



GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-452)

Seguridad en Windows Mobile 6.5

MAYO 2013

Edita:



© Centro Criptológico Nacional, 2013
NIPO: 002-13-1023-X

Fecha de Edición: Mayo de 2013

Raúl Siles ha participado en la elaboración y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

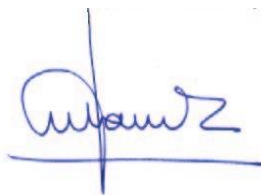
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Mayo de 2013



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1	INTRODUCCIÓN	7
2	OBJETO.....	7
3	ALCANCE.....	8
4	ENTORNO DE APLICACIÓN DE ESTA GUÍA	8
5	CONFIGURACIÓN DE SEGURIDAD DE WINDOWS MOBILE 6.5	11
5.1	ACTUALIZACIÓN DEL SISTEMA OPERATIVO: MICROSOFT	11
5.1.1	PASO A PASO: INSTALACIÓN DE LA ACTUALIZACIÓN DE HORARIO DE VERANO DE MICROSOFT	13
5.2	ACTUALIZACIÓN DEL SISTEMA OPERATIVO: FABRICANTE	15
5.2.1	PASO A PASO: INSTALACIÓN DE LA ACTUALIZACIÓN DEL SISTEMA SMS DE HTC	17
5.3	MICROSOFT ACTIVESYNC	19
5.4	HERRAMIENTAS DE ACCESO AL REGISTRO PARA WINDOWS MOBILE.....	28
5.5	MODELO DE SEGURIDAD DE WINDOWS MOBILE.....	30
5.6	POLÍTICAS DE SEGURIDAD, CONFIGURACIONES DE SEGURIDAD Y ROLES DE SEGURIDAD EN WINDOWS MOBILE	37
5.7	SECURITY CONFIGURATION MANAGER POWERTOY	38
5.8	MODIFICACIÓN LOCAL DE POLÍTICAS DE SEGURIDAD.....	42
5.9	GESTIÓN EMPRESARIAL DE DISPOSITIVOS BASADOS EN WINDOWS MOBILE.....	44
5.9.1	GESTIÓN DE SEGURIDAD DEL HARDWARE DEL DISPOSITIVO MÓVIL.....	45
5.10	ACCESO FÍSICO AL DISPOSITIVO MÓVIL	46
5.10.1	PIN DE LA TARJETA SIM.....	46
5.10.2	PIN O CONTRASEÑA DE ACCESO DEL DISPOSITIVO MÓVIL.....	49
5.10.3	RECUPERACIÓN DE LA CONTRASEÑA DE ACCESO	60
5.11	PANTALLA DE DESBLOQUEO: PREVISUALIZACIÓN DE DATOS	63
5.12	CIFRADO DE DATOS EN WINDOWS MOBILE	64
5.12.1	CIFRADO DEL DISPOSITIVO MÓVIL	64
5.12.2	CIFRADO DE LAS TARJETAS DE ALMACENAMIENTO EXTERNAS	67
5.13	ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL	68
5.14	CONFIGURACIÓN POR DEFECTO DEL DISPOSITIVO MÓVIL	72
5.15	LOCALIZACIÓN GEOGRÁFICA	74
5.15.1	QUICKGPS	76
5.15.2	A-GPS.....	76
5.15.3	SERVICIOS DE LOCALIZACIÓN: GOOGLE Y HTC	77
5.15.4	SERVICIOS DE LOCALIZACIÓN: BING.....	80
5.15.5	INFORMACIÓN GEOGRÁFICA EN FOTOGRAFÍAS	81
5.16	COMUNICACIONES USB.....	82
5.17	COMUNICACIONES BLUETOOTH	83
5.17.1	DESACTIVACIÓN DE LAS COMUNICACIONES BLUETOOTH.....	83
5.17.2	DOS EN EL NOMBRE BLUETOOTH.....	85
5.17.3	DISPOSITIVOS BLUETOOTH EMPAREJADOS.....	88
5.17.4	CONFIGURACIÓN GENERAL DE BLUETOOTH	91
5.17.5	CONFIGURACIÓN AVANZADA DE BLUETOOTH	95
5.17.6	OBEX FILE TRANSFER (Y MECANISMOS DE SEGURIDAD)	96
5.17.7	OBEX OBJECT PUSH	102
5.17.8	MANOS LIBRES BLUETOOTH	104
5.17.9	SAP: SIM ACCESS PROFILE	113
5.17.10	RED DE ÁREA PERSONAL (PAN)	114

5.17.11	OTROS PERFILES BLUETOOTH.....	117
5.17.12	ATAQUES BLUELINE.....	120
5.17.13	DOS EN EL NOMBRE BLUETOOTH.....	121
5.18	COMUNICACIONES WI-FI	122
5.18.1	DESACTIVACIÓN DE LAS COMUNICACIONES WI-FI.....	122
5.18.2	SELECCIÓN DE LA RED DE DATOS EN WINDOWS MOBILE.....	127
5.18.3	ATAQUES BLUELINE	127
5.18.4	DOS EN EL NOMBRE BLUETOOTH.....	128
5.18.5	RECOMENDACIONES DE SEGURIDAD PARA LA CONEXIÓN A REDES WI-FI	130
5.18.6	CONEXIÓN AUTOMÁTICA A REDES WI-FI.....	141
5.18.7	ENRUTADOR WI-FI.....	143
5.19	COMUNICACIONES GSM (2G): MENSAJES DE TEXTO (SMS).....	145
5.19.1	EJECUCIÓN DE CONTENIDO WEB EN MENSAJES DE TEXTO	147
5.20	COMUNICACIONES GSM (2G) Y UMTS (3G): VOZ Y DATOS	152
5.20.1	DESACTIVACIÓN DE LAS COMUNICACIONES DE VOZ Y DATOS 2G/3G	152
5.20.2	CONFIGURACIÓN DE LA RED DE DATOS DE TELEFONÍA MÓVIL.....	158
5.20.3	SELECCIÓN DE LA RED DE DATOS 3G.....	161
5.20.4	RECOMENDACIONES DE SEGURIDAD PARA LA CONEXIÓN A REDES 2G/3G	164
5.21	COMUNICACIONES TCP/IP	168
5.21.1	ADAPTADORES DE RED.....	168
5.21.2	PERFIL DE CONEXIÓN: INTERNET O TRABAJO	169
5.21.2.1	WI-FI: PERFIL DE CONEXIÓN INTERNET O TRABAJO	173
5.21.3	SEGURIDAD EN TCP/IP.....	176
5.21.4	ESCANEADO DE PUERTOS TCP Y UDP.....	177
5.21.5	SSL/TLS	178
5.21.6	IPV6.....	178
5.21.7	VPN.....	180
5.22	COMUNICACIONES EN ENTORNOS DE RED MICROSOFT.....	183
5.23	COPIAS DE SEGURIDAD	185
5.23.1	MICROSOFT MY PHONE.....	185
5.24	SERVICIOS DE NOTIFICACIÓN OPCIONALES	193
5.25	SERVICIOS DE DATOS	195
5.26	GESTIÓN EMPRESARIAL DE SEGURIDAD DE LAS APLICACIONES.....	200
5.27	APLICACIONES CLIENTE	200
5.28	ACTUALIZACIÓN DE APLICACIONES MICROSOFT.....	201
5.28.1	BING	201
5.28.2	OFFICE MOBILE	202
5.28.3	.NET COMPACT FRAMEWORK	203
5.29	NAVEGACIÓN WEB: INTERNET EXPLORER MOBILE	205
5.29.1	PROVEEDOR DE BÚSQUEDAS AUTOMÁTICO	210
5.29.2	IDENTIFICACIÓN DEL NAVEGADOR WEB	210
5.29.3	CONTENIDOS ADOBE FLASH	213
5.29.4	CONTENIDOS ADOBE PDF.....	215
5.29.5	SSL/TLS	215
5.30	CORREO ELECTRÓNICO (E-MAIL).....	218
5.30.1	DIRECT PUSH.....	221
5.31	REDES SOCIALES.....	223
5.31.1	GESTIÓN DE CREDENCIALES DE LAS REDES SOCIALES	224
5.31.2	AUTENTIFICACIÓN Y SEGURIDAD DE LAS COMUNICACIONES DE LAS REDES SOCIALES	226
5.32	APLICACIONES DE TERCEROS: WINDOWS MARKETPLACE FOR MOBILE.....	227
6	APLICACIÓN DE LA GUÍA DE SEGURIDAD CCN-STIC-452	231

7	APÉNDICE A: TABLA DE POLÍTICAS DE SEGURIDAD DE WINDOWS MOBILE	235
8	APÉNDICE B: MYMOBILER.....	250
9	REFERENCIAS	251

1 INTRODUCCIÓN

1. El desarrollo de los dispositivos móviles y de las tecnologías inalámbricas en los últimos años ha revolucionado la forma de trabajar y comunicarse. El uso creciente de estas tecnologías sitúa a los dispositivos móviles como uno de los objetivos principales de las ciberamenazas.
2. La proliferación de dispositivos móviles en los últimos años, junto al aumento de las capacidades, prestaciones y posibilidades de utilización de los mismos, hace necesario evaluar en profundidad la seguridad ofrecida por este tipo de dispositivos, así como de los mecanismos de protección de la información que gestionan, dentro de los entornos de Tecnologías de la Información y las Comunicaciones (TIC).
3. Se considera dispositivo móvil aquél dispositivo de uso personal o profesional de reducido tamaño que permite la gestión de información y el acceso a redes de comunicaciones, tanto de voz como de datos, y que habitualmente dispone de capacidades de telefonía, como por ejemplo teléfonos móviles, *smartphones* (teléfonos móviles avanzados o inteligentes) y agendas electrónicas (PDA), independientemente de si disponen de teclado o pantalla táctil.
4. Pese a que los dispositivos móviles se utilizan para comunicaciones personales y profesionales, privadas y relevantes, y para el almacenamiento de información sensible, el nivel de percepción de la amenaza de seguridad real existente no ha tenido trascendencia en los usuarios finales y las organizaciones.
5. El presente documento realiza un análisis detallado de los mecanismos y la configuración de seguridad recomendados para uno de los principales sistemas operativos de dispositivos móviles utilizados en la actualidad, Microsoft Windows Mobile® 6.5, con el objetivo de reducir su superficie de exposición frente a ataques de seguridad.

2 OBJETO

6. El propósito del presente documento es proporcionar una lista de recomendaciones de seguridad para la configuración de dispositivos móviles basados en Microsoft Windows Mobile® versión 6.5 (en adelante Windows Mobile 6.5), cuyo objetivo es proteger el propio dispositivo móvil, sus comunicaciones y la información y datos que gestiona y almacena.
7. La presente guía proporciona los detalles específicos de aplicación e implementación de las recomendaciones de seguridad generales descritas en la guía principal de esta misma serie, que presenta la información necesaria para la evaluación y análisis de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los dispositivos móviles en la actualidad.
8. La serie CCN-STIC-450, “Seguridad en dispositivos móviles”, se ha estructurado en dos niveles: una guía genérica centrada en el análisis de seguridad en dispositivos móviles (CCN-STIC-450), complementada por guías específicas para los principales sistemas operativos empleados por los dispositivos móviles hoy en día. Por este motivo, antes de la lectura y aplicación de la presente guía, asociada a un sistema operativo (y versión concreta del mismo), se recomienda la lectura de la guía general de seguridad:
 - CCN-STIC-450 - Seguridad en dispositivos móviles

Adicionalmente, se recomienda la lectura de las guías de esta misma serie asociadas a otros sistemas operativos y versiones en caso de ser necesaria su aplicación en otros terminales:

- CCN-STIC-451 - Seguridad en Windows Mobile 6.1
- CCN-STIC-452 - Seguridad en Windows Mobile 6.5
- CCN-STIC-453 - Seguridad en Android 2.x
- CCN-STIC-454 - Seguridad en Symbian

Nota: esta serie de guías están diseñadas considerando como requisito la necesidad de encontrar un equilibrio entre seguridad y funcionalidad en relación a las capacidades disponibles en los dispositivos móviles a proteger, con el objetivo de poder hacer uso de la mayoría de características disponibles en los mismos de forma segura.

3 ALCANCE

9. Las Autoridades responsables de la aplicación de la Política de Seguridad de las TIC (STIC) determinarán su análisis y aplicación a los dispositivos móviles ya existentes o futuros bajo su responsabilidad.

