u> de todo el equipamiento con al menos las siguientes opciones:

- Inventario
- Localización, usuario asignado, etc.
- Escalado de incidencias con identificación del dispositivo
- Histórico de mantenimiento correctivo
- Planes de mantenimiento preventivo, histórico de mantenimiento preventivo
- Situación de equipamiento a nivel de S.O. parcheado, etc.

- Posibilidad de control remoto del equipo
- Despliegue centralizado de parches y actualizaciones
- Indicador de actividad
- MDM/MTP para el caso de Tablets (100% compatible con el equipamiento re-plataformado así como con el nuevo).
- Alarmas de garantías de fabricante, etc.

Gestión global del proyecto (PMO)

1.- Gestión global del proyecto, plazos, entregas, calidades, etc.

El persona o responsable por la parte del licitante que gestione este proyecto será un equipo técnico con conocimiento directo del ámbito de estos servicios y que aporte liderazgo y seguimiento desde una posición técnica y de gestión y no sólo de gestión, se entiende esta posición como una oficina técnica con capacidad de planificación y coordinación de tareas y equipos.

Alcance / Entregables mínimos:

- Trabajo on-site durante toda la implantación (no se prevé una dedicación full-time para este proyecto).
- PMO
- Seguimiento periódico
- QA
- Planes de remediación
- Cierre del proyecto y activación servicios de soporte.

Servicios recurrentes:

1.- Servicio de Plataformado o replataformado de equipos Y MENSUALIDAD de equipamiento/licencias en uso.

Alcance / Entregables mínimos:

Para la parte de elementos centrales de la solución: los servidores, capacidades y licenciamiento serán sugeridos por parte del licitante con los requisitos mínimos que sirvan para soportar el rendimiento actual y con suficiente escalabilidad futura, la SFMADRID sólo contratará un servicio global con un tope de presupuesto mensual.

Sustitución de equipos "críticos" en menos de 4 horas (servicio 24x7).
Se definen como dispositivos críticos, el 10% de los que se encuentren en uso, que se identificarán en el inventario durante la implantación (PC's, tablets, portátiles, etc.) y se revisarán mensualmente.

Entrega de equipos re-plataformados en menos de 2 días hábiles desde petición ante roturas u equipos que queden obsoletos.

Entrega de equipos nuevos en menos de 4 días hábiles desde petición.

Revisiones ilimitadas de las maquetas durante el año en base a cambios del equipamiento.

Se adjuntan cálculos de la situación actual y la necesidad de re-plataformado y reemplazo (estas cifras podrán variar más / menos un 5% sin implicar un extra-coste):

Equipamiento Actual	
PC Base	134
Portátil Base	10
PC +	0
Tablets	99
Portatil +	2
	245

(*) + 1 Docking y 1 Pantalla de un segundo equipamiento

Equipamiento Actual a RE-PLATAFORMAR	
PC Base	37
Portátil Base	9
PC +	0
Tablets	66
Portatil +	2
	114

Equipamiento Nuevo	
PC Base	85
Portátil Base	0
PC +	15
Tablets	42
Portatil +	18
	160

Equipamiento TOTAL	
PC Base	122
Portátil Base	9
PC +	15
Tablets	108
Portatil +	20

274

Licenciamiento **Actual**	
Empresa Essentials (On.line)	86
Empresa Premium (Instalable)	39
Sólo correo (On.Line)	95
Exchange Online Plan 1	31
Project Essentials	0
Project Professional	2
Antivirus (**por dispositivo**)	
	253

Licenciamiento Nuevo	
Empresa Essentials (On.line)	2
Empresa Premium (Instalable)	15
Sólo correo (On.Line)	13
Exchange Online Plan 1	4
Project Essentials	2
Project Professional	0
Antivirus (**por dispositivo**)	274
	310

Licenciamiento TOTAL	
Empresa Essentials (On.line)	88
Empresa Premium (Instalable)	54
Sólo correo (On.Line)	108
Exchange Online Plan 1	35
Project Essentials	2
Project Professional	2
Antivirus (**por dispositivo**)	274
	289

- Pantalla

10 modelos 28" 4K 3840 x 2160 o superior para comité de dirección y responsables de departamento.
123 modelos 1920 x 1080 FHD 24" pulgadas o superior LED.
43 monitores de reciente adquisición se mantienen en el mismo usuario.

- Teclado + Ratón
  20 modelos inalámbricos para comité de dirección y responsables de departamento.
  146 de puestos modelo por cable.

El equipamiento, software, licencias, conexiones y/o cualquier otra parte de esta solución deberá estar siempre en correcto estado de uso y con garantía del fabricante.

Gracias a este servicio se sustituirán los equipos que hayan sufrido robos, roturas, fallos eléctricos o cualquier tipo de desperfecto que impida su uso en perfectas condiciones incluyendo la obsolescencia anteriormente mencionada todo ello SIN coste extra para la SFMADRID, el licitante protegerá física y lógicamente toda la solución para evitar que en la medida de lo posible este tipo de eventualidades.

Disponibilidad mínima del Servicio de Hosting de elementos centrales 99,5% en 24x7

2.- Servicios de Incidencias 24x7

Sistema de ticketing y protocolo de resolución de incidencias con aplicabilidad a todos los bienes y servicios implantados.

El adjudicatario deberá diseñar los sistemas de monitorización necesarios para anticipar caídas de los bienes y servicios implantados y asegurar el cumplimiento de los SLA's.

Se parte de la premisa que los servicios se deben diseñar como servicios de uso intensivo y poca tolerancia a fallos, 24x7x365 con alta disponibilidad y redundancia, así como con una rápida recuperación en el caso de fallos.

En actividades de resolución de incidencias y mantenimiento correctivo, el equipo de la SFMADRID actuará cuando sea necesario como equipo de diagnosis y primer nivel de soporte y posteriormente el equipo del adjudicatario realizará el resto del trabajo hasta resolución incluyendo cualquier necesidad de desplazamiento o trabajo de campo.

En horario fuera de soporte del área de IT de la SFMADRID los directores y responsables de servicio actuarán como personal de contacto, para facilitar su gestión el adjudicatario proveerá a la SFMADRID de un/unos formularios con el protocolo de información que el usuario debe documentar antes de llamar a soporte con aquellas verificaciones y diagnosis necesarias a realizar desde el punto de vista de un usuario y que aceleren la resolución de la incidencia al adjudicatario.

Escalado de incidencias ilimitado (canal correo y telefónico) y garantía de resolución por SLA.

En la resolución se emitirá en un 25% de los casos encuesta al usuario.

Incidentes VIP = < 30 minutos 98%
Incidentes críticos = 4h 98%

Incidentes importantes = 8h 98%
Incidentes básicos = 16h 98%
(tiempos de resolución)

Incidencias reabiertas <= 1%

Reclamaciones de usuario inferiores al 2% de las incidencias abiertas

Puntuación media en encuestas >= 7 puntos sobre 10 durante los 3 primeros meses y 8 a partir del 3er mes en adelante

TODAS las reclamaciones de usuario o las respuestas inferiores a 6 puntos deberán tener un plan de remediación con eliminación de causa raíz (se presentarán informes en seguimiento del servicio).

Disponibilidad de los servicios On-line 99,5% (Office 365, Antivirus)

Informes periódicos de seguimiento de este servicio en reunión mensual con SLA's asociados.

El equipo que gestione estos servicios deberá estar localizado en Madrid Capital y con capacidad de desplazamiento a las oficinas de SFMADRID en caso de emergencia con medios propios y con equipamiento propio.

3.- Servicios de Peticiones de Servicio, Operación/Explotación

Sistema de ticketing y protocolo de resolución de peticiones de servicio, Operación/Explotación con aplicabilidad a todos los bienes y servicios implantados.

En actividades de resolución de peticiones de servicio, Operación/Explotación, el equipo de la SFMADRID actuará cuando sea necesario como equipo de diagnosis y primer nivel de soporte y posteriormente el equipo del adjudicatario realizará el resto del trabajo hasta resolución incluyendo cualquier necesidad de desplazamiento o trabajo de campo.

Se entenderá también por ejemplo como petición de servicio la de mudanza o desplazamiento del equipamiento de una localización a otra o su desconexión temporal y almacenamiento durante obras o similar.

Alcance / Entregables mínimos:
Peticiones a solicitar con acuerdo de fecha de entrega en base a complejidad/impacto y seguimiento de la misma con SLA (cumplimiento de la fecha de entrega acordada en un 98% de las ocasiones, entrega de la estimación de esfuerzo y fecha de resolución objetivo en menos de 2 días desde petición).

Las peticiones recurrentes se diseñarán de forma estándar con requisitos mínimos de información, aprobación, protocolo de actuación y tiempos de respuesta, etc. (por ejemplo, alta/baja/modificación de usuario o petición de recuperación).

Peticiones de Emergencia (las que afecten a la disponibilidad) con resolución < 4 horas

Informes periódicos de seguimiento de este servicio en reunión mensual con SLA's asociados.

El equipo que gestione estos servicios deberá estar localizado en Madrid Capital.

4.- Servicios de Gestión de Cambio

Peticiones a solicitar con acuerdo de fecha de entrega en base a complejidad/impacto y seguimiento de la misma con SLA (cumplimiento de la fecha de entrega acordada en un 98% de las ocasiones).

Gestión de cambios estándar con periodicidad mínimo bisemanal.

Peticiones de Emergencia (las que afecten a la disponibilidad) con resolución < 4 horas

Informes periódicos de seguimiento de este servicio en reunión mensual con SLA's asociados.

El equipo que gestione estos servicios deberá estar localizado en Madrid Capital.

5.- Servicios de Monitorización y disponibilidad: Equipamiento, Antivirus, Exchange, Onedrive, Sharepoint, Skype for business/Microsoft Teams, etc.

Se realizará una configuración de monitorización personalizada a la implantación.

Las modificaciones en Monitorización se gestionarán como Gestión de Cambio y/o Petición de Servicio con sus SLA's ya descritos.

Informes periódicos de seguimiento de este servicio en reunión mensual.

6.- Servicios de Administración: Equipamiento, Antivirus, Exchange, Onedrive, Sharepoint, Skype for business/Microsoft Teams, etc.

Dentro de estas actividades se incluyen todas las relativas a la administración y mantenimiento preventivo, el adjudicatario ofrecerá un servicio de mantenimiento preventivo que complemente al correctivo de puntos anteriores. Entenderemos por mantenimiento preventivo aquellas tareas diseñadas con el objetivo de anticiparse a cualquier incidencia o problema que pudiera surgir.

Para ello se revisarán los equipos y servicios, realizando pruebas y estudios periódicos que verifiquen el correcto funcionamiento de las instalaciones. El adjudicatario elaborará un plan completo de tareas a realizar a nivel preventivo para el mantenimiento del sistema, el cual deberá documentarse de forma adecuada y será entregado periódicamente para su seguimiento y evaluación.

El adjudicatario contemplará la reposición de cualquier parte del equipamiento que presente fallo (siendo esto transparente para la SFMADRID), lo mismo ocurre con la actualización de versiones que corrijan errores del software de aplicación de cualquiera de los sistemas instalados, se deberá asegurar en todo momento que el equipamiento, licencias y servicios permanezcan en correcto uso y con garantía en vigor de sus fabricantes.

Finalmente es importante que el adjudicatario también tenga en cuenta y que valore adecuadamente que cualquier cambio o upgrade deberá realizarse manteniendo en la medida de lo posible la coherencia y compatibilidad de la implantación y que si es necesario conllevará el consecuente reciclaje de formación/gestión del cambio (a técnicos y usuarios) y por supuesto upgrade de la documentación asociada.

Alcance / Entregables mínimos:

Programa personalizado de administración y actualización de la plataforma, parcheado, mantenimiento preventivo, etc.

Programa de verificaciones periódicas y mantenimiento preventivo, ajustes de rendimiento, revisión de crecimiento y espacios, etc. etc.

Las modificaciones en Administración se gestionarán como Gestión de Cambio y/o Petición de Servicio con sus SLA's ya descritos.

Informes periódicos de seguimiento de este servicio en reunión mensual.

El equipo que gestione estos servicios deberá estar localizado en Madrid Capital.

7.- <u>Servicios de Back-up: Equipamiento, Exchange, Onedrive, Sharepoint, Skype for business/Microsoft Teams, etc.</u>

Se realizará una configuración de back-up personalizada a la implantación para aquellos bienes o servicios que lo requieran.

La solución de back-up permitirá la restauración rápida de equipamiento, conexiones con O365, solución antivirus, conexiones con ADFS o cualquier otro elemento externo o software que gobierne la solución, integraciones y demás, al igual que permitirá restauración de equipos de forma rápida (maqueta + personalización del usuario), documentación de usuario o departamental (OneDrive, Sharepoint en servicio ON-line), así como buzones de correos completos (no correos individuales igualmente en servicio ON-line). Se parte de la premisa que no existirán ficheros fuera de los de sistema operativo, posibles archivados de correo, en los equipos de los usuarios estando todo en los servicios On-Line, las carpetas de OneDrive o SharePoint que estén sincronizadas se asegurarán en su versión on-line lo mismo que el correo y en caso de pérdida del equipo se volverán a sincronizar.

Full back-up instantáneo, réplica entre cabinas
Política de copias diarias, semanales y mensuales a detallar por el proveedor.

Solicitudes de Recuperación de archivos/directorios/equipamiento mediante peticiones de servicio.

Informes periódicos de seguimiento de este servicio en reunión mensual.

8.- <u>Servicios de Recuperación y Continuidad de negocio</u>

El adjudicatario proveerá los procedimientos necesarios a ejecutar ante fallos o errores que se pudieran dar en los bienes o servicios contratados. Por la criticidad del negocio de la SFMADRID se establecerán planes de verificación de la continuidad de los servicios contratados y el adjudicatario propondrá simulacros planificados para verificar la continuidad del servicio.

Los servicios de recuperación ante fallos y plan de continuidad se ejecutarán al menos una vez al año y se mantendrán actualizados con frecuencia mensual y/o ante cambios de gran impacto.

Se entiende este servicio de recuperación como una solución que se basa en el servicio de back-up (explicado en punto aparte) de recuperación en el mismo site desde el que se presta el servicio regular, no existe centro alternativo, sino que simplemente se protege el dato con back-up y capacidad de restauración y recuperación con éxito.

Capacidad de recuperación parcial ante fallos o errores de equipos y licencias individuales.

Dentro de estos servicios se enmarca igualmente la definición de un plan de emergencia que contendrá la descripción del plan de actuación que deberá seguirse en el caso de que se produzca un desastre o incidencia en el servicio.

Como peticiones recurrentes inicialmente se tendrán las siguientes (si el licitante no está de acuerdo con esta lista y justifica una más adecuada se analizará su propuesta, también se admiten extensiones de este listado):

Recuperación y Continuidad de Negocio	Frecuencia
Simulacro TOTAL	Anual
Envío de informe de contingencia	On-demand
Envío de informe de replicación	On-demand
Recuperación de un desastre real	On-demand
Pérdida de información en servicios On-line etc.	Baja
Recuperación de un equipamiento de usuario, equipo o tablet	Baja

Alcance / Entregables mínimos:
Capacidad de recuperación de cero de toda la plataforma con verificación anual de su correcto funcionamiento.

Capacidad de recuperación parcial ante fallos o errores, a solicitar mediante petición de servicio.

Capacidad de recuperación parcial ante fallos o errores de equipos y licencias individuales. Se incluye en este apartado la posibilidad de activar cuentas de correo electrónico consideradas críticas (a identificar durante el proceso de implantación, se añade ejemplos de las cuentas actualmente consideradas críticas: EMSF20@, coordinadores@, oficinasdebarrio@, expedientes@, tablet@, control@, recepción M30-Sur, floristería M30-Sur, dir-comer, sanidad@) en un sistema de correo alternativo en el caso de caída del principal, dicho sistema solo se utilizará durante la contingencia sin acceso a correos del sistema primario.

RTO y RPO a detallar por el proveedor.

Informes periódicos de seguimiento de este servicio en reunión mensual.

9.- Servicios de Seguridad

Servicios de monitorización de seguridad global de toda la implantación, con especial atención a las interconexiones con terceros y accesos; y coordinación con los servicios centrales de seguridad de red que tiene contratados la SFMADRID.

Igualmente, los servicios de verificación de seguridad (penetration test, etc.) se ejecutará a la finalización de la implantación y posteriormente una vez al año o cuando se hagan cambios significativos en la implantación.
Conexión segura con Red Privada Virtual de la SFMADRID, plataformado de equipos cumpliendo políticas de la RPV y Directorio Activo, etc.

Servicios de seguridad propios de equipamiento (PC y tablets) y O365 con monitorización constante de vulnerabilidades y pruebas de intrusión anuales.

Aplicación del parcheado y resolución de vulnerabilidades y/o amenazas a través de servicio de administración tanto a equipos como aquello que pudiera afectar a servicios On-line o a los propios servicios On-line.

En caso de ataque o infección por virus a nivel de los PC/portátiles/tablets o de cualquiera de los servicios On-line, actuación de bloqueo de la amenaza en menos de 4h con horario de servicio 8x5 o 24x7 en aquellos ataques que impacten en el nivel de disponibilidad, eliminación total del virus o la amenaza y actualización de los sistemas en menos de 12 horas desde detección.

El adjudicatario justificará en su respuesta a este pliego el plan de trabajo a este respecto teniendo en cuenta que debe cumplir normativa 27001 tanto en la realización de los servicios como en el caso de que en su ejecución existan incidencias.

Informes periódicos de seguimiento de este servicio en reunión mensual.

El equipo que gestione estos servicios deberá estar localizado en Madrid Capital y con capacidad de desplazamiento a las oficinas de SFMADRID en caso de emergencia.

10.- Servicios de Seguimiento del Servicio y Mejora Continua

Sistema de Cálculo y seguimiento de los niveles de servicio (SLAs), diseño y ejecución proactiva de planes de mejora (con aplicación para todos los bienes y servicios).

La empresa adjudicataria deberá proporcionar las herramientas necesarias para la medición de la calidad del servicio y facilitar periódicamente los datos correspondientes basados en medidas objetivas que permitan acreditar la calidad del servicio prestado.

Las paradas de servicio programadas por el contratista de cualquier bien o servicio de este pliego deberán avisarse con una antelación mínima de cinco días laborables para solicitar la conformidad con la SFMADRID, proporcionando entre otros datos, fecha y hora de la parada, duración estimada, objeto de la intervención, tareas a realizar, elementos y servicios afectados por la parada, así como datos de las personas encargadas de su ejecución.

Asimismo, el compromiso de calidad se medirá en relación al tiempo medio de detección y comunicación de averías y el tiempo medio de resolución de las mismas.

El licitante podrá incluir otros SLA's que no se encuentren reflejados y que aporten elementos adicionales a los servicios solicitados de gran valor pero manteniendo los solicitados expresamente.

El equipo responsable por la parte del licitante que gestione este servicio será un equipo técnico con conocimiento directo del ámbito de estos servicios y que aporte liderazgo y seguimiento desde una posición técnica y de gestión y no sólo de gestión, se entiende esta posición como una oficina técnica con capacidad de planificación y coordinación de tareas y equipos.

Alcance / Entregables mínimos:
Seguimiento periódico mensual en detalle con informes de la actividad, así como de los SLA's y niveles de su cumplimiento.

Programa de Innovación, planes estratégicos y mejora continua del servicio global, aseguramiento de la calidad a sugerir por el solicitante, que al menos contenga lo siguiente:

planes de mejora del servicio 2 veces al año con planes reales que mejoren la tecnología o usabilidad o que repercutan en mejora de costes o percepción de usuario y que tengan un plazo de implantación en menos de 1,5 meses.

Cumplimiento de la entrega de los informes de seguimiento y punto de situación del servicio a tiempo en un 98% de las ocasiones (2° día laborable de cada mes)

El equipo que gestione estos servicios deberá estar localizado en Madrid Capital y con capacidad de desplazamiento a las oficinas de SFMADRID en caso de emergencia y para las reuniones periódicas de seguimiento.

Documentación de estos servicios, así como el plan de transición y devolución del servicio.

1.- Documentación de estos servicios, así como el plan de transición y devolución del servicio.

Documentación y gestión de la transición, devolución del servicio.
Informe inicial de servicios, solución y plataforma entregado en la activación de los servicios.

Actualización de la documentación e inventarios cada mes (el inventario se utilizará para el cálculo de la mensualidad del equipamiento y licencias).

Entrega de la documentación actualizada 2 meses de antelación de la renovación del servicio con todo el protocolo y detalle de la creación en el nuevo entorno, así como del método más rápido y seguro para su migración.

El plan de devolución del servicio se diseñará para una ejecución inferior a 1 mes desde su inicio y no supondrá un coste extra para la SFMADRID.

Cumplimiento de los plazos de entrega de la documentación en un 98% de las ocasiones.

A la finalización de la contratación la SFMADRID se reserva la opción de compra del equipamiento en ese momento en uso, para ello los licitantes determinarán de antemano el valor residual del equipamiento aportando una tabla de amortización o similar, ya sea en el momento de contratación o en cualquiera de las posibles ampliaciones/sustituciones o cualquier cambio.

3ª. FECHA, FORMA Y LUGAR DE REALIZACIÓN DE LOS SERVICIOS

La fecha de finalización de la implantación e inicio de los servicios recurrentes será de **no más de 20 semanas desde el inicio del proyecto**, teniéndose en cuenta que **desde la semana 9 se irá realizando el despliegue gradual de la solución y migración**, se adjunta ejemplo ilustrativo del plan de proyecto (el adjudicatario deberá aportar el suyo equivalente a este en el caso de desacuerdo y justificar las diferencias):

	Predecesoras/	1				2				3				4				5			
	Dependencias	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20
1.- Análisis de SITUACIÓN ACTUAL	N/A																				
2.- DISEÑO / IMPLANTACIÓN	1																				
3.- TRANSICIÓN y GESTIÓN DEL CAMBIO	1;2																				
4.- Desactivación y destrucción equipamiento actual	1;2;3																				
X. Activación de Servicios recurrentes, Config. Recuperación, etc.	1;2;3;4																				
1. Gestión global del proyecto, plazos, entregas, calidades, etc.	N/A																				

El inicio del proyecto se iniciará **como máximo 15 días después de firma del contrato**.

4ª. RESPONSABLE DEL SERVICIO

El adjudicatario designará a una persona que actuará ante la SFMADRID, como responsable e interlocutor válido para atender cualquier cuestión relacionada con la entrega y los trabajos encomendados o incidencias que puedan surgir ante la contratación de esta prestación, bien por indicación de la SFMADRID o del propio proveedor.

5ª. CLÁUSULAS SOCIALES DE CARÁCTER OBLIGATORIO

1.- La empresa adjudicataria de la prestación debe respetar las normas sociolaborales vigentes en España y en la Unión Europea, así como las de la Organización Internacional del Trabajo.

Su incumplimiento conllevará las penalizaciones contenidas en el Pliego de Cláusulas Administrativas.