4 ENTORNO DE APLICACIÓN DE ESTA GUÍA

10. Windows Mobile 6.5 es la última versión disponible del sistema operativo de Microsoft para dispositivos móviles, antes de la llegada de Windows Phone 7 (<http://www.windowsphone7.com>) a final del año 2010.
11. Windows Mobile 6.5 es una actualización incremental de la versión 6.1 de Windows Mobile, que a su vez fue una actualización incremental de la versión 6.0, conocida como “Crossbow”. Este sistema operativo fue lanzado originalmente en el año 2000 bajo el nombre Windows CE Pocket PC.
12. Windows Mobile 6.5 fue anunciada por Microsoft en febrero de 2009 y liberada a los fabricantes en mayo de ese mismo año. Como resultado, los primeros dispositivos móviles basados en Windows Mobile 6.5 estuvieron disponibles en el mercado en octubre de 2009.
13. Los contenidos de esta guía aplican a dispositivos móviles basados en Windows Mobile 6.5 en castellano (ESN, SPA o ES - Spanish), y en concreto a la versión *Professional* (para dispositivos con pantalla táctil y con Mobile Office, referenciados como “Pocket PC”), más completa que la versión *Standard* (para dispositivos sin pantalla táctil y sin Mobile Office, referenciados como “Smartphone”) o la versión *Classic* (dispositivos móviles sin funcionalidad de telefonía, como PDAs, también referenciados como “Pocket PC”).
14. La guía ha sido probada y verificada con la versión Windows Mobile 6.5 Professional, CE OS 5.2.21869 (21869.5.0.82), del sistema operativo.

Nota: la información general del dispositivo móvil está disponible bajo la opción “Inicio – Configuración – Acerca del teléfono”, y en concreto, la información de la versión del sistema operativo se encuentra bajo la categoría “Información de software – Versión del SO”.

15. La versión de Microsoft ActiveSync utilizada es la 4.5.0 (Build 5096) sobre Windows XP SP3 en inglés.

Nota: para la elaboración de la guía se ha empleado la versión de Windows XP en inglés en el ordenador utilizado para la sincronización con el dispositivo móvil, con el objetivo de ejemplificar la compatibilidad de idiomas entre el terminal y el ordenador. La simplicidad de las funciones disponibles a través de ActiveSync, pese a utilizarse otro idioma, no debería dificultar la comprensión de la presente guía.

Adicionalmente, otras utilidades de gestión de la seguridad de los dispositivos móviles están únicamente disponibles en inglés, como la herramienta “Security Configuration Manager PowerToy for Windows Mobile” de Microsoft, analizada posteriormente [Ref.- 10].

16. Pese a la confusión asociada a la nomenclatura, Windows Mobile 6.5 está basado en el kernel (núcleo del sistema operativo) Windows CE 5.2, frente al kernel Windows CE 6.0 que será empleado en Windows Phone 7.

17. El hardware sobre el que se ha verificado la presente guía tiene las siguientes características:

- Dispositivo móvil HTC HD2 (T8585):
 - Versión de la radio: 2.07.51.22_2
 - Versión del protocolo: 15.32.50.07U
 - Versión de la ROM: 1.66.76641 ESN – 1.66.412.1 (76641)
 - Fecha de la ROM: 01/12/10
 - Versión Manila: 2.5.19211619.0

Nota: el dispositivo móvil empleado es un terminal libre, es decir, no asociado a ningún operador de telefonía móvil, con el objetivo de analizar las características y valores por defecto de Windows Mobile 6.5 sin verse afectadas por las posibles modificaciones y personalizaciones llevadas a cabo por los operadores de telefonía.

Nota: debe tenerse en cuenta que se pueden presentar diferencias en la apariencia de las capturas de pantallas utilizadas a lo largo de la presente guía y la pantalla de otros dispositivos móviles basados en Windows Mobile 6.5, debido al modelo, fabricante o versión del SO.

Asimismo, algunas de las funcionalidades analizadas son propias del fabricante del dispositivo móvil empleado, HTC, por lo que las recomendaciones de seguridad no aplican a otros dispositivos móviles basados en Windows Mobile 6.5. Se recomienda llevar a cabo un análisis de seguridad similar al mostrado para estas funcionalidades adicionales añadidas por los fabricantes con el objetivo de determinar las recomendaciones a aplicar en dispositivos móviles de otros fabricantes y en sus aplicaciones propietarias.

Nota: Manila 2.5 es la interfaz gráfica de HTC para Windows Mobile 6.5, también denominada TouchFLO3D (sucesor de TouchFLO), diseñada para ofrecer accesos directos a las aplicaciones y mayor funcionalidad y facilidad de uso a través de la pantalla táctil. HTC

Sense es el nuevo interfaz de usuario de HTC basado en (y sucesor de) TouchFLO3D, qué entre otros, introduce una nueva pantalla principal (*Home*) respecto a Windows Mobile 6.5.

18. Las referencias y capacidades de Microsoft Exchange Server, y del componente Exchange ActiveSync (EAS), mencionadas a lo largo de la presente guía se centran principalmente en la versión Microsoft Exchange Server 2007 [Ref.- 34], en adelante referenciado como Microsoft Exchange.

Nota: el Service Pack 1 (SP1) de Microsoft Exchange Server 2007 añade capacidades adicionales para la gestión y configuración de seguridad de dispositivos móviles [Ref.- 36].

19. Se recomienda siempre recabar e inventariar la información de versiones, tanto hardware como software, de los dispositivos móviles a proteger, con el objetivo de disponer de toda la información necesaria a la hora de tomar decisiones relativas a la aplicación de nuevas actualizaciones de seguridad.
20. Debe prestarse especial atención al contrato de telefonía, y en concreto de datos, asociado a la tarjeta SIM (*Subscriber Identity Module*) empleada en el dispositivo móvil Windows Mobile 6.5, ya que la ausencia de capacidades de comunicación de datos puede hacer que el uso del terminal se vuelva casi impracticable, al recibirse constantemente mensajes sobre la ausencia de conectividad (imágenes inferiores): “No se puede conectar – Marcado: Se ha desconectado el módem de respuesta...” y “Advertencia – Hay un problema de conexión al servicio de GPRS en la red local registrada”.



21. Igualmente, debe prestarse especial atención al tipo de dispositivo móvil (marca y modelo) donde se desea aplicar la guía ya que la relación de los elementos descritos o referenciados en la presente guía (interfaz de usuario, aplicaciones, servicios, políticas de

seguridad, etc) puede diferir ligeramente en función de la personalización del sistema operativo realizada por el fabricante del terminal.

22. Antes de aplicar esta guía en un entorno de producción debe confirmarse su adecuación a la organización objetivo, siendo probada previamente en un entorno aislado y controlado donde se puedan realizar las pruebas necesarias y aplicar cambios en la configuración para que se ajusten a los criterios específicos de cada organización.

5 CONFIGURACIÓN DE SEGURIDAD DE WINDOWS MOBILE 6.5

5.1 ACTUALIZACIÓN DEL SISTEMA OPERATIVO: MICROSOFT

23. Windows Mobile 6.5 incorpora numerosas diferencias y mejoras con respecto a versiones anteriores de este sistema operativo [Ref.- 3], como por ejemplo un nuevo interfaz gráfico de usuario (GUI), la nueva pantalla principal o *Home* (denominada *Hoy o Today*), o una nueva versión del navegador web Internet Explorer (IE) Mobile 6.

Nota: la nueva pantalla principal o Home está disponible únicamente en Windows Mobile 6.5 Professional, ya que la versión Windows Mobile 6.5 Standard mantiene la pantalla principal de Windows Mobile 6.1.

24. Microsoft proporciona información sobre las opciones disponibles para la actualización a Windows Mobile 6.5 en diferentes dispositivos móviles en función del fabricante y del operador de telefonía móvil [Ref.- 2].
25. En el caso de disponer de un terminal para el que se dispone de actualización a Windows Mobile 6.5 (por ejemplo desde Windows Mobile 6.1), se recomienda aplicar la actualización sobre el dispositivo móvil con el objetivo de instalar la última versión disponible de este sistema operativo.
26. Desde su publicación, se han liberado dos versiones adicionales de esta plataforma (como evolución hacia Windows Phone 7): Windows Mobile 6.5.1 y 6.5.3 (empleado en dispositivos Sony Ericsson Aspen a comienzo de 2010) [Ref.- 20], añadiendo un interfaz de usuario más amigable, botones basados en iconos (en lugar de texto), una nueva aplicación para gestionar los contactos, soporte para A-GPS (Assisted-GPS o GPS asistido), y mejoras de rendimiento, en IE Mobile 6 y en el sistema de mensajes de texto.
27. La versión Windows Mobile 6.5 (analizada en la presente guía) tiene asociada la numeración 21xxx para las subversiones o *builds*, mientras que Windows Mobile 6.5.1 emplea la numeración 23xxx. Debe tenerse en cuenta que las mencionadas actualizaciones posteriores a la versión 6.5 están disponibles únicamente para ciertas marcas y modelos concretos de dispositivos móviles.
28. Las diferentes versiones del sistema operativo Windows Mobile son proporcionadas como una imagen de la memoria ROM (o firmware) del dispositivo móvil, que debe ser cargada en el terminal, sustituyendo por completo a la versión existente previamente y eliminando todos los datos y configuración del usuario, fijando los valores de configuración de fábrica durante el proceso.
29. Debe tenerse en cuenta que antes de realizar una actualización completa del sistema operativo del dispositivo móvil, si la opción “Cifrar archivos colocados en tarjetas de almacenamiento” está activa (ver apartado “5.12.2. Cifrado de las tarjetas de almacenamiento externas”), es necesario hacer una copia de seguridad (por ejemplo,

empleando ActiveSync o Windows Mobile Device Center) de todos los datos disponibles en la tarjeta de almacenamiento. En caso contrario, no será posible acceder a los datos cifrados almacenados en la tarjeta tras la actualización.

Nota: la opción “Cifrar archivos colocados en tarjetas de almacenamiento” está disponible en el menú “Inicio – Configuración – Seguridad – Cifrado”.

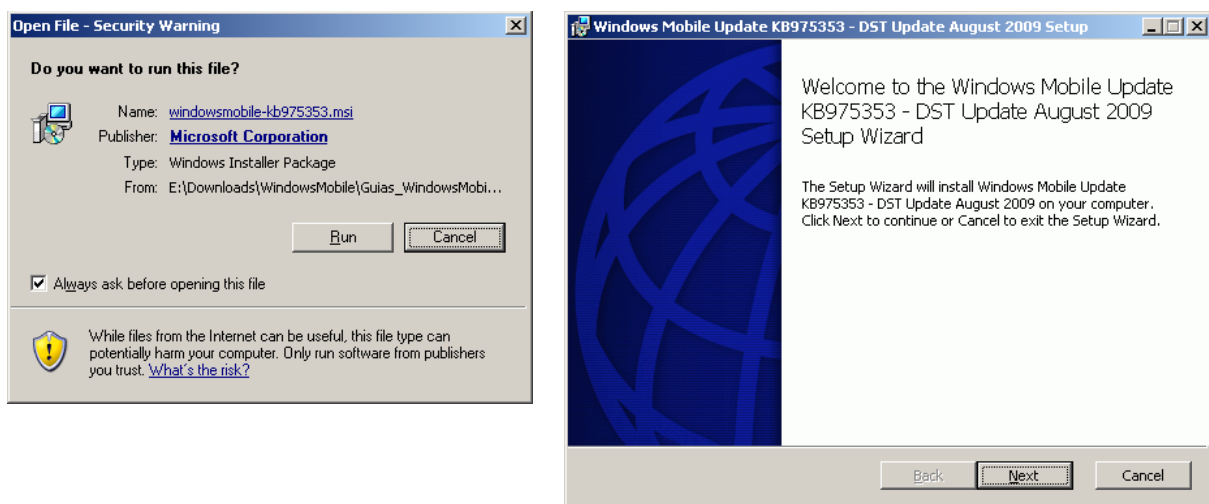
30. Las imágenes de nuevas versiones de la ROM son proporcionadas normalmente por el fabricante del dispositivo móvil (ver apartado “5.2. Actualización del sistema operativo: Fabricante”), y no directamente por Microsoft [Ref.- 2]. En algunos casos, el operador de telefonía móvil al que está asociado el terminal es el que proporciona las nuevas versiones de la ROM del dispositivo móvil. La compañía que proporciona la actualización también facilita las instrucciones para la aplicación de la misma.
31. La versión de la ROM proporcionada por el fabricante del terminal o el operador de telefonía móvil puede variar respecto a la numeración original de las versiones del sistema operativo de Microsoft (ver “versión de la ROM” en el apartado “4. Entorno de aplicación de esta guía”).
32. Pese a que existen foros en Internet dónde se distribuyen imágenes de ROM para múltiples sistemas operativos y fabricantes de terminales (como XDA Developers - <http://forum.xda-developers.com>), desde el punto de vista empresarial, en ningún caso se recomienda la instalación del sistema operativo desde una fuente no oficial.
33. En el mundo Windows Mobile, las actualizaciones individuales adicionales a las actualizaciones de la versión completa del sistema operativo son muy limitadas, en contraposición a las actualizaciones para otros sistemas operativos de Microsoft cliente o servidor, como Windows XP, Vista, 7, 2003, ó 2008. Esta situación afecta tanto a las actualizaciones generales sobre los distintos componentes del sistema operativo, como a las actualizaciones específicas de seguridad.
34. Microsoft publica de forma muy restringida actualizaciones individualizadas para la plataforma Windows Mobile, como por ejemplo la “Actualización de horario de verano” (*Update your Windows phone for Daylight Saving Time*) publicada en agosto de 2009 [Ref.- 23] (ver apartado “5.1.1. Paso a paso: Instalación de la actualización de horario de verano de Microsoft”).
35. Con el objetivo de mantener el dispositivo móvil actualizado, Microsoft recomienda visitar periódicamente desde el propio dispositivo móvil la página de actualizaciones de Windows Mobile, disponible en:
<http://mobile.microsoft.com/windowsmobile/es-es/updates.mspx> (español)
<http://mobile.microsoft.com/windowsmobile/en-us/updates.mspx> (inglés)
36. Finalmente, para la gestión del dispositivo móvil, Microsoft proporciona una aplicación que debe ser instalada en un ordenador y que permite la instalación de software y actualizaciones en el dispositivo móvil, tanto del propio Microsoft, como del fabricante del terminal o de otras compañías.