2.- En toda la documentación, publicidad, imagen o materiales que deban aportar los licitadores, o que sean necesarios para la ejecución del contrato, deberá hacerse un uso no sexista del lenguaje, evitando cualquier imagen discriminatoria de las mujeres o estereotipos sexistas, y fomentando con valores de igualdad la presencia equilibrada, la diversidad y la corresponsabilidad.

3.- La empresa adjudicataria tiene la obligación de adoptar las medidas de seguridad y salud en el trabajo que sean obligatorias para prevenir de manera rigurosa los riesgos que pueden afectar a la vida, integridad y salud de las personas trabajadoras.

Asimismo, deberá acreditar el cumplimiento de las obligaciones siguientes:

- La evaluación de riesgos y planificación de la actividad preventiva correspondiente a la actividad contratada.
- La formación e información en materia preventiva a las personas adscritas a la ejecución del contrato.
- El justificante de la entrega de equipos de protección individual que, en su caso, sean necesarios.

La empresa adjudicataria deberá acreditar el cumplimiento de estos extremos mediante declaración responsable, indicando de modo concreto las medidas y actuaciones llevadas a cabo, en cumplimiento de lo anterior.

4.- La empresa adjudicataria deberá acreditar, mediante declaración responsable, la afiliación y el alta en la Seguridad Social de las personas trabajadoras destinadas a la ejecución del contrato. Esta obligación se extenderá a todo el personal subcontratado por la empresa adjudicataria principal destinada a la ejecución del contrato.

Para la acreditación del cumplimiento de esta obligación, se exigirá a la empresa adjudicataria, al inicio de la ejecución del contrato, la presentación de una declaración responsable en la que se señale que las personas trabajadoras destinadas a la ejecución del contrato se encuentran afiliadas y dadas de alta en la Seguridad Social.

En todo caso, el órgano de contratación podrá solicitar, cuando lo considere oportuno, la aportación de la documentación que acredite el contenido de la declaración responsable.

5.- Con carácter previo a la finalización del contrato, la empresa adjudicataria deberá presentar un informe relativo al cumplimiento de las obligaciones sociales que le fueran exigibles legal o contractualmente,

6.- Las personas responsables del contrato supervisarán, con carácter anual, el cumplimiento de las obligaciones que, en relación con las cláusulas sociales se hayan impuesto directamente a la empresa adjudicataria en el pliego, o hayan sido ofertadas por éste, así como las que deriven de la legislación social y laboral vigentes.

De esta supervisión se evacuará el pertinente Informe escrito, que será remitido al contratista, y del que pudieran derivarse las responsabilidades pertinentes.

6ª. FUNCIONES DE VIGILANCIA Y CONTROL DEL CONTRATO POR PARTE DE LA SFMADRID.

La SFMADRID inspeccionará en todo momento la forma de prestación de los diferentes servicios en relación con las especificaciones del presente PPTP, a cuyo efecto mantendrá un servicio de inspección con la organización que estime oportuna.

Las facultades de los empleados de la SFMADRID designados para desempeñar las funciones de inspección, serán las siguientes:

a) Controlar que la entrega de los materiales se hace de manera adecuada y estos se encuentran en perfecto estado.

b) Controlar que los trabajos se efectúen oportunamente y en la forma estipulada.

c) Controlar si se cumple tanto lo estipulado en el presente PPTP, como en los posibles compromisos posteriores del adjudicatario en cuanto a la prestación del servicio de garantía.

Las decisiones de los empleados de la SFMADRID serán ejecutivas y se cumplirán de forma inmediata, o en su caso, en el plazo que fije el adjudicatario o persona que en cada momento lo represente con el visto bueno del responsable que la Dirección de la SFMADRID designe en cada momento.

ANEXO I
Cheklist Plataformado PC

DATOS DE ASIGNACIÓN	
USUARIO	UBICACIÓN (SEDE / PLANTA)
EMAIL EXTERNO	EMAIL INTERNO

PLATAFORMADO DE EQUIPOS; CHECKLIST	
TAREA	RESULTADO
0. Obtención de datos de usuario y migración del correo de POP3 a IMAP	
0.1. En el ordenador antiguo o a replataformar subir todos los archivos personales a One Drive	
0.2. Comprobar si tiene licencia de Office Local, en caso de que sí, apuntar en Observaciones software y licencia	
0.3. Si en el ordenador antiguo o a replataformar tiene el correo configurado como POP3, configurar cuenta por IMAP y migrar todo el correo a la carpeta IMAP	
1. Configuración de red	
1.1. Configuración de interfaz de red (DHCP)	
1.2. Configuración de recursos compartidos (Detección de redes y compartición de archivos e impresoras)	
1.3. Configuración de Hostname	
1.4. Configuración de VPN si es necesario	
2. Configuración inicial	
2.1. Vincular el ordenador con el dominio de SFMADRID	
2.2. Eliminar usuarios anteriores y que no pertenezcan al dominio	
2.3. Logarse con usuario de administración	
2.4. Configurar actualizaciones de Windows: Actualizaciones de Microsoft y avisar antes de cada reinicio.	
2.5. Realizar todas las actualizaciones de Windows	
2.6. Activar la característica de Windows: SMB 1.0/CIFS File Sharing Support y Servicios de Impresión y Documentos	
2.7. Actualizar servidor de sincronización horaría por hora.rediris.es	
2.8. Revisar que el servicio de sincronización horaria esta como automático	
2.9. Liberar espacio en disco (Avanzado y completo)	
2.10. Omitir alertas del centro de seguridad de Windows si hubiera alguna	
3. Instalación de software corporativo y sus actualizaciones y esintalación de software preinstalado innecesario:	
3.1. 7Zip	
3.2. Acrobat Reader	
3.3. Kitty y sus configuraciones	
3.4. GDC y sus configuraciones	
3.5. Java	
3.6. Navegadores Web: Chrome y Firefox	
3.7. Notepad++	
3.8. VNC: Instalación y configuración del servidor	
3.9. VLC	
3.10. Desintalación de software innecesario preinstalado	

PLATAFORMADO DE EQUIPOS; CHECKLIST	
TAREA	RESULTADO
4. Comprobación de usuario en el directorio activo	
4.1. Comprobar si el usuario dispone de licencia de Office 365 y que tipo de licencia posee	
4.2. Comprobar si el usuario existe en el directorio activo, si no existe solicitar su creación usando la plantilla y enviandoselo a Telefónica para su creación	
4.3. Hacemos login con el usuario del directorio activo	
5. Instalación y configuración de software específico: Aplicaciones Visual Basic. Solo realiar en aquellos casos en las que los usuarios trabajen con aplicaciones de este tipo. Si no es necesario saltar al siguiente punto	
5.1. Copia de fichero de hosts y services de Windows	
5.2. Instalación de los Drivers ODBC de Informix tanto de 32 como de 64 bits	
5.2.2. Configurar los conectores de ODBC de Informix oportunos para el funcionamiento de las aplicaciones.	
5.3. Instalación de Visual Basic 6.0, realizando la instalación por defecto quitando en la personalización el apartado de "Data Access"	
5.3.1. Copia de las aplicaciones de Visual Basic correspondientes y creación de los accesos directos.	
6. Instalación y configuración de software específico: Sistemas de Información	
6.1. Filezilla	
6.2. Genero Studio	
6.3. TortoiseSVN	
6.4. SoapUI	
6.5. VNC: Instalación del cliente	
7. Instalación y configuración de software específico: Común	
7.1. Abrimos Acrobat Reader y lo seleccionamos como predeterminado para abrir ficheros .pdf	
7.2. Abrimos Firefox y lo seleccionamos como navegador predeterminado	
8. Personalizaciones de Windows	
8.1. Desactivar sugerencias del menú de inicio (Personalización / Inicio)	
8.2. Desinstalación de aplicaciones preinstaladas no deseadas	
8.3. Activar mostrar extensiones de archivos conocidos	
8.4. Instalación de fuentes (Futura STD) y plantillas corporativas	
8.5. Configuración de impresoras	
8.6. Omitir alertas del centro de seguridad de Windows si hubiera alguna	
8.7. Crear carpeta compartida C:\escaner, crear acceso directo en el escritorio, y permitir al usuario que determinemos la lectura y escritura en ella	
8.8. Revisar si el usuario necesita otras aplicaciones, instalarlas e incluir un acceso directo en el escritorio por cada una de ellas. En el caso de que sea aplicación web solo crear acceso directo en el escritorio. Algunos ejemplos son los siguientes: A3, ADALIDES, CITRIX RECEIVER, CORREO INTERNO, INTRANET DEL AYUNTAMIENTO DE MADRID, LEXNET, PYV	
8.9. Eliminar accesos directos inecesarios para el usuario	

PLATAFORMADO DE EQUIPOS; CHECKLIST	
TAREA	RESULTADO
9. Instalación y configuración de software adicional: Usuarios con licencias Office 365 Empresa Essentials y Exchange Online Plan 1. Si no dispone de este tipo de licencias saltar al siguiente punto	
9.1. Instalamos y realizamos login en One Drive. Configuramos One Drive para que realice la sincronización de las carpetas personales (Escritorio, Documentos e Imágenes)	
9.2. Instalamos y configuramos Skype Empresarial	
9.3. Instalamos la última versión de LibreOffice así como su ayuda offline	
9.3.1. Configuramos la fuente predeterminada (Futura Std) para todos los documentos en Writter. Podemos hacerlo directamente desde las Opciones de Writter.	
9.3.2. Configuramos la fuente predeterminada (Futura Std) para todos los documentos en Calc. Para relizarlo hay que seleccionar en una hoja nueva todo e libro y aplicar la fuente, guardar el documento como plantilla y establecerla como predeterminada.	
9.4. Instalamos la última versión de Thunderbird	
9.4.1. Abrimos Thunderbird	
9.4.2. Activar la extensión Lighting que nos permite el uso del calendario en todos los perfiles	
9.4.3. Instalar en todos los perfiles las extensiones TBSync y Provider for Exchange	
9.4.4. En las opciones configuramos la fuente por defecto (Futura Std - Pequeña)	
9.4.5. En las opciones configuramos e instalamos el paquete de idioma Español para la correción situado en Redacción / Ortografía	
9.4.6. Configuración de cuenta de correo externa en todos los perfiles (Siempre por IMAP)	
9.4.6.1. En la pestaña general de la cuenta debemos configurar nuestra firma, siempre pasando el archivo HTML (recordad que debemos hacer esto para tantos perfiles como usen el buzón / ordenador)	
9.4.6.2. Hacemos clic en el botón de "Administrar identidades..."	
9.4.6.2.1. En el caso de que se trate de una cuenta antigua y se realice el login con el dominio emsf.es, debemos sustituir la dirección de correo electrónico por el nuevo dominio sfmadrid.es	
9.4.6.2.2. Dirigirnos a la pestaña "Redacción y direcciones", en y poner mi firma debemos seleccionar "Bajo mi respuesta (sobre el texto citado), así como marcar la opción de "Incluir firma en las respuestas" e "Incluir firma en los re-envíos". Aceptamos y salimos de esta ventana.	
9.4.6.3. En la pestaña de "Copias y carpetas" de la cuenta debemos desmarcar la opción de "Al enviar mensajes, automaticamente, Poner una copia en:". Aceptamos la configuración y volvemos a la ventana principal.	
9.4.7. Hacemos clic con el botón derecho sobre nuestro perfil de correo recientemente creado y hacemos clic sobre "Suscribirse..." En la ventana emergente debemos seleccionar "Elementos enviados", "Borradores" y "Correo no deseado"	
9.5. Configuramos la extensión de TbSync, debemos sincronizar todas las opciones disponibles y poner que se realice automáticamente cada 20 minutos	
9.6. Eliminar del escritorio los accesos de correo electrónico que no sean Thunderbird	

PLATAFORMADO DE EQUIPOS; CHECKLIST	
TAREA	RESULTADO
10. Instalación y configuración de software adicional: Usuarios con licencias Office 365 Empresa Premium y Project Online Profesional. Si no dispone de este tipo de licencias saltar al siguiente punto	
10.1. Instalamos y realizamos login en One Drive. Configuramos One Drive para que realice la sincronización de las carpetas personales (Escritorio, Documentos e Imágenes)	
10.2. Instalamos todas las aplicaciones de Office (versión de escritorio).	
10.3. Acrimos cualquiera de las aplicaciones como Excel o Word y realizamos el login oportuno con la cuenta de OFFICE 365 que corresponda	
10.4. Abrimos Microsoft Outlook	
10.4.1. Configuramos la cuenta de correo externo en Microsoft Outlook	
10.4.1.1. Configurar la firma del correo electrónico para envíos y respuestas	
10.4.2. Configuramos fuente predeterminada como Futura STD	
10.4.3. Eliminar del escritorio los accesos de correo electrónico que no sean Microsoft Outlook	
10.5. Configurar Teams iniciando sesión y configurandola para que se abra en segundo plano	
11. Realizamos pruebas para comprobar el correcto funcionamiento	
11.1. Abrimos cmd	
11.1.1. Comprobamos con ipconfig que la dirección IP asignada por DHCP es la correcta	
11.1.2. Realizamos por ping pruebas de conectividad básica	
11.2. Abrimos explorador de Windows	
11.2.1. Comprobamos que tras logarnos con el usuario del directorio activo aparecen las unidades de red pertinentes, si no es así, reclamar a Telefónica.	
11.2.2. Comprobamos que se muestran las extensiones de todos los archivos	
11.3. Abrimos el gestor de correo electrónico	
11.3.1. Comprobamos que el usuario tiene la firma correctamente configurada	
11.3.2. Comprobamos que el usuario puede gestionar su calendario	
11.3.3. Comprobamos que el usuario tiene acceso correcto a los contactos corporativos	
11.3.4. Realizamos pruebas de envío y recepción	
11.4. Comprobación de que todo el software instalado personalizado funciona sin problemas	
11.5. Realización de pruebas de impresión en las impresoras configuradas	
11.6. Realizamos pruebas de escaneado en el caso de que sea necesario	
11.7. Ponerse en contacto con la persona responsable del proceso (Daniel Sanchez / Rafael Villa) para comprobar que llegamos a los equipos por VNC	
12. Entrega / Formación / Recopilación de Datos	
12.1. Completar los datos de finalización del plataformado	
12.2. Facilitar documentación con datos de acceso al usuario e indicar que deben cambiar su contraseña	
12.3. Acceder con el usuario con sus credenciales y comprobar junto a él que todo esta bien, y que puede acceder a todo. Proporcionar formación en los aspectos que el usuario considere oportunos acerca del nuevo sistema operativo.	
12.4. Entregar checklist y documentación completado a la persona responsable disponible de Sistemas de la Información (Daniel Sanchez / Rafael Villa)	

PLATAFORMADO DE EQUIPOS; CHECKLIST			
DATOS DE ASIGNACIÓN			
USUARIO		UBICACIÓN (SEDE / PLANTA)	
EMAIL EXTERNO		EMAIL INTERNO	
REEMPLAZO EQUIPAMIENTO			
PC RETIRADO		¿DESTRUIR?	
MODELO	N.º INVENTARIO / SERIE	IP	
PC NUEVO			
MODELO	N.º INVENTARIO / SERIE	IP	
LICENCIA		HOSTNAME	
MONITOR RETIRADO		¿DESTRUIR?	
MODELO		N.º INVENTARIO / SERIE	
MONITOR NUEVO			
MODELO		N.º INVENTARIO / SERIE	
OBSERVACIONES			

ANEXO II
Nota técnica configuración Tablets

1. OBJETIVO

El presente documento, describe la configuración propuesta por parte del cliente Servicios Funerarios de Madrid (SFM) sobre la plataforma VMware AirWatch.

2. DOCUMENTACIÓN RELACIONADA

Como apoyo a la elaboración de este documento, se han tenido en cuenta documentación y/o ayuda de fabricante VMware, así como la propia del servicio móvil gestionado Movistar y documentación ofrecida por parte del cliente.

3. DESCRIPCIÓN

El cliente Servicios Funerarios De Madrid (SFM), tiene contratado la gestión de dispositivos mediante plataforma VMware AirWatch para poder gestionar de forma remota sus dispositivos móviles con un volumen aproximado de 100 dispositivos Android.

Para la gestión de los dispositivos, se plantea desde Telefónica, una propuesta de configuración bajo Android Enterprise (Work Manage) salvo que el dispositivo no sea compatible. Dispositivos no compatibles con esta integración serán gestionados/administrados por el método convencional “Admin Device” reconocidos como dispositivos Android Legacy.

Los dispositivos serán asociados a usuarios definidos por parte del cliente bajo una estructura de grupos organizativos.

A continuación, se van a ir describiendo las distintas configuraciones propuestas, requerimientos, conclusiones, etc.

4. ESCENARIO

Las configuraciones, requerimientos, conclusiones, etc. descritos en este documento se basan en lo realizado en la plataforma VMware AirWatch donde el cliente va a inscribir los dispositivos en producción, aunque las pruebas se han realizado en un entorno separado a tal efecto.

El aplicativo VMware AirWatch, se dispone en versión 9.6.0.16.

- Url.: https://mdm.movistar.es/AirWatch
- OG: MDM0125841-EMP.MUN.DE SERV. FUNER. Y CEM. DE MADRID
- ID Group: MDM0125841
- Aplicativo VMware Hub 19.03.(aplicativo de inscripción)
- Conectividad Wifi (inscripción) y 4G (resto de conexión)

- Dispositivos:
    - Dispositivos Huawei MediaPad M5

5. PROPUESTA DE CONFIGURACION

A continuación, se describen las configuraciones propuestas por cada uno de los puntos anteriormente citados.

Las capturas que se muestran corresponden al entorno de cliente a modo de comprobación de la propia configuración solicitada, bajo el nombre de grupo organizativo siguiente:

- MDM0125841-EMP.MUN.DE SERV. FUNER. Y CEM. DE MADRID

Aquellas parametrizaciones concretas que no sean citadas se dejarán tal y como estén por defecto.

El orden en el que se describen las configuraciones en este documento atiende al que se ha seguido a la hora de parametrizar el entorno de cliente.

Todas las configuraciones descritas a continuación, a no ser que se describa lo contrario explícitamente, han sido configuradas desde el nivel del grupo organizativo padre.

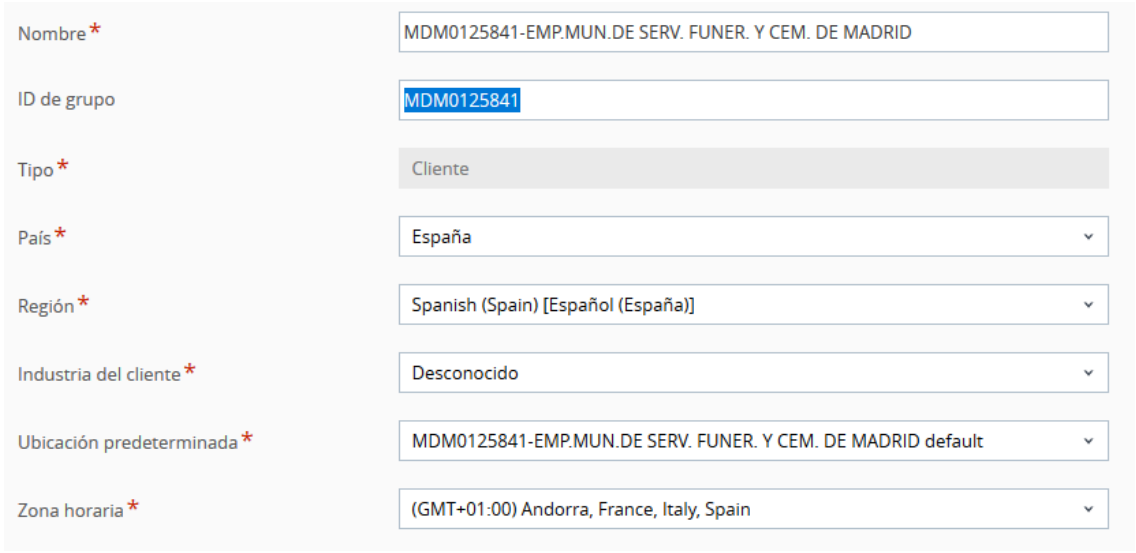
GRUPO ORGANIZATIVO CLIENTE

En la plataforma VMware AirWatch, se debe contar con un grupo organizativo de tipo cliente (customer), el cual será el entorno del cliente.

Sobre este grupo organizativo, es donde se realizarán todas las configuraciones de ajustes raíz, grupos, perfiles, carga de usuarios, inscripciones, etc. para el proyecto.

El ID de inscripción del grupo padre, por defecto, es el identificador del código de servicio del cliente: **MDM0125841**. Este ID no debe ser modificado.

El parámetro de región y zona horaria deberán parametrizarse a “España/Spain”.



CONFIGURACIÓN AJUSTES RAÍZ

En los ajustes raíz del entorno del cliente, sobre el grupo organizativo padre, existen las siguientes configuraciones.

INTEGRACION ANDROID ENTERPRISE

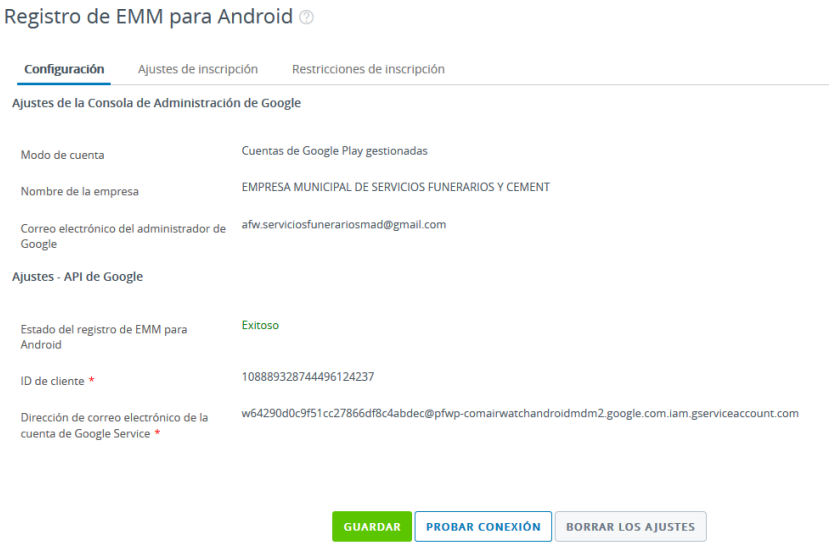
Integración ***Registro de EMM para Android*** *desde Ajustes > Android*

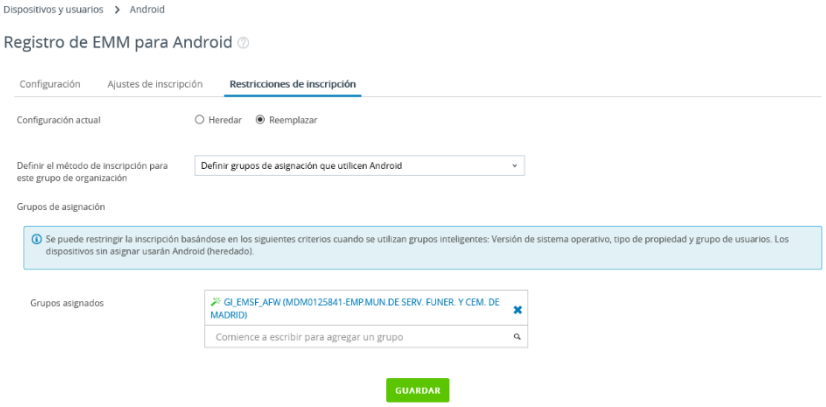
- Esta parametrización, activa la integración con Google para la gestión de los dispositivos mediante Android Enterprise.
- Para esta integración, se requiere de una cuenta Gmail.