Nota: la presente guía emplea el término “ordenador” para referenciar al equipo portátil o de sobremesa (o escritorio) empleado para la sincronización y gestión remota del dispositivo móvil.

37. En el caso de ordenadores con Windows XP la aplicación se denomina Microsoft ActiveSync [Ref.- 8] (en adelante ActiveSync, analizada en el apartado “5.3. Microsoft ActiveSync”), mientras que en el caso de ordenadores con Windows Vista y Windows 7 debe emplearse la aplicación denominada Centro de Dispositivos de Windows Mobile (*Windows Mobile Device Center*) [Ref.- 9].
38. Desde el punto de vista de seguridad es necesario actualizar igualmente todas las aplicaciones instaladas sobre el sistema operativo (ver apartado “5.28. Actualización de aplicaciones Microsoft”).

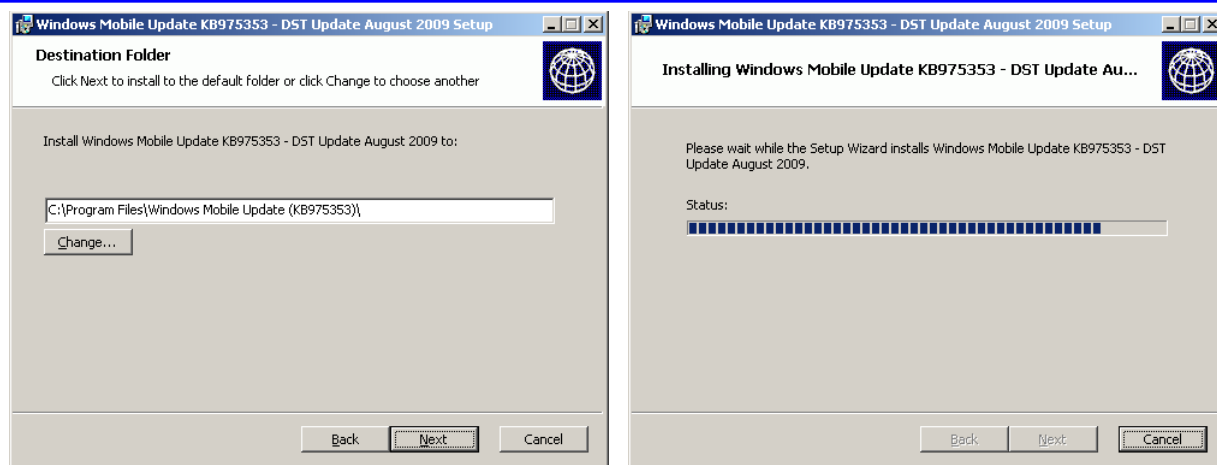
5.1.1 PASO A PASO: INSTALACIÓN DE LA ACTUALIZACIÓN DE HORARIO DE VERANO DE MICROSOFT

39. A continuación se muestra paso a paso el proceso de instalación de la actualización individual del horario de verano para Windows Mobile 6.5 proporcionada por Microsoft en agosto de 2009 [Ref.- 23] con el objeto de ejemplificar el proceso de instalación de actualizaciones individuales de Microsoft en Windows Mobile 6.5.
40. **Paso 1:** conectar el dispositivo móvil al ordenador con ActiveSync (ver apartado “5.3. Microsoft ActiveSync”) para establecer una conexión entre ambos.
41. **Paso 2:** ejecutar en el ordenador el fichero asociado a la actualización de horario de verano, denominado “windowsmobile-kb975353.msi”.

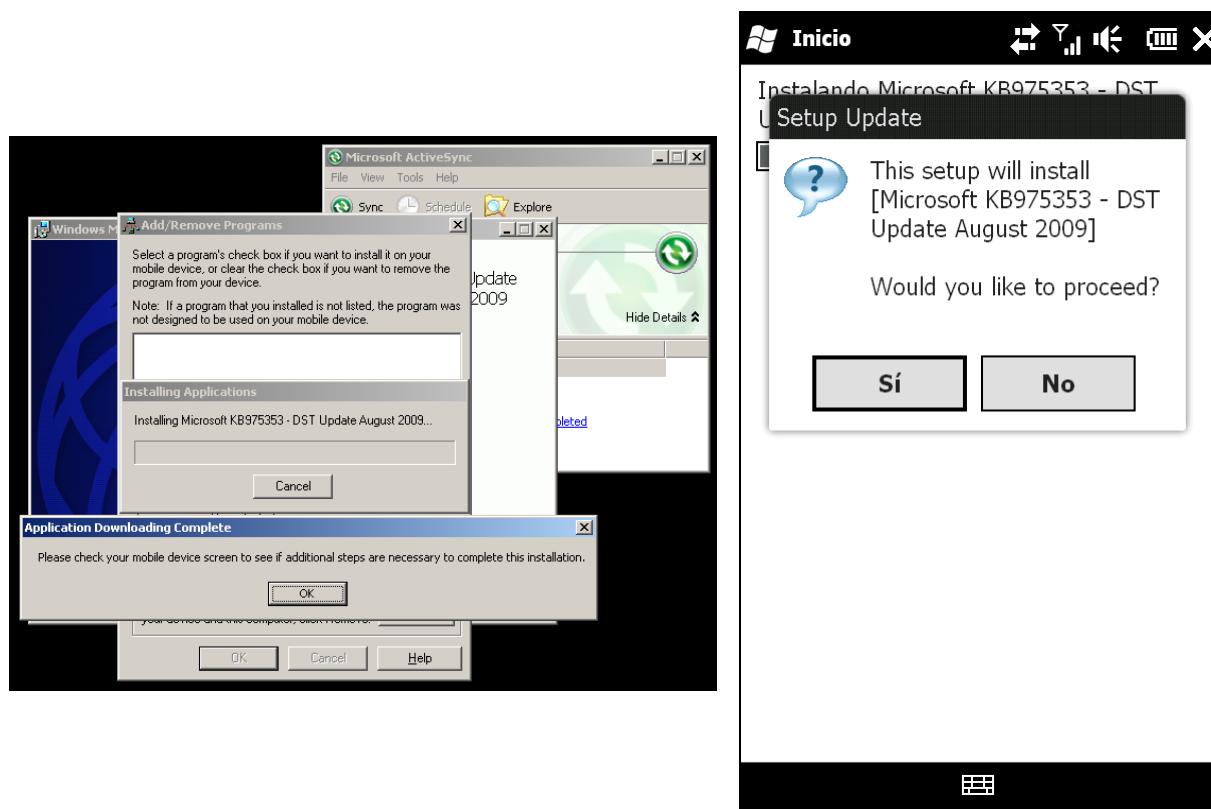


Nota: también existe la posibilidad de descargar la actualización de horario de verano en formato .CAB (en lugar de .MSI) con el objetivo de transferir directamente dicho fichero al dispositivo móvil, por ejemplo vía e-mail o vía web, para su ejecución, sin ser necesario durante el proceso de instalación el uso de un ordenador y ActiveSync.

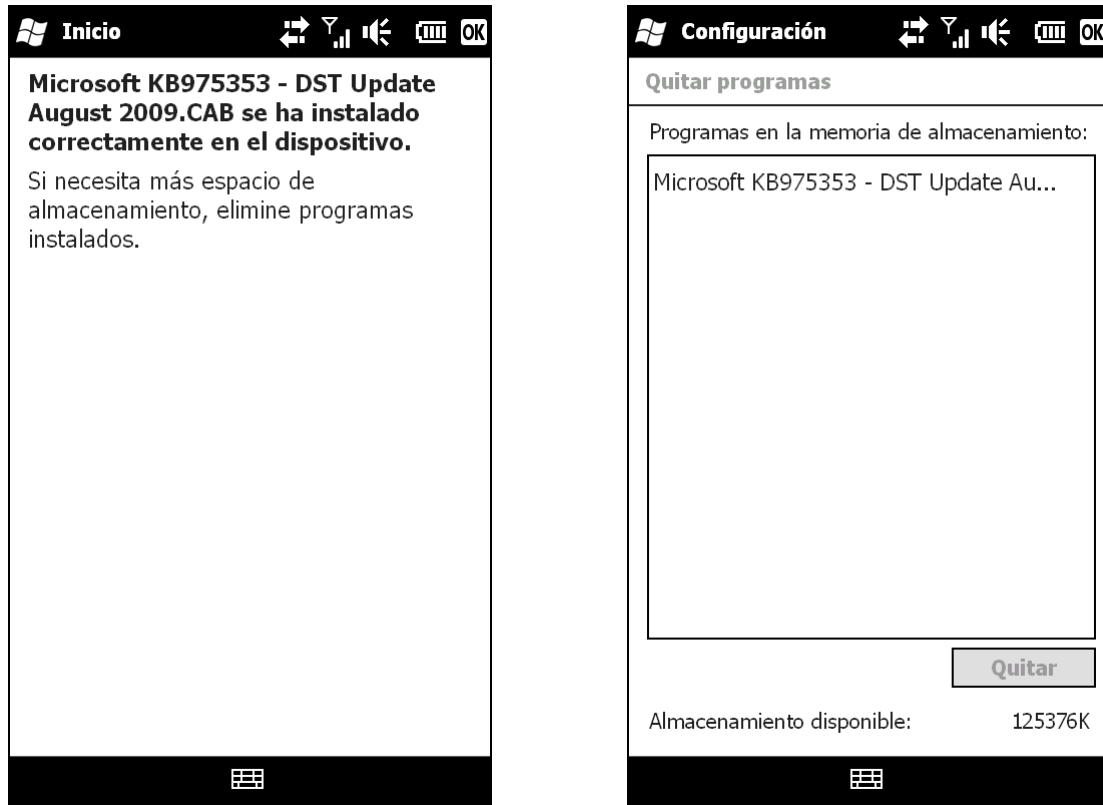
42. **Paso 3:** tras aceptar los términos de licencia de Microsoft, la actualización instalará en el ordenador los componentes necesarios para proceder a realizar la actualización en el dispositivo móvil.



43. **Paso 4:** tras proceder a la instalación, la actualización transfiere automáticamente el fichero .CAB asociado al dispositivo móvil para su ejecución y solicita confirmación al usuario para proceder a su instalación en el dispositivo móvil.



44. **Paso 5:** una vez completada la instalación, la actualización notifica el estado de la misma en la pantalla del dispositivo móvil. Adicionalmente, es posible verificar que la misma ha sido instalada con éxito a través del menú “Inicio – Configuración – Aplicación – Eliminar programas” de Windows Mobile 6.5:



5.2 ACTUALIZACIÓN DEL SISTEMA OPERATIVO: FABRICANTE

45. El fabricante del dispositivo móvil (o el operador de telefonía) puede publicar actualizaciones para el terminal, adicionalmente (o exclusivamente) al fabricante del sistema operativo, Microsoft.
46. El orden de prioridad para la instalación de actualizaciones, especialmente de nuevas versiones de ROM, con el objetivo de preservar toda la funcionalidad del dispositivo móvil es el siguiente: operador de telefonía (terminales no libres), fabricante y Microsoft.
47. El fabricante del dispositivo móvil empleado como referencia en la presente guía, HTC, publica actualizaciones software en su página web de asistencia o soporte [Ref.- 6], en base al modelo de terminal. Debe seleccionarse por tanto el tipo de dispositivo móvil para acceder a todas las actualizaciones disponibles, como por ejemplo HTC HD2 [Ref.- 7].

Nota: debe tenerse en cuenta que existe la posibilidad de que las actualizaciones de la ROM del dispositivo móvil disponibles en la web del fabricante sean más antiguas que la versión instalada por defecto en el dispositivo móvil adquirido.

Por ejemplo, el dispositivo móvil HTC HD2 empleado para la elaboración de la presente guía disponía de las versiones indicadas en el apartado “4. Entorno de aplicación de esta guía”. Sin embargo, las versiones de ROM disponibles en la web de HTC tras su adquisición eran anteriores:

- RUU_Leo_HTC_SPA_1.48.412.2_Radio_Signed_15.28.50.07U_2.05.51.05_2_Ship_HT045NW05170.exe
- RUU_Leo_HTC_SPA_1.66.412.1_Radio_Signed_15.30.50.07U_2.06.51.07_Ship_HT045NW05170.exe

Si se presta especial atención a la numeración de versiones de la actualización más reciente disponible en la web de HTC (lista superior), se confirma que la versión de ROM más reciente es la 1.66.412.1 (la misma que la del dispositivo empleado), pero con una versión de radio y una versión del protocolo inferiores a las suministradas en el dispositivo empleado: 2.06.51.07 frente a 2.07.51.22_2, y 15.30.50.07U frente a 15.32.50.07U, respectivamente.