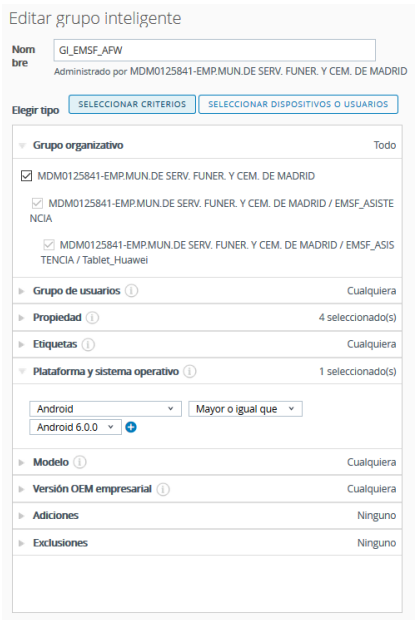
Como se puede observar en las siguientes imágenes se ha elegido una parametrización en la que pueden convivir dispositivos Android Enterprise y Android Legacy.

La propia plataforma gestionará los dispositivos de un modo u otro según el sistema operativo de los terminales, teniendo en cuenta los estándares impuestos por el proveedor (Google).

Dispositivos a partir de Android 6.0.0 serán inscritos por la propia plataforma como dispositivo Android Enterprise.


Registro de EMM para Android
Configuración
Ajustes de inscripción
Restricciones de inscripción
Ajustes de la Consola de Administración de Google
Modo de cuenta
Cuentas de Google Play gestionadas
Nombre de la empresa
EMPRESA MUNICIPAL DE SERVICIOS FUNERARIOS Y CEMENT
Correo electrónico del administrador de Google
afw.serviciosfunerariosmad@gmail.com
Ajustes - API de Google
Estado del registro de EMM para Android
Exitoso
ID de cliente *
108889328744496124237
Dirección de correo electrónico de la cuenta de Google Service *
w64290d0c9f51cc27866df8c4abdec@pfwp-comairwatchandroidmdm2.google.com.iam.gserviceaccount.com
GUARDAR
PROBAR CONEXIÓN
BORRAR LOS AJUSTES


Dispositivos y usuarios
Android
Registro de EMM para Android
Configuración
Ajustes de inscripción
Restricciones de inscripción
Configuración actual
Heredar
Reemplazar
Definir el método de inscripción para este grupo de organización
Definir grupos de asignación que utilicen Android
Grupos de asignación
Se puede restringir la inscripción basándose en los siguientes criterios cuando se utilizan grupos inteligentes: Versión de sistema operativo, tipo de propiedad y grupo de usuarios. Los dispositivos sin asignar usarán Android (heredado).
Grupos asignados
GI_EMSF_AFW (MDM0125841-EMP.MUN.DE SERV. FUNER. Y CEM. DE MADRID)
Comience a escribir para agregar un grupo
GUARDAR


Editar grupo inteligente
Nombre
GI_EMSF_AFW
Administrado por MDM0125841-EMP.MUN.DE SERV. FUNER. Y CEM. DE MADRID
Elegir tipo
SELECCIONAR CRITERIOS
SELECCIONAR DISPOSITIVOS O USUARIOS
Grupo organizativo
Todo
MDM0125841-EMP.MUN.DE SERV. FUNER. Y CEM. DE MADRID
MDM0125841-EMP.MUN.DE SERV. FUNER. Y CEM. DE MADRID / EMSF_ASISTENCIA
MDM0125841-EMP.MUN.DE SERV. FUNER. Y CEM. DE MADRID / EMSF_ASISTENCIA / Tablet_Huawei
Grupo de usuarios
Cualquiera
Propiedad
4 seleccionado(s)
Etiquetas
Cualquiera
Plataforma y sistema operativo
1 seleccionado(s)
Android
Mayor o igual que
Android 6.0.0
Modelo
Cualquiera
Versión OEM empresarial
Cualquiera
Adiciones
Ninguno
Exclusiones
Ninguno

COMUNICACIONES PUSH AWCM

Comunicaciones Push hacia dispositivos vía AWCM (activado por defecto)

- Aunque esta opción viene configurada por defecto de la forma deseada, es recomendable revisar que esta, esté correctamente habilitada, para que la comunicación de plataforma contra los dispositivos sea mediante AWCM (AirWatch Cloud Messaging).
- La comprobación se realiza en Ajustes > Configuración del Agent > AirWatch Cloud Messaging.

5.1.1. INSCRIPCION

Las políticas de inscripción actualmente son heredadas del nivel global definidas por parte de Telefónica.

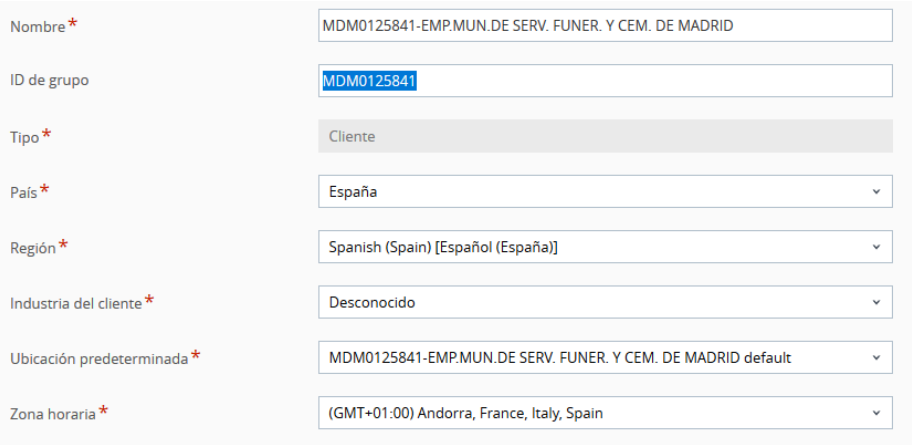
Estas políticas pueden ser redefinidas a petición de cliente siendo así más restrictivas:

CONFIGURACIÓN DE GRUPOS ORGANIZATIVOS

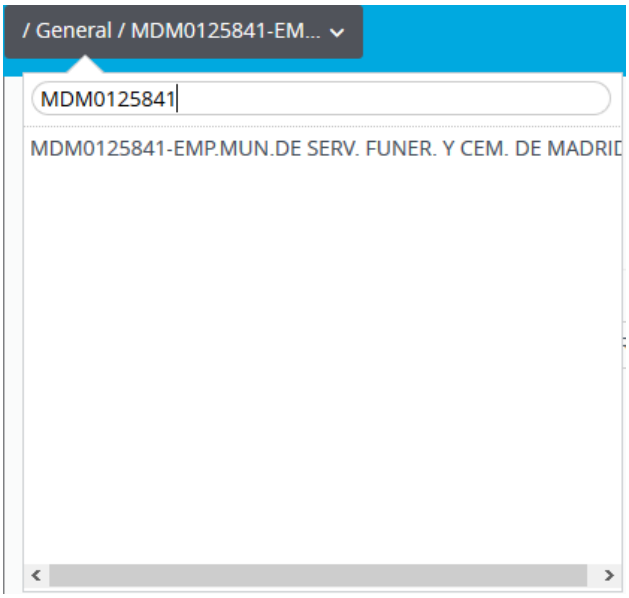
Se ha redefinido la gestión de grupos organizativos que tenía el cliente definido. Simplificando a un solo grupo organizativo con el siguiente nombre e identificador:

- **Grupo Organizativo:** MDM0125841-EMP.MUN.DE SERV. FUNER. Y CEM. DE MADRID
- **ID de Grupo:** MDM0125841

- Detalle del grupo organizativo hijo:



- Detalle de jerarquía del entorno del cliente:



CONFIGURACIÓN DE GRUPOS DE USUARIOS

Se han creado varios grupos de usuarios:

- "GU_O365" este grupo de usuarios está vinculado al grupo inteligente GI_O365 el cual asignará las aplicaciones de la suite de MS Office 365 a los usuarios que se asignen en el grupo.

Nombre de grupo	Tipo	Grupo organizativo
GU_O365	Personalizado	MDM0125841-EMP.MUN.DE SERV. FUNER. Y CEM. DE MADRID

**Al asignar un usuario a este grupo el aplicativo WPS Office será suprimido de los dispositivos asociados al usuario.*

- "GU_GOOGLE" este grupo de usuarios está vinculado al grupo inteligente GI_GOOGLE el cual asignará las aplicaciones de la suite de Google a los usuarios que se asignen en el grupo. Mas adelante en el documento se detalla el proceso.

Nombre de grupo	Tipo	Grupo organizativo
GU_GOOGLE	Personalizado	MDM0125841-EMP.MUN.DE SERV. FUNER. Y CEM. DE MADRID

CONFIGURACION DE GRUPOS DE ASIGNACION "GI"

Todos los GI han sido creados del tipo "seleccionar criterios", donde sean seleccionado los criterios específicos según la necesidad.

A nivel de grupos de asignación, se han definido los siguientes grupos:

- GI_Aplicaciones Corporativas

  El grupo es utilizado para asignar las aplicaciones asociadas al plataformado de los dispositivos definido por el cliente.

- GI_Dispositivos_Samsung

  La función de este grupo es de diferenciar los dispositivos Samsung del resto de dispositivos, es utilizado para desplegar aplicaciones especificas solo para dispositivos Samsung como puede ser AirWatch Samsung ELM Service o cliente de correo nativo como puede ser Samsung Mail, (queda a disposición de uso, aunque para el este caso no es necesario).

- GI_EMSF_AFW

El grupo es utilizadoo para la asignación de perfiles/políticas de configuración a los dispositivos inscritos utilizando Android Enterprise.

- GI_EMSF_LEGACY

El grupo se ha definido para la asignación de perfiles/políticas de configuración a los dispositivos inscritos utilizando Android Legacy. (queda a disposición de uso, aunque para el este caso no es necesario).

- GI_O365

El uso del grupo impulsa la asignación de aplicaciones de la Suite de MS Office 365 a los dispositivos de los usuarios pertenecientes al grupo de usuarios **GU_O365.**

- GI_GOOGLE

El uso del grupo impulsa la asignación de aplicaciones de la Suite de Google a los dispositivos de los usuarios pertenecientes al grupo de usuarios **GU_GOOGLE**.

CONFIGURACION DE PERFILES DE ANDROID (ANDROID ENTERPRISE)

La creación/publicación de perfiles de configuración se realiza desde la opción de perfiles, disponible en consola VMware AirWatch desde Dispositivos > Recursos y Perfiles > Perfiles > Android.

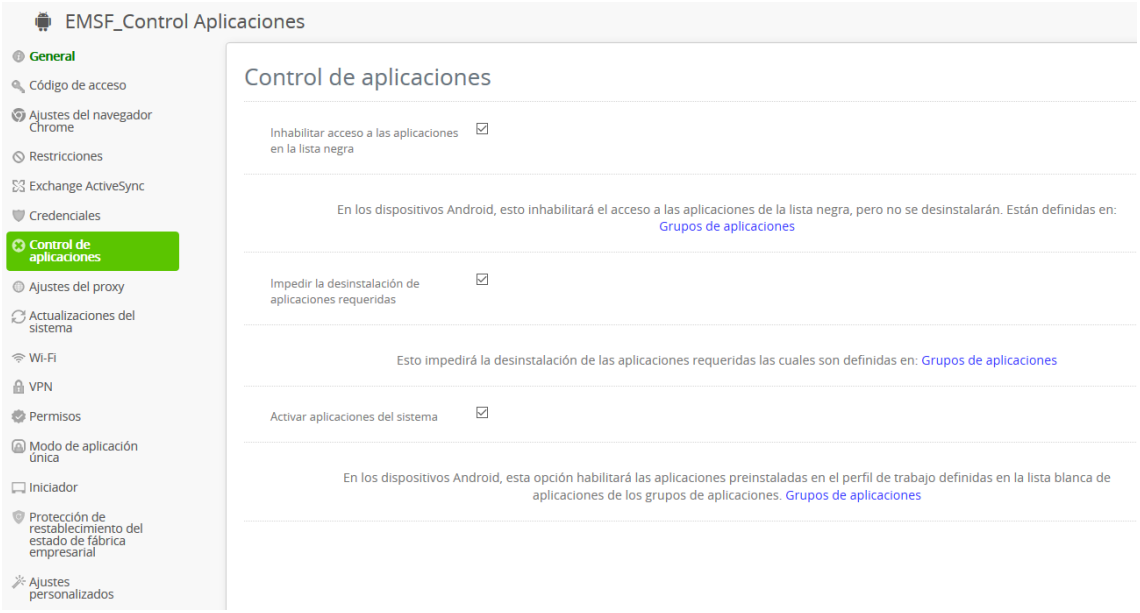
La asignación de estos perfiles va asociada al grupo inteligente “GI_EMSF_AFW”

A continuación, se describen las funciones que tienen cada uno de los perfiles definidos para los dispositivos asignados.

CONTROL DE APLICACIONES

El objetivo es incluir en lista blanca las aplicaciones del sistema operativo de los dispositivos, es por ello la definición de un perfil de control de aplicaciones. En este caso en concreto se ha definido como EMSF_Control Aplicaciones.

Aplicaciones de terceros dedicadas a fines no corporativos (Entretenimiento, Deportes, Juegos, Redes Sociales, etc.) instaladas en el sistema operativo serán bloqueadas gracias a este perfil.



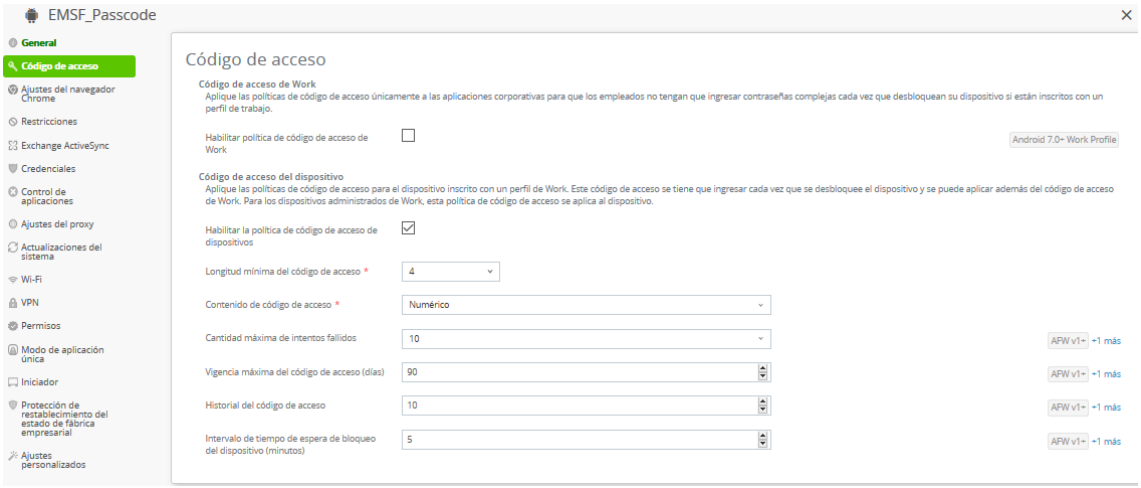
CÓDIGO DE ACCESO

Para aumentar la seguridad a los dispositivos se ha definido un perfil de código de acceso, denominado EMSF_Passcode.

Como se puede observar se ha definido un código de bloqueo de mínimo cuatro dígitos numéricos. Un máximo de intento de fallos de 10.

El usuario deberá refrescar el código cada 90 días teniendo en cuenta que existe un historial de 10 códigos anteriores.

Para terminar, el dispositivo se bloqueará automáticamente cada 5 min como así se ha solicitado.



RESTRICCIONES

Se ha definido un perfil de restricciones para los dispositivos siguiendo las directrices de cliente. Las opciones descritas será objeto de restricción, las opciones no descritas estarán disponibles en los dispositivos debido a que no están siendo objeto de ningún tipo de restricción. Pueden ser ajustables a necesidad del usuario final.

- Funcionalidades de dispositivo:
  - Bloqueo del restablecimiento del dispositivo por parte del usuario final.
  - Bloqueo para inhibir la integración con Google Enterprise.
  - Inhabilitación de reinicio seguro de los terminales.

- Aplicación
  - Bloqueo de instalación de aplicaciones de fuentes desconocidas.
- Sincronización y almacenamiento
  - Bloqueo de la depuración de USB.
  - Bloqueo de la transferencia de archivos por USB.
  - Bloqueo de medios físicos de almacenamiento.

- Red
  - Bloqueo de redes WiFi.
  - Bloqueo de cambios al perfil de administración WiFi.

- Servicios de ubicación
  - Restringir el uso de la ubicación a alta precisión.

El perfil es denominado EMSF_Restricciones.

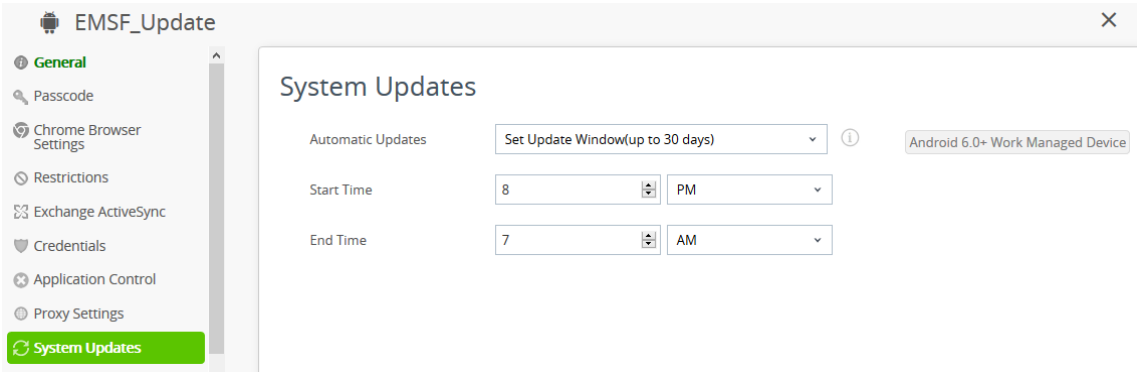
ACTUALIZACIONES DE SISTEMA

Desde el portal de gestión MDM VMware AirWatch se ha definido un perfil para gestionar las actualizaciones del sistema operativo de los dispositivos.

Se sabe que un proceso de upgrade de un dispositivo puede tardar varios minutos (aprox 45 min), es por ello por lo que se ha definido un horario fuera del horario pico de trabajo, para que no afecte en el caso de negocio del cliente.

La configuración definida para los dispositivos es de una ventana de actualización de entre las 20.00h hasta las 07.00h del día siguiente.

**Debe existir actualización disponible para los dispositivos. Adicionalmente los dispositivos deben estar conectados a la plataforma MDM.*



ASIGNACION DE APLICACIONES

A petición del cliente se han incluido en el despliegue de aplicaciones desde el portal MDM VMware AirWatch las indicadas a continuación:

A continuación, se describen las parametrizaciones de cada grupo inteligente.

GRUPO INTELIGENTE "GI_APLICACIONES CORPORATIVAS"

A continuación, se citarán las aplicaciones que se desplegarán a los dispositivos almacenados en el grupo organizativo "EMSF Asistencia".

Es por tanto que el grupo inteligente "GI_Aplicaciones Corporativas" empujará las aplicaciones

- Google Maps
- CamScanner
- Adobe Reader
- Whatsapp
- Google Chrome
- Hojas de cálculo de Google
- Google Drive
- Microsoft Outlook
- Microsoft OneDrive
- WPS Office

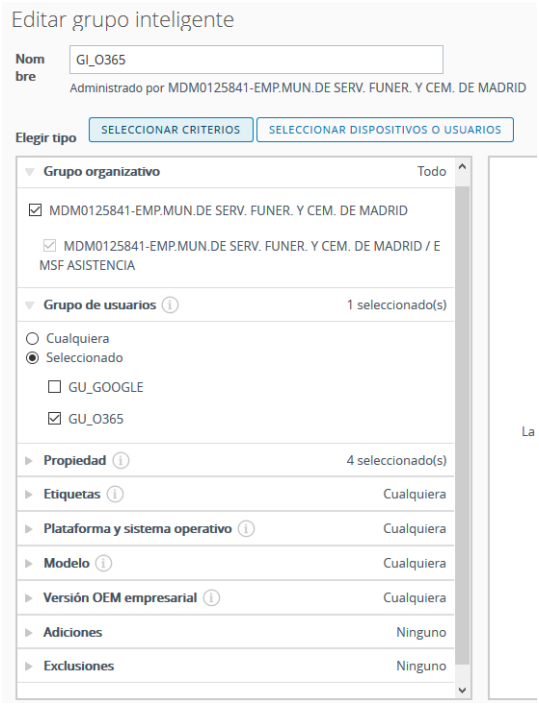
GRUPO INTELIGENTE "GI_O365"

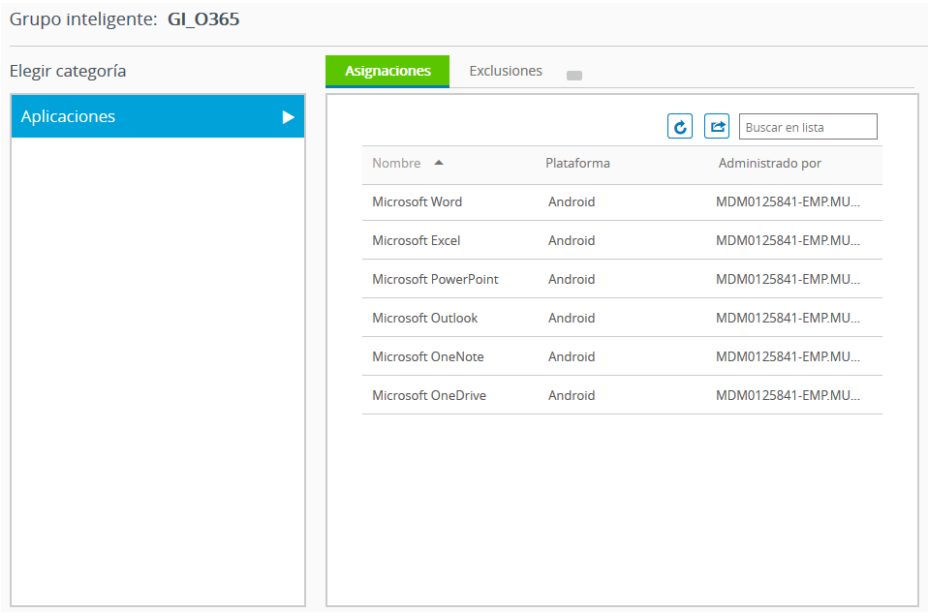
Las aplicaciones citadas a continuación son desplegadas a través de la asignación del grupo inteligente denominado "GI_O365"