48. Como norma general, y salvo que exista un motivo que desaconseje su instalación, se recomienda aplicar sobre el dispositivo móvil todas las actualizaciones facilitadas por el fabricante, ya que pese a que las mismas no reflejen explícitamente que se trata de actualizaciones de seguridad, pueden solucionar vulnerabilidades de seguridad públicamente conocidas.
49. Por ejemplo, la siguiente actualización de Java (aunque la descripción de la misma referencia Javascript, un lenguaje de programación completamente distinto a Java) disponible en la web de HTC para el dispositivo móvil empleado, HTC HD2, tiene implicaciones de seguridad sobre la ejecución de aplicaciones en el terminal, aunque el término seguridad no se menciona en ningún momento en la descripción de la actualización (ver apartado “5.19.1. Ejecución de contenido web en mensajes de texto”):

Fecha : 2010-03-25

Categoría : Actualizar

[Descargar](#)

Mensaje emergente de Java en la actualización para HTC HD2

Esta actualización para HTC HD2 evita que los mensajes javascript se abran automáticamente cuando aparece el mensaje de notificación. Esto evita que el teléfono abra aplicaciones no deseadas o molestas.

Fecha : 2010-03-25

Categoría : Actualizar

[Descargar](#)

Actualización ROM para el HTC HD2

Existe una actualización ROM disponible para descargar por los usuarios del HTC HD2. Como siempre, HTC está comprometido

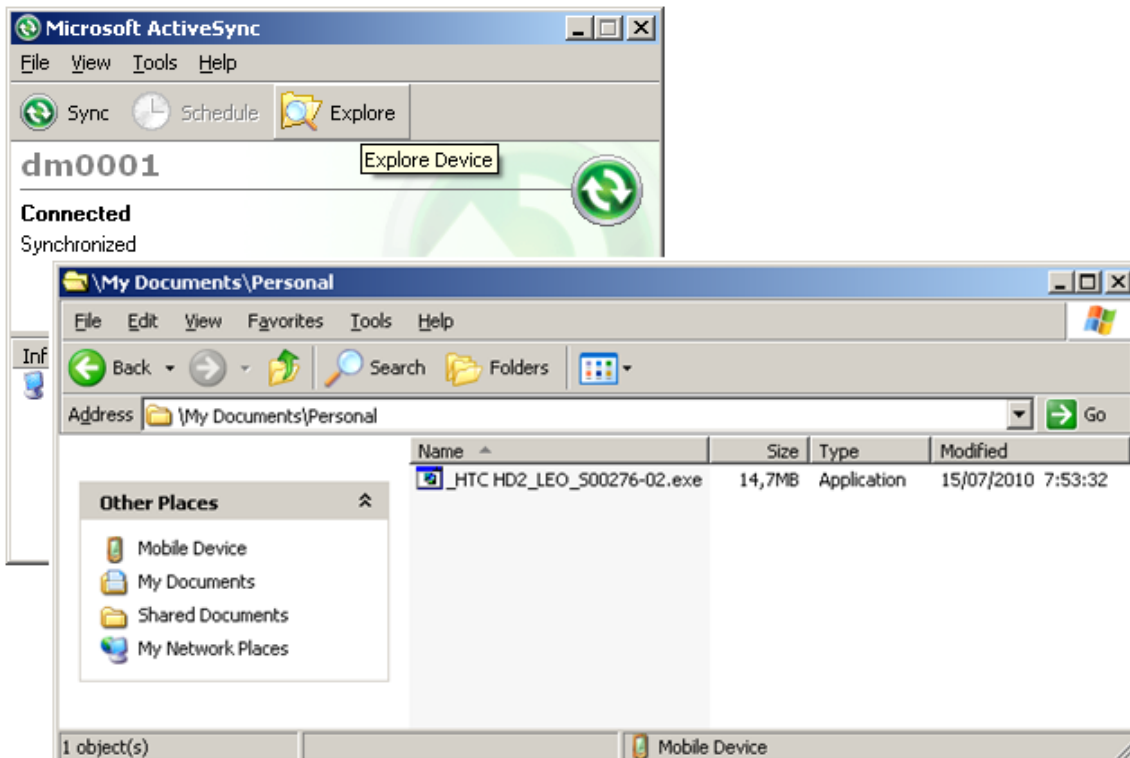
50. Para cada una de las actualizaciones disponibles se recomienda revisar y seguir las instrucciones de instalación del fabricante. En el caso de HTC es necesario instalar cada una de las actualizaciones de forma independiente, no existiendo la posibilidad de instalar todas las actualizaciones disponibles mediante una única operación.
51. El apartado “5.2.1. Paso a paso: Instalación de la actualización del sistema SMS de HTC” muestra paso a paso como llevar a cabo una de las actualizaciones disponibles por parte del fabricante.
52. En el caso de disponer de actualizaciones para la ROM (o firmware) del dispositivo móvil HTC, es necesario indicar el número de serie del terminal para su descarga. HTC verifica si la descarga de la ROM es válida para el dispositivo móvil, permitiendo o no la misma en función de dicha comprobación. Por ejemplo, la actualización a la última ROM disponible en inglés (ver detalles posteriormente) no es válida para un dispositivo móvil con una ROM en español, hecho que es notificado al usuario mediante el mensaje: “*Sorry, this software download is not suitable for your device.*”.
53. El número de serie puede obtenerse a través de la opción “Inicio – Configuración – Acerca del teléfono”, y en concreto, bajo la categoría “Identidad del teléfono – Número de serie”.
54. Adicionalmente, es posible obtener el número de serie del dispositivo móvil retirando la batería del mismo. Tras retirar la batería, se verá una etiqueta blanca con texto dónde se

ubica el número de serie (con el texto “Número de serie: HTxxxxxxxxxxxxxx” o “Número de serie: SZxxxxxxxxxxxxxx” para dispositivos móviles HTC).

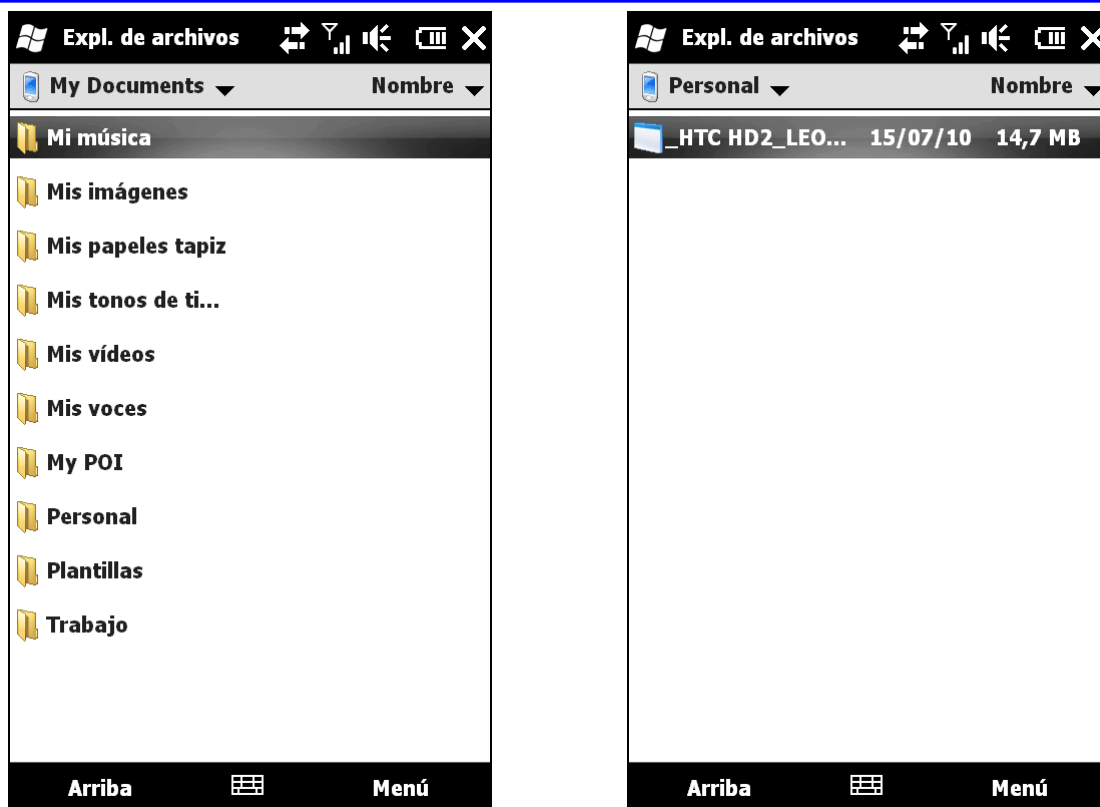
55. Durante la elaboración de la presente guía, HTC, en su página web en inglés, disponía de una nueva actualización de la ROM, concretamente la versión 1.66.707.1 [Ref.- 26]. Sin embargo, la página web de HTC en español [Ref.- 7] reflejaba la ROM versión 1.66.412.1 como última versión disponible.

5.2.1 PASO A PASO: INSTALACIÓN DE LA ACTUALIZACIÓN DEL SISTEMA SMS DE HTC

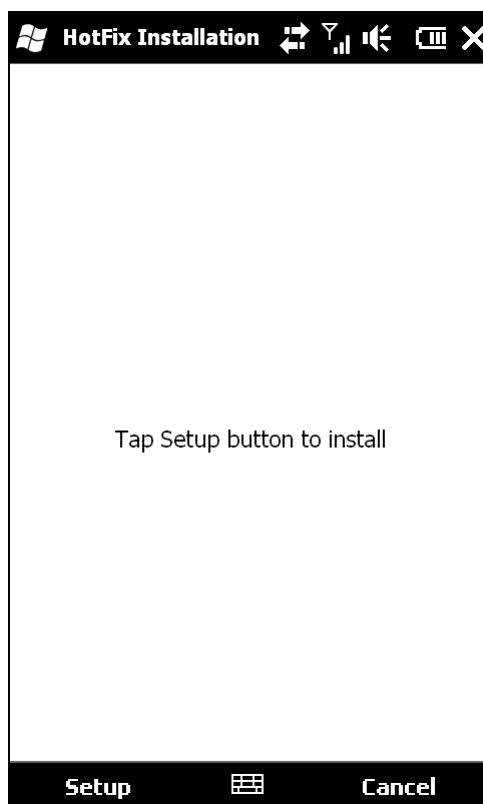
56. A continuación se muestra paso a paso el proceso de instalación de la actualización del sistema de mensajes de texto (SMS) para Windows Mobile 6.5 proporcionada por HTC en julio de 2010 [Ref.- 7] [Ref.- 48] con el objeto de ejemplificar el proceso de instalación de actualizaciones individuales críticas de HTC en Windows Mobile 6.5 (ver los detalles de la vulnerabilidad en el apartado “5.19.1. Ejecución de contenido web en mensajes de texto”).
57. **Paso 1:** conectar el dispositivo móvil al ordenador con ActiveSync (ver apartado “5.3. Microsoft ActiveSync”) para establecer una conexión entre ambos.
58. **Paso 2:** copiar desde el ordenador al dispositivo móvil el fichero asociado a la actualización del sistema SMS, denominado “_HTC HD2_LEO_S00276-02.exe”, por ejemplo, mediante el explorador (botón “Explore”) de ActiveSync, en la carpeta “My Documents\Personal”.



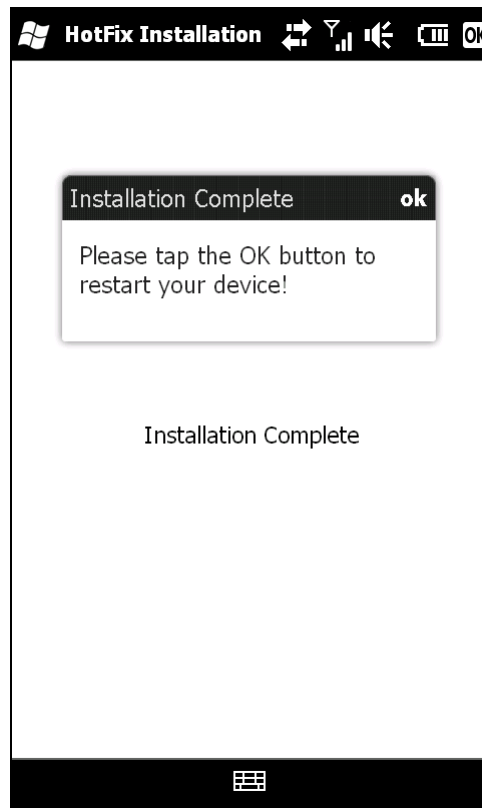
59. **Paso 3:** desde el explorador de Windows Mobile 6.5, disponible en “Inicio – Explorador de archivos”, se debe acceder a la carpeta dónde se ha copiado el fichero y ejecutar la actualización, simplemente seleccionando (o pulsando sobre) el fichero.