- Microsoft Excel

- Microsoft OneNote
- Microsoft PowerPoint
- Microsoft Word

**La asignación del aplicativo contendrá la configuración de correo corporativo en el caso de los dispositivos Android Enterprise (en el caso de Android legacy no es compatible).*



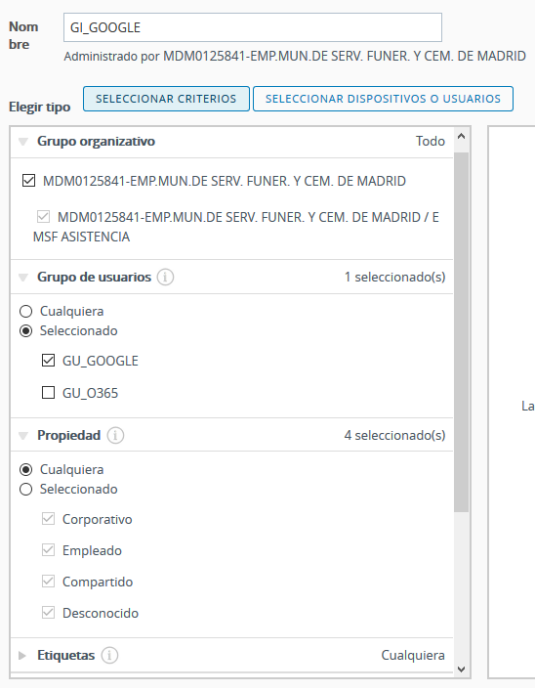


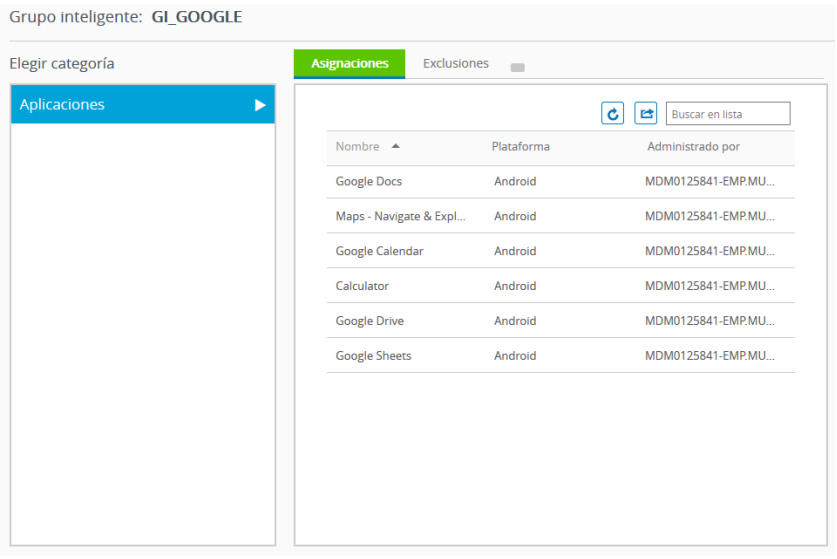
El despliegue de estas aplicaciones será realizado a peticion de cliente si el lo requiere.

GRUPO INTELIGENTE “GI_GOOGLE”

Si ha definido un grupo inteligente dedicado a la distribución de las aplicaciones de Google. El grupo ha sido denominado “”GI_GOOGLE, como puesta en marcha se han asociado las principales aplicaciones de la suite de Google.

- Google Documentos
- Google Calendar
- Google Calculadora
- Google Drive

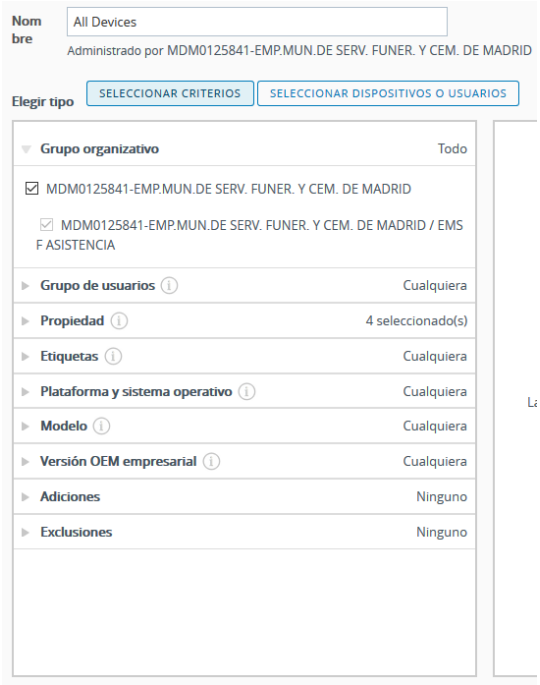


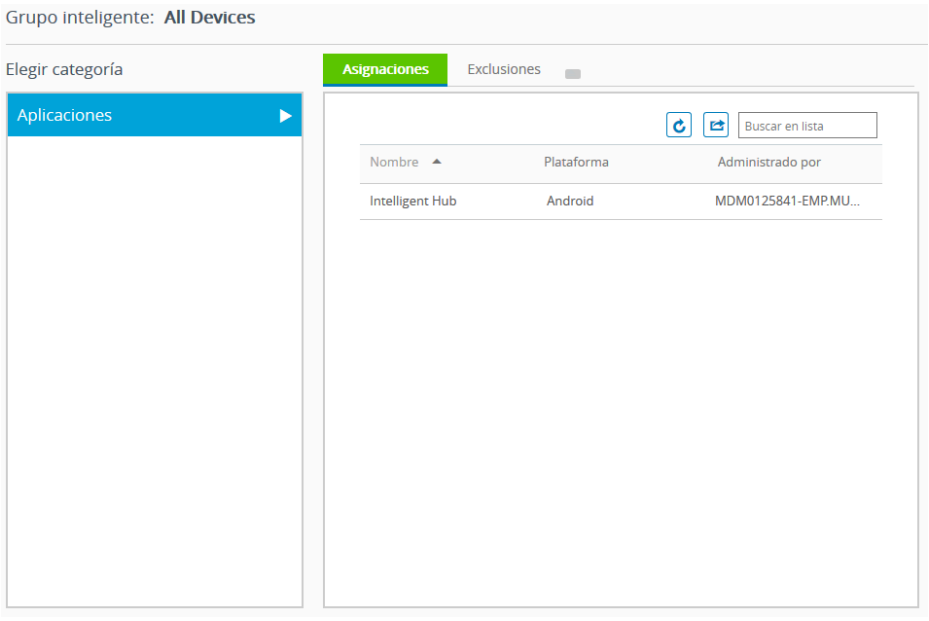


GRUPO INTELIGENTE “ALL DEVICES”

El grupo inteligente “ALL DEVICES” es un grupo inteligente creado por defecto en el entorno del cliente. En este caso es utilizado para la asignación del agente de gestión del portal MDM (Intelligent Hub).

**La asignación del aplicativo a por este grupo afectará a todos los dispositivos del tenant. Esta asignará ayudará a que todos los dispositivos tengan el agente de Airwatch actualizado, con las bondades que conlleva.*





CONFIGURACIÓN DE DISPOSITIVOS

A continuación, se describen las operativas a realizar que no pueden ser automatizadas por el MDM.

Para culminar el trabajo de maquetado de los dispositivos es necesario describir las operaciones a realizar para ejecutar la propuesta de configuración interpuesta por el cliente.

Hay que tener en cuenta que las operaciones descritas en este punto no pueden ser automatizadas por el MDM ya sea por limitaciones de gestión por parte de la plataforma MDM como por limitaciones de los propios dispositivos.

AJUSTES

En el caso de sistema operativo Android no se pueden definir ciertos ajustes como:

- Imagen corporativa, el cliente ha solicitado la asignación de una imagen de marca. Es necesaria aplicarla como **fondo de pantalla** y **fondo de bloqueo.**

El fondo de pantalla está disponible a través de la url:

https://ds-mdm.movistar.es/MyDevice/s/5127/ed125cd5-f70f-405e-aaf0-7b001abc11b9

- Enlace de periféricos por bluetooth, desde el entorno MDM se ha definido que la tarjeta bluetooth este definida para emparejarse con un periférico compatible, pero es necesario emparejarlo de forma manual.
- Configuración de idioma por defecto y único, se debe seleccionar el idioma español.

APLICACIONES

A petición de cliente se deben aplicar una determinada configuración para ciertas aplicaciones incluidas en el maquetado del dispositivo.

- **Microsoft Outlook:** Se requiere de habilitar de permisos a la aplicación para que pueda descargar documentos en el espacio de almacenamiento del dispositivo.

- **Google Drive**: es necesario que este logado una cuenta genérica proporcionada por el cliente:
  - Usuario: informesdeasistencia@gmail.com
  - Contraseña: Informesdeasistencia2019

- **WhatsApp:** es necesario introducir el número de teléfono corporativo del usuario final (+34 6XX XXX XXX) e introducir el código de validación recibido por SMS.
- **Microsoft OneDrive:** el aplicativo no permite lanzar configuración avanzada a la que añadir la cuenta O365. Es necesario asignar la cuenta de O365 y la contraseña asociada a la cuenta.
  - Usuario: usuario_cliente@emsf.es
  - Contraseña: [contraseña_cliente]

Se requiere de habilitar de permisos a la aplicación para que pueda descargar documentos en el espacio de almacenamiento del dispositivo.

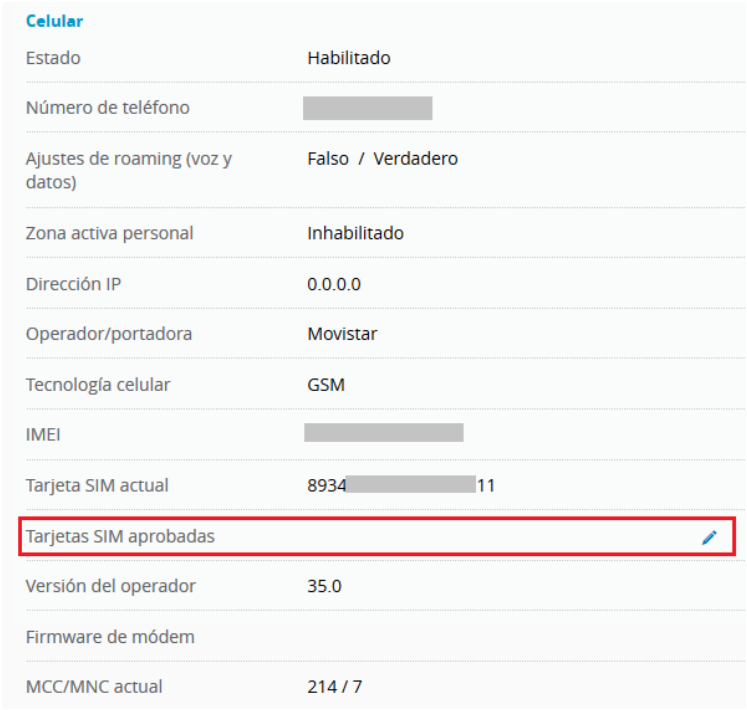
TELECOM

El módulo Telecom es utilizado para supervisar el uso básico de la red móvil de los dispositivos inscritos en el entorno.