60. **Paso 4:** mediante el botón “Setup” es posible proceder a la instalación. Durante el proceso de instalación se solicitará confirmación al usuario para llevar a cabo la misma.



61. **Paso 5:** la actualización de componentes principales de Windows Mobile 6.5, como por ejemplo el sistema de SMS, requiere reiniciar el dispositivo móvil para que sea aplicada completamente.



62. **Paso 6:** una vez completada la actualización, se recomienda eliminar el fichero de instalación con el objetivo de liberar espacio de almacenamiento en el dispositivo móvil. Debe tenerse en cuenta que Windows Mobile no dispone de una papelera de reciclaje para la restauración de ficheros borrados previamente.

5.3 MICROSOFT ACTIVESYNC

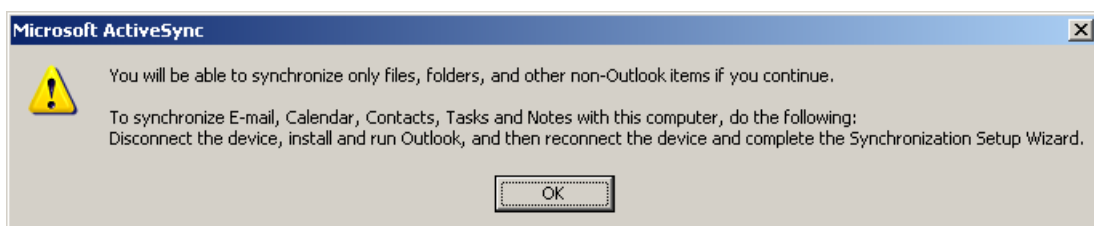
63. Microsoft ActiveSync es una aplicación de escritorio para Windows XP que permite la comunicación y sincronización de ordenadores con dispositivos móviles basados en Windows Mobile.
64. La conexión entre el dispositivo móvil y el ordenador habitualmente se realiza a través de cable USB, aunque es posible emplear conexiones inalámbricas por infrarojos (IrDA) o Bluetooth.
65. Desde el punto de vista de seguridad se recomienda el establecimiento de conexiones ActiveSync mediante USB frente a las conexiones inalámbricas.
66. ActiveSync emplea diferentes canales de transferencia de datos, mediante TCP/IP, para establecer la comunicación entre el dispositivo móvil y el ordenador, por lo que es necesario verificar la configuración del cortafuegos disponible en el ordenador.
67. Concretamente, la instalación de ActiveSync crea las siguientes cuatro entradas por defecto en el cortafuegos de Windows XP, necesarias para permitir el tráfico de entrada a las aplicaciones y procesos de ActiveSync en los puertos TCP especificados (entre paréntesis se detallan los puertos TCP y UDP empleados, y en qué circunstancias):

- ActiveSync Application: WCESMgr.exe (Una vez se ha establecido una conexión mediante ActiveSync, emplea los puertos TCP/999 [1] y TCP/5678 [2]).
- ActiveSync Connection Manager: wcescomm.exe (TCP/5679, puerto principal empleado por ActiveSync para recibir nuevas conexiones, y TCP/7438).
- ActiveSync RAPI Manager: rapimgr.exe (TCP/990 [1] y, una vez se ha establecido una conexión mediante ActiveSync, emplea también el puerto TCP/5721 [2]).
- ActiveSync Service: TCP/26675 [1] (empleado por WCESMgr.exe una vez se ha establecido una conexión mediante ActiveSync).

Notas: los puertos TCP empleados por ActiveSync están asociados a diferentes interfaces de red del ordenador según su tipo. Existen tres categorías:

- Las conexiones marcadas como [1] están vinculadas a todos los interfaces de red del ordenador (0.0.0.0).
- Las conexiones marcadas como [2] están asociadas a una dirección en el rango dinámico 169.254.X.Y/24 (DHCP privado).
- En caso de no indicarse la dirección con número entre corchetes, la conexión sólo se asocia a la dirección IP principal del ordenador o al interfaz de loopback (127.0.0.1).

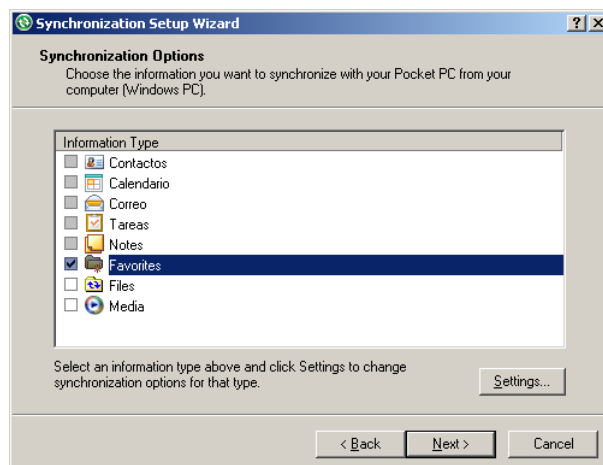
68. La posibilidad de sincronizar correos electrónicos (e-mail), el calendario, los contactos, las tareas y las notas a través de ActiveSync sólo está disponible si se dispone de Microsoft Outlook instalado en el ordenador (no siendo válido Microsoft Outlook Express). En caso contrario, sólo será posible sincronizar ficheros, carpetas y otros elementos no asociados a Microsoft Outlook.
69. Al conectar por primera vez el dispositivo móvil al ordenador dónde ActiveSync está instalado es posible crear un vínculo (o asociación) entre ambos equipos.
70. En el caso de no disponer de Microsoft Outlook instalado en el ordenador, ActiveSync notificará al usuario sobre las limitaciones existentes para la sincronización de correos electrónicos, eventos de calendario, contactos, tareas y notas:



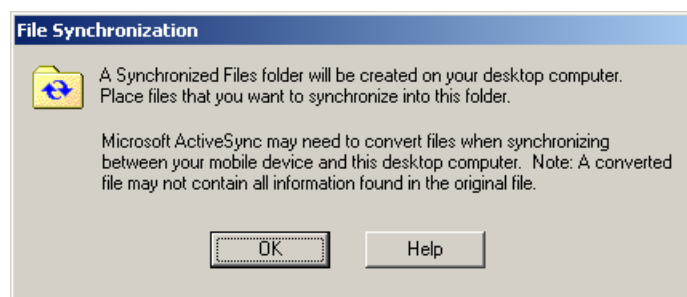
71. El asistente guiará al usuario a través de los pasos necesarios para configurar qué información será sincronizada entre ambos equipos:



72. En el caso de cancelar el establecimiento del vínculo entre ambos equipos, será posible acceder al dispositivo móvil desde el ordenador a través de ActiveSync, pero no se dispondrá de ninguna de las capacidades automáticas de sincronización.
73. En el caso de proceder al establecimiento del vínculo, es necesario definir qué elementos serán sincronizados entre los dos equipos, como por ejemplo la lista de favoritos del navegador web, carpetas y ficheros, y ficheros multimedia (si no se dispone de Microsoft Outlook). La siguiente imagen muestra los elementos sincronizados por defecto:



74. Si se selecciona la posibilidad de sincronizar ficheros, se obtendrá un mensaje que informa sobre la creación de una nueva carpeta en el escritorio del ordenador, “Synchronized Files”. Todos los ficheros depositados en dicha carpeta serán sincronizados automáticamente con el dispositivo móvil:



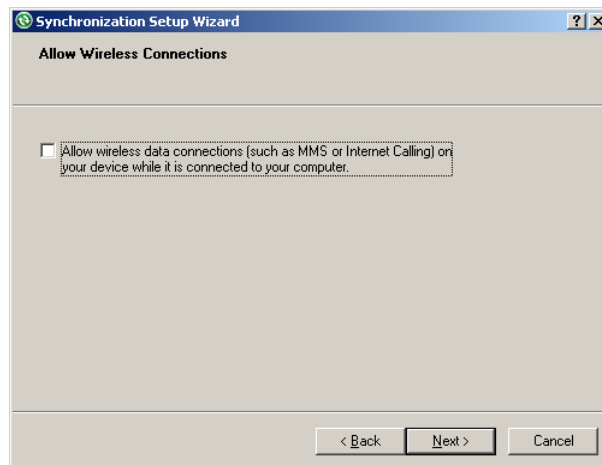
75. La carpeta de sincronización en Windows XP es creada por defecto en “C:\Documents and Settings\<USUARIO>\My Documents\<NOMBRE_TERMINAL> My

Documents\”, junto a un acceso directo en el escritorio del usuario referenciando dicha carpeta.

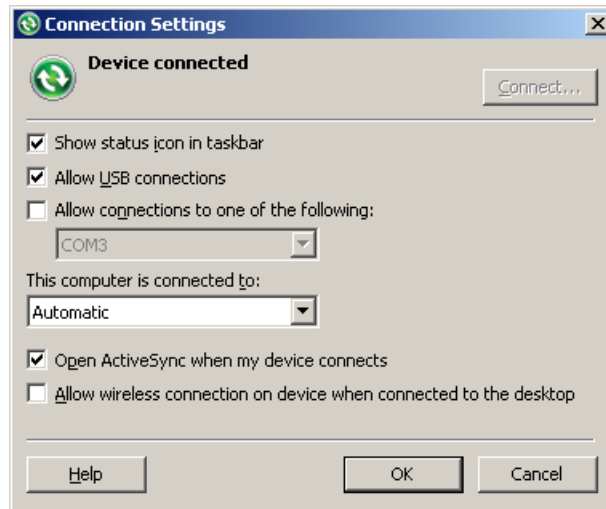
76. Si se selecciona la posibilidad de sincronizar ficheros multimedia (Media), se habilita la posibilidad de sincronizar el dispositivo móvil mediante las capacidades de sincronización de Windows Media Player:



77. Finalmente, debe definirse si es posible hacer uso de algunas de las capacidades de telefonía y comunicaciones de datos del dispositivo móvil, como los mensajes multimedia (MMS) o las conexiones de datos 2G/3G, mientras el terminal está conectado al ordenador a través de ActiveSync:



78. Desde el punto de vista de seguridad, el permitir este tipo de comunicaciones de telefonía móvil mientras el dispositivo móvil está conectado al ordenador podría habilitar la interconexión entre diferentes redes de datos, con los riesgos que ello conlleva. Por ejemplo, podría exponer las redes de datos a las que está conectado el ordenador, y que desde la red del operador de telefonía móvil (2G/3G) se realizasen ataques sobre éstas a través del terminal. Por tanto, se recomienda no habilitar esta opción en ActiveSync.
79. En caso de haber sido habilitada durante la creación del vínculo es posible deshabilitarla posteriormente a través de la opción “Connection Settings – Allow wireless connection on device when connected to the desktop” de ActiveSync, bajo el menú “File”:



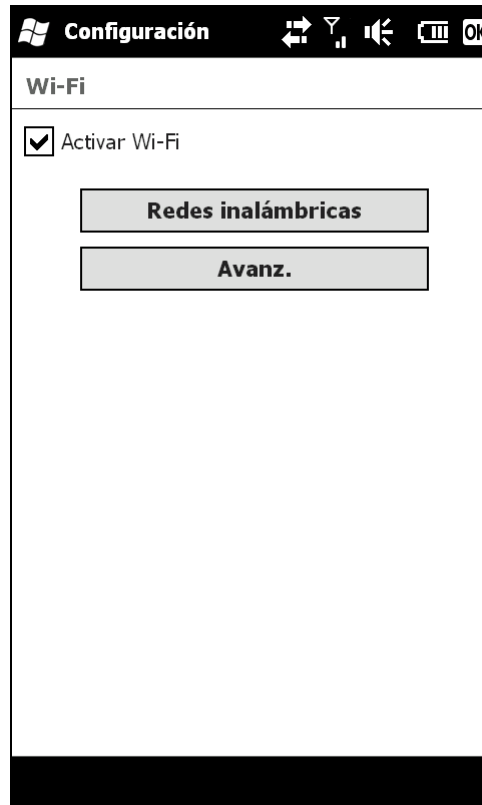
Nota: la desactivación de esta funcionalidad es inmediata, sin embargo, la activación de la misma requiere desconectar y volver a conectar el dispositivo móvil al ordenador.

Pese a que la funcionalidad de esta opción de configuración afecta principalmente a las comunicaciones inalámbricas móviles del dispositivo móvil (2G/3G), también tiene implicaciones sobre las comunicaciones Wi-Fi, tal y como se detalla posteriormente.

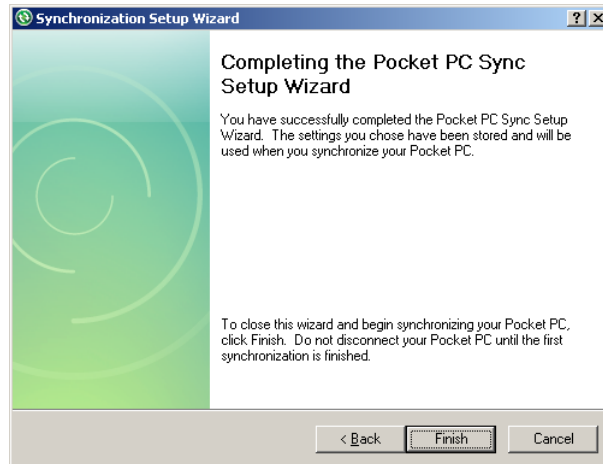
80. Independientemente de si se permiten o no las conexiones inalámbricas de telefonía móvil mientras el dispositivo móvil está conectado al ordenador, ActiveSync (desde la versión 4.0) deshabilita también automáticamente en el “Comm Manager” (de HTC) las conexiones a través de la red Wi-Fi (WLAN), no permitiendo su activación (opción en color gris) desde el “Comm Manager” (menú “Inicio – Configuración – Controles inalámbricos”) del dispositivo móvil. El objetivo de la restricción es similar al de la opción previa, evitar desde el punto de vista de seguridad que la conexión del dispositivo móvil al ordenador permita la interconexión entre diferentes redes de datos, con los riesgos que ello conlleva. Por ejemplo, que desde la red Wi-Fi a la que está conectado el dispositivo móvil se realizasen ataques sobre las redes a las que está conectado el ordenador:



81. Si se disponía de una conexión Wi-Fi activa en el momento de conexión del dispositivo móvil al ordenador con ActiveSync, ésta será interrumpida (se deshabilita el interfaz Wi-Fi).
82. Debe tenerse en cuenta, que pese a que la funcionalidad Wi-Fi está deshabilitada en el “Comm Manager”, es posible habilitar el interfaz Wi-Fi incluso cuando ActiveSync está activo a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Conexiones – Wi-Fi”:



83. Una vez activado el interfaz Wi-Fi, si se establece una conexión inalámbrica con una red Wi-Fi, el interfaz volverá a ser deshabilitado automáticamente por el mecanismo de protección de ActiveSync mencionado. Sin embargo, debe tenerse en cuenta que la conexión llegará a establecerse y por unos segundos el dispositivo móvil dispondrá de conectividad TCP/IP en la red Wi-Fi (respondiendo incluso a paquetes de *ping*, ICMP).
84. En ActiveSync 4.5, si la opción “Allow wireless connection on device when connected to the desktop” (descrita previamente) está seleccionada en la configuración del vínculo de ActiveSync con el dispositivo móvil, será posible hacer uso de la conexión Wi-Fi en el dispositivo móvil, no interrumpiéndose la conexión al conectarse a ActiveSync o pudiendo activarse desde el menú “Conexiones – Wi-Fi” mencionado previamente. Sin embargo, la funcionalidad del interfaz Wi-Fi a través de “Comm Manager” seguirá deshabilitada.
85. En resumen, pese a que por diseño Microsoft deshabilita el interfaz Wi-Fi del dispositivo móvil al conectarse mediante ActiveSync, el usuario puede habilitarlo de nuevo y disponer de ambas conexiones activas simultáneamente.
86. Tras configurar los diferentes elementos asociados al vínculo entre el dispositivo móvil y el ordenador, el asistente confirmará que la asociación ha sido creada con éxito:

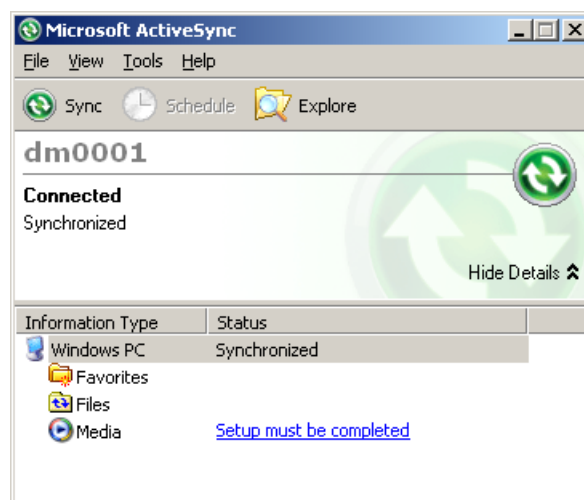


87. Adicionalmente, la conexión del dispositivo móvil a un ordenador con ActiveSync habilita la disponibilidad de conexiones de datos (como por ejemplo, conexión a Internet) desde el terminal a través de ActiveSync (conexión denominada *desktop* o *network pass-through*; DeskTop Pass-Through (DTPT) [Ref.- 55]), empleando para ello la conexión de datos del ordenador (LAN, Wi-Fi, etc). El ordenador actúa por tanto para el dispositivo móvil como pasarela hacia otras redes de datos, en función de su configuración, personalizable desde ActiveSync [Ref.- 78].

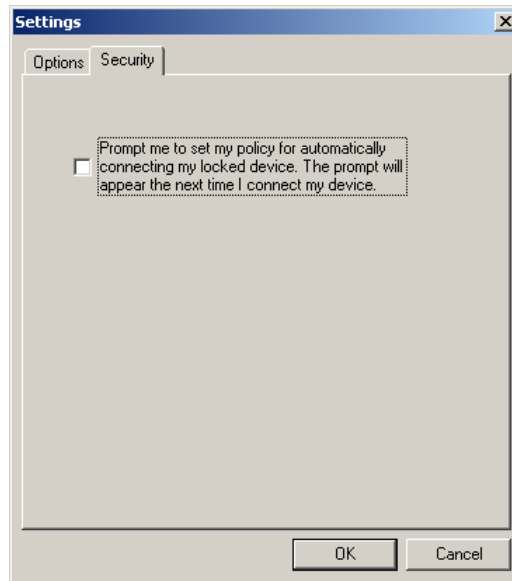
Nota: los parámetros de configuración de DeskTop Pass-Through (DTPT) pueden ser gestionados a través de la siguiente clave del registro de Windows Mobile 6.5, incluyendo las direcciones IP asignadas al dispositivo móvil y al ordenador:

HKEY_LOCAL_MACHINE\Comm\DTPT

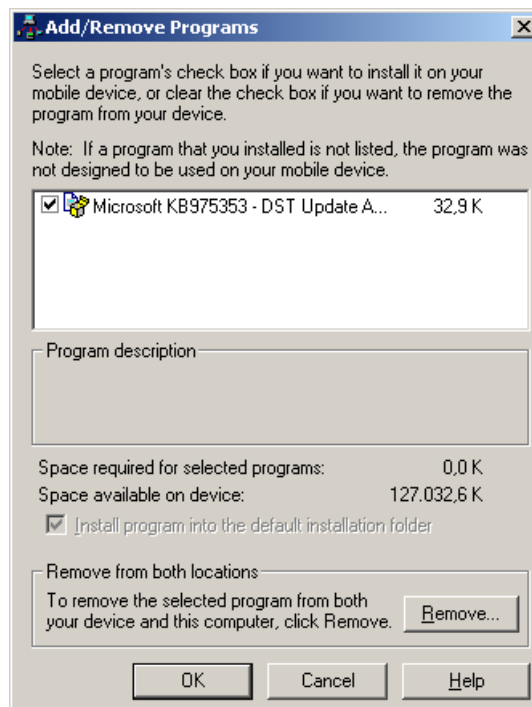
88. Se recomienda que las capacidades de interconexión de múltiples redes, *bridging* o *forwarding*, estén deshabilitadas en el ordenador con ActiveSync, con el objetivo de evitar que desde otras redes a las que está conectado el ordenador se pueda acceder a la red DTPT, y por tanto, al dispositivo móvil.
89. Una vez el dispositivo móvil ha sido vinculado con el ordenador, ambos llevarán a cabo la sincronización y el estado de la conexión en ActiveSync aparecerá como “Connected”.



90. En caso de querer modificar las opciones de sincronización seleccionadas durante la configuración inicial, o aplicadas actualmente, es necesario emplear el menú “Tools – Options...” de ActiveSync.
91. A través del menú “Tools – Options...” y de la pestaña “Security” de ActiveSync, o directamente desde el menú “Tools – Security...”, es posible habilitar (o deshabilitar) que ActiveSync pregunte al usuario la próxima vez que se conecte el terminal si desea que la clave de acceso al dispositivo móvil sea almacenada por ActiveSync, con el objetivo de proceder al desbloqueo automático del terminal en el futuro para realizar las tareas de sincronización (ver apartado “5.10.2. PIN o contraseña de acceso del dispositivo móvil”):



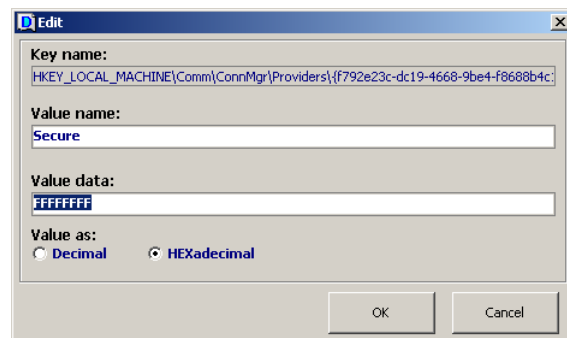
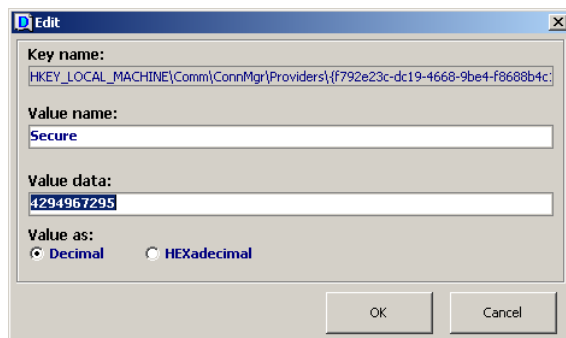
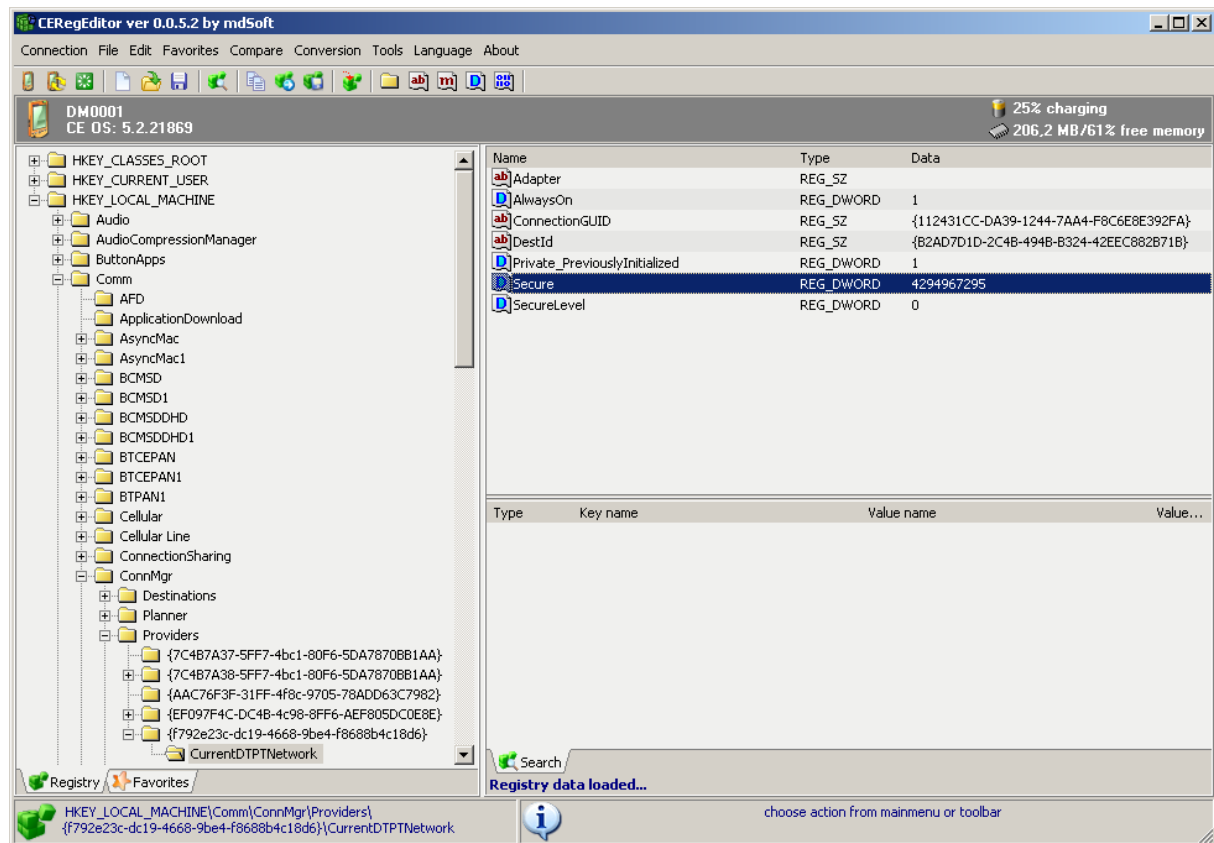
92. Desde el menú “Tools – Add/Remove Programs...” de ActiveSync es posible gestionar el software disponible en el ordenador para el dispositivo móvil y el software instalado en el propio dispositivo móvil:



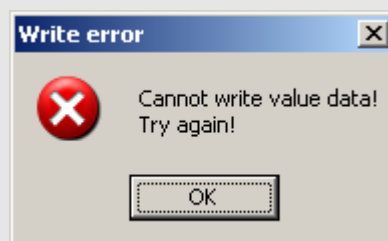
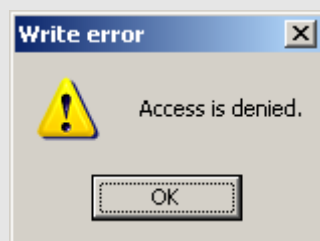
93. Las capacidades de gestión locales de ActiveSync para dispositivos móviles basados en Windows Mobile pueden ser extendidas a través de aplicaciones de terceros, como por ejemplo, MyMobiler (ver apartado “8. Apéndice B: MyMobiler”).