MODULO DE RED EN LOS DISPOSITIVOS

A petición de cliente se ha solicitado restringir el dispositivo a la red de cliente debido a que se desconoce si el cliente hace uso de un APN privado, se ha determinado vincular el ICC de la tarjeta SIM al dispositivo por medio del portal MDM.

Si este no coincidiese con el enumerado en la plataforma MDM el dispositivo carecerá de red móvil.



De manera automatizada desde telefónica se reservará el uso a la SIM instalada en el momento del enrollment del dispositivo en el portal MDM.

CARGA Y ASIGNACION DE USUARIOS

CARGA DE USUARIOS

La carga de usuarios ha sido realizada mediante batch, con el fichero en formato .csv correspondiente.

Teniendo en cuenta los siguientes datos:

- Nombre de usuario de inscripción
- Nombre para mostrar en consola
- Apellido para mostrar en consola
- Password para inscripción
- Dirección de correo electrónico
- Grupo Organizativo de inscripción

**Los datos de los usuarios han sido proporcionados por cliente siendo la entidad custodia de las contraseñas de los usuarios.*

Se adjunta fichero .csv de la carga actual de usuarios.

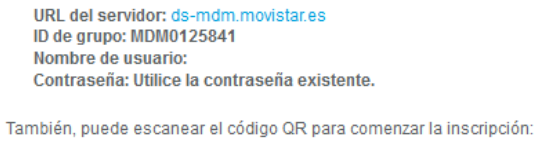
MÉTODO DE INSCRIPCIÓN

Para inscribir los dispositivos en la plataforma MDM vamos a utilizar dos métodos de inscripción dependiendo del dispositivo.

INSCRIPCIÓN ENTERPRISE

Dado que la configuración del entorno está integrada con Android Enterprise, en el arranque inicial del dispositivo (valores de fabricante), cuando éste, solicite inicio de sesión con cuenta de Google, se introducirá el identificador **afw#hub** lo que desencadenará mediante varias pantallas de asistente, la descarga del agente de VMware Hub y la inscripción como Android Enterprise Manage.

Una vez completado estos pasos, se mostrará el agente VMware Hub, solicitando la inscripción en MDM, donde se utilizará la inscripción mediante la opción “Código QR”, donde se utilizará el código QR facilitado o la configuración de manera manual.



**Este QR es solamente a nivel de demostración en este documento; no se debe utilizar para inscripciones en producción.*

Nota: Si durante este proceso de instalación de VMware Hub, por inactividad u otro motivo, el dispositivo requiere la atención de inicio de sesión en la barra de notificaciones (Acción necesaria en cuenta), se deberá abrir de forma manual la App “Hub” para continuar con el proceso de inscripción.

Cuando el propio agente de inscripción VMware Hub lo requiera, se deberá introducir el usuario y contraseña para continuar la inscripción.

La tarea completa de inscripción puede demorar varios minutos en función de la carga de red de datos, tamaño de aplicaciones a descargar, etc.

INSCRIPCION LEGACY

El entorno de cliente sigue operativo para inscribir dispositivos Android en modo Legacy.

(Método disponible para dispositivos Android con SO inferior a la versión 6.0). Es por ello que se explica el método de inscripción por si en algún momento de la vida del servicio fuese necesario.

Para este método es necesario iniciar el dispositivo (no es necesario parametrizar ninguna característica adicional).

Es necesario estar conectado a una red. Se requiere descargar el aplicativo Intelligent Hub desde el aplicativo Play Store .

Para ello es necesario asociar una cuenta de Gmail en el dispositivo y poder descargar el aplicativo.

Una vez completado estos pasos, se mostrará el agente VMware Hub en el dispositivo solicitando la inscripción en MDM, donde se utilizará la inscripción mediante la opción “Código QR”, donde se utilizará el código QR facilitado.

URL del servidor: ds-mdm.movistar.es
ID de grupo: MDM0125841
Nombre de usuario:
Contraseña: Utilice la contraseña existente.

También, puede escanear el código QR para comenzar la inscripción:

Este QR es solamente a nivel de demostración en este documento; no se debe utilizar para inscripciones en producción.

También es posible realizar el proceso de manera manual introduciendo en el campo:

Servidor o dirección de correo electrónico: ds-mdm.movistar.es

ID de grupo: MDM0125841

Cuando el propio agente de inscripción VMware Hub lo requiera, se deberá introducir el usuario y contraseña para continuar la inscripción.

La tarea completa de inscripción puede demorar varios minutos en función de la carga de red de datos, tamaño de aplicaciones a descargar, etc.

En medio de este proceso, requerirá el cifrado del dispositivo, el cual, para ello, debe contar con al menos el 80% de carga de batería y estar conectado el dispositivo al cargador.

ADMINISTRADORES

Se propone la creación de distintas cuentas de administración para todos los interlocutores de cliente que actúen en el entorno MDM.

El rol utilizado será: Telefónica Modelo Gestionado.

Por parte de Telefónica se proporcionará soporte a nivel de los usuarios de control con rol AirWatch Administrator.

Se creará un usuario administrador temporal, con el fin que el integrador pueda acometer tareas de gestión.

Una vez finalizado el proyecto el usuario será eliminado.

CONCLUSIONES

A continuación, se describen los requerimientos necesarios para la ejecución de la configuración, consideraciones, riesgos propios de la configuración propuesta y riesgos generales asociados a generalidades del dispositivo, plataformado, etc. no propios de la configuración y/o gestión desde MDM.

REQUERIMIENTOS A CLIENTE

En el siguiente listado, se describen los requerimientos acordes a la configuración propuesta en este documento.

Requerimientos obligatorios:

1. Se requiere de una conexión (ADSL/FTTH) sin restricciones a internet con el fin de realizar el enrollment de los dispositivos.
   Si por motivos de seguridad no fuera posible, se debe asegurar el encaminamiento de la conectividad a:
   - https://mdm.movistar.es
   - https://ds-mdm.movistar.es
   - https://ap-mdm.movistar.es/api
   - https://cm-mdm.movistar.es:443/awcm

2. Cuenta Gmail o asociada con Google para hacer la integración de Android Enteprise.
   - Se necesita la cuenta de correo electrónico y contraseña, para hacer la integración y publicación de Apps.
     - Usuario: afw.serviciosfunerariosmad@gmail.com
     - Password: Fune2018
3. Cuenta Gmail para realizar enrollment de dispositivos en modo Admin Device (Legacy).

Requerimientos opcionales:

1. Servicio de Office365 con licenciamiento para hacer uso de OneDrive.
   - Cada usuario vinculado al portal MDM deberá de tener una cuenta de servicio O365.

2. Cuenta Gmail para hacer uso de los servicios de Google como Google Drive como requiere el cliente.
    - El cliente ha proporcionado una cuenta genérica de Google:
        - Usuario: informesdeasistencia@gmail.com
        - Contraseña: Informesdeasistencia2019

Estos requerimientos pueden aumentar tras la conclusión, revisión y ejecución del proyecto, pruebas de nuevas configuraciones o cambios de configuración por parte de cliente.

CONSIDERACIONES

Todo lo ejecutado en esta propuesta de configuración, atiende a una configuración ideada a raíz de los requerimientos de cliente, pudiéndose dar el caso de requerimientos adicionales de cliente que no hayan sido contemplado y probados en esta propuesta.

Cabe recordar que el identificador a utilizar en el momento del enrollment para Android Enterprise es el siguiente: **afw#hub**.

Se ha observado que, por las características del dispositivo, el completado de inscripción y configuraciones, requiere dejar márgenes de tiempo de inicio de aplicado de configuraciones, descarga de aplicaciones, etc., por lo que aun cuando se haya concluido la inscripción del dispositivo, hay que dejar el tiempo prudencial necesario para que inicie las acciones de configuración (incluso aunque parezca que no se están haciendo acciones sobre el dispositivo),

Esta misma configuración propuesta, se ha probado con dispositivos de características similares a los proporcionados por el cliente, observándose una inscripción, descarga de aplicaciones y aplicado de configuraciones correctos.

Si durante este proceso de instalación de VMware Hub, por inactividad u otro motivo, el dispositivo requiere la atención de inicio de sesión en la barra de notificaciones (Acción necesaria en cuenta), se deberá abrir de forma manual la App “Hub” para continuar con el proceso de inscripción.

Es muy importante que, a la hora de realizar la inscripción, se cuente con una conexión de red (WIFI/ MOVIL) fiable y sin restricciones, dado que, de lo contrario, pueden existir retrasos en la entrega de configuraciones, descarga de aplicaciones, etc. y con ello demorar el proceso de plataformado.

Para mayor seguridad y control de la información contenida en los buzones de correo sincronizados en los dispositivos se recomienda realizar la integración de la plataforma MDM con la plataforma Office 365, la cual permitirá:

- Restringir el acceso al correo electrónico a solo dispositivos corporativos.
- Mejora en la automatización de la configuración de los ajustes y credenciales de acceso al correo.
- Supervisar la actividad del correo electrónico empresarial.
- Definir las acciones y las pólizas de conformidad para el correo electrónico.
- Bloquear el acceso al correo electrónico basado en marca, modelo o sistema operativo.

Es una integración que no requiere de un despliegue adicional del ya existente.

Se recomienda la integración de la plataforma MDM contra un servicio LDAP propio del cliente para una mayor gestión y securización de los usuarios del portal MDM.

Se ha solicitado que el GPS este permanentemente activado. La plataforma MDM tiene capacidad de localización de dispositivos. La plataforma MDM no es un sistema/servicio de localización, aunque tiene esa capacidad por lo que no se recomienda hacer uso como sistema principal de control. No ofrece una fiabilidad más allá de un 70%.

RIESGOS

Al hacer uso de una cuenta genérica de Google para el uso de Google Drive se incumple con uno de los términos de uso y condiciones de Google LLC

Límites en el acceso a los Dispositivos. Google puede imponer ocasionalmente ciertos límites con respecto al número de aplicaciones de software o de Dispositivos con los que se puede acceder al Contenido (para obtener más información, consulta el enlace de ayuda al Contenido correspondiente en Google Play). Google puede registrar y almacenar los números de identificación únicos de los Dispositivos para aplicar estas restricciones.

Se recomienda hacer cuentas compartidas o utilizar una cuenta “madre” que hace de MASTER y una cuenta de manera individual por cada usuario con permisos a los recursos de la cuenta “madre”

https://support.google.com/a/answer/33330?hl=es

Aunque la operación ofrecida por el cliente es totalmente valida

El cliente ha solicitado cambios en los dispositivos que no pueden ser gestionados por el Servicio MDM Movistar. Es por ello por lo que no pueden automatizarse, al haber una implicación por personas puede existir algún “error humano”.

ANEXO III
Protocolo Puesta en Marcha Tablets

SOLICITAR ESTE ANEXO A LA EMSFCM, S.A. A TRAVES DEL MAIL concursos@sfmadrid.es

ANEXO IV
Fondo de Pantalla

SOLICITAR ESTE ANEXO A LA EMSFCM, S.A. A TRAVES DEL MAIL concursos@sfmadrid.es

ANEXO V
Futura STD.Zip

SOLICITAR ESTE ANEXO A LA EMSFCM, S.A. A TRAVES DEL MAIL concursos@sfmadrid.es