5.4 HERRAMIENTAS DE ACCESO AL REGISTRO PARA WINDOWS MOBILE

94. La presente guía ofrece múltiples referencias a claves del registro de Windows Mobile que permiten llevar a cabo la consulta y modificación de numerosos parámetros de configuración y seguridad internos del sistema operativo.
95. Por defecto, Windows Mobile no dispone de ninguna aplicación que permita al propietario del dispositivo móvil consultar o modificar el registro de Windows Mobile, tal y como ocurre en los sistemas operativos estándar Windows con herramientas como “regedit.exe” o “regedt32.exe”.
96. Existen tres opciones para la modificación del registro en Windows Mobile:
- Herramientas de gestión del registro para Windows Mobile:
Las aplicaciones diseñadas para Windows Mobile permiten la gestión del registro desde el propio dispositivo móvil, como por ejemplo “PHM Registry Editor” [Ref.- 27].
 - Herramientas de gestión del registro desde un ordenador a través de ActiveSync:
Las aplicaciones diseñadas para ordenadores Windows permiten la gestión remota del registro del dispositivo móvil desde el ordenador a través de ActiveSync, como por ejemplo “CeRegEditor” [Ref.- 28] o “Remote Registry Editor” [Ref.- 42], herramienta englobada dentro de Microsoft Visual Studio y del entorno de desarrollo Windows Mobile 6 SDK.
 - Creación y ejecución de un fichero .CAB:
Es posible crear un fichero .CAB (Cabinet) que, al ser ejecutado en el dispositivo móvil, lleve a cabo la modificación de ciertas claves del registro para un propósito o tarea específica. Herramientas, como la mencionada en la categoría anterior (ej. CeRegEditor), facilitan la creación del fichero .CAB a partir de un fichero .REG estándar.
97. La utilización de herramientas que permiten la gestión del registro desde un ordenador a través de ActiveSync es muy conveniente, y por tanto, constituyen la opción recomendada (junto a la utilización de ficheros .CPF para despliegues masivos), ya que se dispone de todas las capacidades de un ordenador estándar para dicha gestión, tanto a nivel de interfaz de usuario (teclado, pantalla, etc), como de capacidades para la realización de copias de seguridad, e importación y exportación de configuraciones:



Nota: En el caso en el que al intentar modificar el registro de Windows Mobile desde una aplicación a través de ActiveSync se obtengan mensajes de acceso denegado (ver siguientes imágenes, correspondientes a la herramienta “CeRegEditor”), es necesario desbloquear la protección de escritura impuesta por el sistema operativo. Por ejemplo, a través de la utilidad del menú “Tools – Unlock registry” de la herramienta “CeRegEditor”, que requiere la ejecución de la aplicación “CERegTools.exe” en el dispositivo móvil, o mediante un fichero XML y “RapiConfig.exe” (ver apartado “5.8. Modificación local de políticas de seguridad”):





El permiso de escritura en el registro por defecto está restringido debido a la política de seguridad de Remote API (RAPI, ID 4097 ó 0x1001), analizada en el apartado “5.8. Modificación local de políticas de seguridad”, y empleada por las herramientas de gestión remota del registro. La aplicación “CERegTools.exe” modifica el valor de esta política al valor “1” en el registro para permitir las operaciones de escritura a través de RAPI.

*** IMPORTANTE ***

Desde el punto de vista de seguridad, y como última acción tras la manipulación del registro de Windows Mobile para la aplicación de las recomendaciones de la presente guía, se recomienda devolver el valor de la clave del registro de la política de seguridad RAPI a su valor por defecto (“2”):

```
[HKEY_LOCAL_MACHINE\Security\Policies\Policies]
"00001001"=dword:00000002
```

En el caso de necesitar modificar el registro posteriormente, será necesario ejecutar “CERegTools.exe” de nuevo o cambiar el valor de la política a “1” a través de un fichero XML y “RapiConfig.exe” (ver apartado “5.8. Modificación local de políticas de seguridad”).

5.5 MODELO DE SEGURIDAD DE WINDOWS MOBILE

98. El modelo de seguridad implementado en dispositivos móviles basados en Windows Mobile se definió en la versión 5.0 [Ref.- 14] y afecta a la seguridad de la configuración del dispositivo móvil, de las aplicaciones que pueden ser ejecutadas sobre éste, y de los accesos remotos a través de RAPI [Ref.- 16].
99. RAPI, Remote API, es la librería que permite la comunicación y la ejecución de acciones entre un ordenador y el dispositivo móvil, empleada por ejemplo por ActiveSync.

100. Desafortunadamente, la plataforma Windows Mobile no fue diseñada con la seguridad en mente desde su concepción, por lo que su modelo de seguridad no es tan avanzado como el de otras plataformas móviles más modernas, y por ejemplo, no dispone de un entorno de ejecución multiusuario.
101. El kernel Windows CE 6.0 que será empleado en Windows Phone 7 presenta una arquitectura más segura, base de futuras versiones de Windows Mobile.
102. El modelo de seguridad, por tanto, emplea una combinación de políticas de seguridad, roles y certificados digitales para gestionar la:
 - Seguridad en la configuración del dispositivo móvil: controla quién dispone de acceso a los parámetros de configuración del dispositivo móvil y el nivel de acceso.
 - Seguridad en la ejecución de aplicaciones: determina si una aplicación puede ser ejecutada y con qué nivel de privilegios.
 - Seguridad en los accesos remotos: controla qué tipo de acciones pueden llevar a cabo las aplicaciones de escritorio en el dispositivo a través de RAPI (o de mensajes OTA, *Over-The-Air*).
103. Adicionalmente a las políticas de seguridad, roles y certificados digitales, Windows Mobile puede emplear métodos adicionales para la protección del dispositivo móvil, como claves del registro adicionales y opciones de administración disponibles en Microsoft Exchange, ambas mencionadas a lo largo de la presente guía.
104. El modelo de seguridad define dos niveles de ejecución o permisos para las aplicaciones: Trusted y Normal. En el nivel “Trusted” la aplicación puede acceder sin limitaciones a todos los recursos del sistema, incluyendo cualquier librería (API), elemento del sistema de ficheros y clave del registro, mientras que en el nivel “Normal” el acceso a ciertas librerías y claves del registro está restringido.
105. Las aplicaciones que ejecutan en modo “Normal”, pese a las restricciones, pueden hacer uso de la funcionalidad estándar del dispositivo móvil, como las capacidades de telefonía de voz, SMS, o acceso a Mobile Office.
106. Las aplicaciones que ejecutan en modo “Trusted” tienen acceso completo al sistema, incluyendo la posibilidad de instalar nuevos certificados digitales o cambiar a modo kernel. La lista concreta de recursos del sistema restringidos, disponibles únicamente en modo “Trusted”, incluye acciones sobre ficheros (por ejemplo en “\Windows\System”), sobre claves del registro (principalmente en la rama HKEY_LOCAL_MACHINE), y acciones asociadas a la gestión de procesos y memoria [Ref.- 17].
107. Las aplicaciones pueden ser clasificadas en tres categorías según como hayan sido firmadas digitalmente (es decir, según su firma Authenticode): privilegiadas, no privilegiadas y no firmadas. Las aplicaciones privilegiadas han sido firmadas con un certificado existente en la *Privileged Certificate Store*, mientras que las no privilegiadas han sido firmadas con un certificado existente en la *Unprivileged Certificate Store*. Por otro lado, las aplicaciones no firmadas no han sido firmadas digitalmente.
108. Authenticode es una tecnología de Microsoft para asociar una firma digital a un fichero, basada en criptografía de clave pública y certificados X.509, para la firma de código. Las aplicaciones pueden por tanto ser firmadas digitalmente a través de las herramientas Authenticode de Microsoft [Ref.- 43].

109. La firma digital (o Authenticode) de la aplicación no evita que la misma contenga vulnerabilidades de seguridad o código malicioso. La firma únicamente permite vincular la aplicación a su desarrollador, asegura su integridad frente a modificaciones, y en algunos escenarios, define el nivel de privilegios de ejecución de la aplicación.
110. La clasificación de los certificados digitales empleados para la firma de aplicaciones en diferentes categorías (o *stores*), privilegiados y no privilegiados, permite definir y utilizar diferentes niveles de acceso para la ejecución de aplicaciones.
111. Los contenedores (o *stores*) para el almacenamiento de certificados digitales en Windows Mobile son [Ref.- 19]: (los dos primeros han sido descritos previamente)
- Privileged Certificate Store
 - Unprivileged Certificate Store
 - Software Publishing Certificate (SPC) Store: certificados empleados para la firma de ficheros .CAB (Cabinet) o .CPF (CAB *Provisioning Format*) que permiten verificar la firma del fichero antes de instalarlo o establecer el role a emplear durante la aplicación de cambios de configuración desde el fichero. Es utilizada principalmente para la instalación en nivel privilegiado (“Trusted”) de una aplicación que ejecutará posteriormente en nivel “Normal”.
 - ROOT (SYSTEM): certificados raíz (o auto-firmados) empleados para autenticación del servidor en conexiones mediante SSL. Sólo pueden ser instalados o modificados con el role MANAGER (al ser de tipo SYSTEM).
 - ROOT (USER): certificados raíz (o auto-firmados) que pueden ser instalados con el role de usuario autenticado (USER_AUTH).
 - CA (SYSTEM): certificados de autoridades certificadoras (CA) intermedias, empleados para establecer cadenas de confianza.
 - CA (USER): certificados de autoridades certificadoras (CA) intermedias, empleados para establecer cadenas de confianza, que pueden ser instalados con el role de usuario autenticado (USER_AUTH).
 - MY (SYSTEM): certificados personales de usuario empleados para autenticación de cliente mediante certificado digital, por ejemplo, en sesiones SSL, autenticación 802.1x, VPN’s, y cifrado y/o firma de correos electrónicos con S/MIME. Sólo pueden ser instalados o modificados con el role MANAGER.
 - MY (USER): certificados personales de usuario empleados para la autenticación de cliente mediante certificado digital.
112. Los contenedores de certificados se encuentran en dos claves del registro:
- HKEY_LOCAL_MACHINE\Comm\Security\SystemCertificates
 - HKEY_CURRENT_USER\Comm\Security\SystemCertificates
113. La primera de ellas en una clave protegida que puede ser accedida por cualquier aplicación (incluyendo las aplicaciones “Normal”), pero sólo puede ser modificada por aplicaciones “Trusted” (reflejada en el nombrado como “SYSTEM”).

114. Las aplicaciones que ejecutan en modo “Normal” no pueden instalar nuevos certificados digitales en los contenedores protegidos (de tipo SYSTEM), sólo pueden instalar nuevos certificados en los contenedores de tipo “USER” (asociados a la segunda clave del registro mencionada: HKEY_CURRENT_USER).

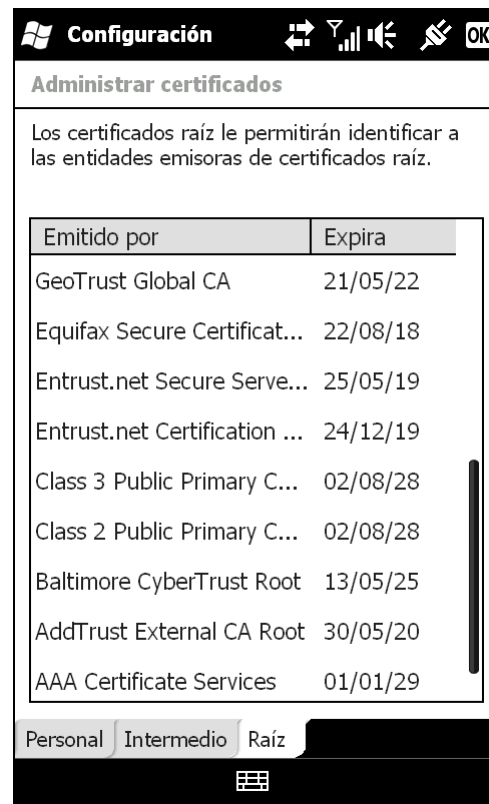
Nota: en numerosas ocasiones los contenedores de certificados son referenciados en la bibliografía y documentación con diferentes nombres, como por ejemplo:

- Privileged Certificate Store, Privileged Execution Trust Authorities Store, etc.
- Unprivileged Certificate Store, Unprivileged Execution Trust Authorities Store, etc.

115. Por defecto, el dispositivo móvil de referencia empleado, basado en Windows Mobile 6.5 Professional, sólo dispone de certificados digitales en tres *stores* (el número total de certificados digitales existentes por defecto en cada *store* está indicado entre paréntesis):

- HKEY_LOCAL_MACHINE\Comm\Security\SystemCertificates\Privileged Execution Trust Authorities (12)
- HKEY_LOCAL_MACHINE\Comm\Security\SystemCertificates\Root (18)
- HKEY_LOCAL_MACHINE\Comm\Security\SystemCertificates\SPC (11)

116. A través del menú “Inicio – Configuración – Seguridad – Certificados”, es posible gestionar los certificados del dispositivo móvil, y en concreto, los certificados personales y de CA’s intermedias (ambos contenedores vacíos por defecto; pestañas “Personal” e “Intermedio”), así como los certificados raíz desde la pestaña “Raíz”:



117. En concreto, la pestaña “Raíz” contiene referencias a los 18 certificados almacenados bajo la clave “HKEY_LOCAL_MACHINE\Comm\Security\SystemCertificates\Root” del registro de Windows Mobile.

118. Los certificados digitales son empleados para la firma de aplicaciones y ficheros ejecutables (.EXE), librerías (DLLs) y ficheros de instalación Cabinet (.CAB).
119. El formato .CAB (Cabinet) es utilizado para la distribución e instalación de aplicaciones (o actualizaciones software) en dispositivo móviles que ejecutan Windows Mobile, pudiendo estar firmados digitalmente.
120. Adicionalmente, los certificados digitales se utilizan para la verificación y cifrado de comunicaciones seguras desde el dispositivo móvil, como sesiones SSL/TLS (Secure Socket Layer/Transport Layer Security), conexiones VPN basadas en IPSec/L2TP o conexiones Wi-Fi mediante PEAP o EAP-TLS.
121. Las implicaciones del uso de certificados digitales en funciones de seguridad críticas requiere que el propietario del dispositivo móvil sea muy cuidadoso a la hora de añadir nuevos certificados digitales al dispositivo móvil, y especialmente, al contenedor de certificados raíz (Root). La instalación de un nuevo certificado digital solo requiere que el usuario seleccione (o pulse) sobre el fichero que lo contiene desde el dispositivo móvil.
122. Existe la posibilidad de añadir nuevos certificados al dispositivo móvil a través de ActiveSync (ver apartado “5.3. Microsoft ActiveSync”), y en concreto a través del menú “Tools – Advanced Tools – Get Device Certificates” y las capacidades de *web enrollment* [Ref.- 75].
123. La relación entre ejecutables y librerías (DLLs) respecto a sus permisos y nivel de ejecución contempla que los procesos que ejecutan en modo “Trusted” no pueden acceder a DLLs con permisos no privilegiados (al estar firmadas con un certificado de la Unprivileged Certificate Store, equivalentes a privilegios de tipo “Normal” durante su ejecución), y por otro lado, los ejecutables pueden cargar DLLs privilegiadas, pero su código ejecutará en modo “Normal” [Ref.- 16].
124. La distribución de aplicaciones en Windows Mobile se puede llevar a cabo mediante ficheros de instalación .CAB, mediante ficheros de instalación desde el ordenador (ej. .EXE ó .MSI), o a través de mensajes SMS.
125. Mediante la revocación de certificados digitales, el operador de telefonía móvil o el propietario del dispositivo móvil, pueden bloquear la ejecución de un grupo de aplicaciones (todas las asociadas a un desarrollador y a su certificado digital) [Ref.- 16].
126. Adicionalmente es posible revocar la ejecución de una aplicación concreta, revocando el *hash* (SHA1) del binario o de un fichero .CAB. En ambos casos se puede emplear la utilidad “revoke.exe” (herramienta disponible dentro del entorno de desarrollo Windows Mobile 6 SDK) para crear el fichero XML con la política de revocación. Este fichero puede ser enviado al dispositivo móvil a través de un mensaje OTA (*Over-The-Air*) o a través de un fichero CPF (*CAB Provisioning Format*).
127. Los dispositivos móviles basados en Windows Mobile pueden ser de dos tipos: **one-tier** o **two-tier**.

Nota: por claridad, la presente guía emplea la nomenclatura “Trusted” y “Normal” (en su acepción inglesa) para definir los niveles de ejecución de una aplicación en Windows Mobile; la nomenclatura **privilegiada, no privilegiada y no firmada** (en su acepción española) para definir el tipo de aplicación en función del certificado empleado para su firma digital; y la nomenclatura **one-tier y two-tier** (en su acepción inglesa) para referenciar los tipos de dispositivos Windows Mobile en función del modelo de seguridad que implementan.

Debe tenerse en cuenta que otra bibliografía y documentación, por ejemplo [Ref.- 16] y [Ref.- 18], referencian los niveles de ejecución como “Privileged” y “Normal”, en lugar de “Trusted” y “Normal”, dada la relación existente entre el nivel de ejecución privilegiado (“Trusted”) y los certificados digitales privilegiados, especialmente en el modelo two-tier.

128. En un dispositivo móvil one-tier sólo existe un nivel o capa de ejecución, por lo que cualquier aplicación ejecuta en modo “Trusted”. Los controles en este entorno se centran en si una aplicación debería ejecutar en función de su firma digital, no disponiéndose de restricciones o permisos de acceso una vez la aplicación es ejecutada.
129. Si la aplicación ha sido firmada con un certificado reconocido por el dispositivo móvil, ésta ejecutará en modo “Trusted” y podrá acceder a todo el sistema. Las aplicaciones ejecutan en dispositivos one-tier empleando el role MANAGER.
130. Si la aplicación no ha sido firmada, o ha sido firmada con un certificado no reconocido por el dispositivo móvil, es necesario realizar comprobaciones adicionales para determinar si se permite su ejecución (incluso consultando al usuario). En el caso de permitirse su ejecución, ejecutará en modo “Trusted”.
131. En un dispositivo móvil two-tier existen dos niveles o capas de ejecución, por lo que las aplicaciones pueden ejecutar en modo “Trusted” o en modo “Normal”. Los controles en este entorno se centran tanto en cómo debería ejecutar una aplicación en función de su firma digital, cómo en los permisos de acceso disponibles.
132. Si la aplicación ha sido firmada con un certificado reconocido por el dispositivo móvil, ésta podrá ser ejecutada, empleándose el certificado para determinar el nivel de privilegios de ejecución. Las aplicaciones que han sido firmadas con un certificado disponible en la Privileged Certificate Store ejecutan en modo “Trusted” y dispondrán de acceso a todo el sistema. Las aplicaciones que han sido firmadas con un certificado disponible en la Unprivileged Certificate Store ejecutan en modo “Normal”, es decir, con restricciones y sin acceso completo a los recursos del sistema, como por ejemplo las librerías (API's) del sistema o claves del registro protegidas.
133. En dispositivos two-tier, las aplicaciones “Trusted” ejecutan empleando el role MANAGER y las aplicaciones “Normal” emplean el role USER_AUTH.
134. Si la aplicación no ha sido firmada, o ha sido firmada con un certificado no reconocido por el dispositivo móvil, es necesario realizar comprobaciones adicionales para determinar si se permite su ejecución (incluso consultando al usuario). En el caso de permitirse su ejecución, ejecutará en modo “Normal”.
135. La siguiente tabla define qué dispositivos móviles soportan el modelo one-tier y two-tier [Ref.- 16], siendo de especial interés las tres últimas plataformas, asociadas a Windows Mobile 6.x:

Plataforma	One-tier	Two-tier
Smartphone for Windows Mobile 2003	Si	Si
Pocket PC for Windows Mobile 2003	No	No
Smartphone for Windows Mobile Version 5.0	Si	Si (defecto)
Pocket PC for Windows Mobile Version 5.0	Si	No
Windows Mobile Professional	Si	No
Windows Mobile Classic	Si	No
Windows Mobile Standard	Si	Si (defecto)

Nota: un dispositivo móvil puede ser convertido de tipo one-tier a two-tier, o viceversa, sólo mediante una reinstalación completa del mismo.

136. Entre las plataformas Windows Mobile actuales, versión 6.x, únicamente la versión *Standard* soporta el modelo two-tier (configuración habilitada por defecto), no siendo una opción disponible en las versiones *Professional* y *Classic*.
137. El modelo two-tier, sólo disponible en la versión *Standard*, viene identificado por la política de seguridad SECPOLICY_PRIVILEGEDAPPS; si su valor es cero, indica que el modelo two-tier está activo y es posible ejecutar aplicaciones sin privilegios (“Normal”) en el dispositivo móvil.
138. En el modelo two-tier, la política de seguridad del dispositivo móvil, almacenada como fichero XML en el mismo, define el nivel de privilegios de cada proceso asignado en el momento de su ejecución.
139. Desde el punto de vista de seguridad, el modelo o dispositivo de dos capas, two-tier, es el más recomendado, ya que permite clasificar y disponer de mayor control sobre las diferentes aplicaciones que pueden ejecutar en el dispositivo móvil. Sin embargo, el modelo two-tier no está disponibles para dispositivos móviles con pantalla táctil, los más avanzados y solicitados por los usuarios actualmente.
140. El concepto de usuario para la ejecución de aplicaciones es inexistente en Windows Mobile, asignándose los permisos de ejecución a cada aplicación individualmente y, principalmente, en función de su firma digital.
141. En resumen, los ficheros con el atributo SYSTEM sólo pueden ser escritos o modificados por procesos ejecutando como “Trusted”, pero todos los ficheros pueden ser leídos por todos los procesos. Igualmente, ciertas claves del registro sólo pueden ser modificadas por procesos ejecutando como “Trusted”, pero el registro al completo puede ser leído por todas las aplicaciones.
142. El programa Mobile2Market (M2M) de Microsoft [Ref.- 13], o Marketplace (ver apartado “5.32. Aplicaciones de terceros: Windows Marketplace for Mobile”), es una plataforma o mercado para la distribución de aplicaciones y software para Windows Mobile.
143. La publicación de una aplicación en el Mobile2Market requiere que la persona o compañía encargada de su desarrollo obtenga la certificación de la misma por parte de Microsoft mediante la firma digital del código con uno de los certificados Mobile2Market.
144. Los dispositivos Windows Mobile pueden disponer de los certificados raíz Mobile2Market asociados a la Privileged Certificate Store y a la Unprivileged Certificate Store, según el tipo de dispositivo (one o two-tier), para la verificación de aplicaciones firmadas con certificados Mobile2Market asignados a desarrolladores.
145. Los dispositivos Windows Mobile 6.x actuales incluyen los certificados Mobile2Market bajo la SPC store (“HKLM\Comm\Security\SystemCertificates\SPC”):
 - Microsoft Mobile Device Privileged Component PCA (Huella digital: 1C9D6E42F467BB135BB1DDBF2624F7ECC3C92DAB).

- Microsoft Mobile Device Unprivileged Component PCA (Huella digital: 1C8229F5C8D6E256BDCB427CC5521EC2F8FF011A).
- Microsoft Mobile Device PCA (Huella digital: 90954D07A0E0CF5206D0729A482D8D9C411459A8).

146. Los desarrolladores pueden utilizar el programa y la certificación Mobile2Market para validar y firmar digitalmente sus aplicaciones con un certificado privilegiado o no privilegiado.

5.6 POLÍTICAS DE SEGURIDAD, CONFIGURACIONES DE SEGURIDAD Y ROLES DE SEGURIDAD EN WINDOWS MOBILE

147. El término política de seguridad en Windows Mobile referencia a un par clave/valor que identifica un parámetro de configuración específico para el dispositivo móvil, como por ejemplo, si las aplicaciones no firmadas digitalmente pueden ser ejecutadas en el dispositivo móvil, ejemplo correspondiente a la política de seguridad identificada por el nombre SECPOLICY_UNSIGNEDAPPS.
148. Las políticas de seguridad vienen identificadas por el nombre de la clave, un valor constante para el que se emplea la siguiente nomenclatura: SECPOLICY_*. Adicionalmente, cada clave puede ser identificada por un número, decimal y/o hexadecimal. Así, la política de seguridad SECPOLICY_UNSIGNEDAPPS corresponde al valor 4102 ó 0x1006.
149. La configuración de la política de seguridad está definida por el valor de la misma, normalmente un valor binario, 0 (falso) o 1 (verdadero), pero no siempre.
150. El conjunto de políticas de seguridad disponibles en Windows Mobile [Ref.- 15] define los parámetros de configuración existentes, su significado, identificador numérico, valor por defecto y valores posibles.

Nota: el Apéndice A (apartado “7”) incluye como referencia la tabla completa en inglés de políticas de seguridad disponibles en Windows Mobile [Ref.- 15].

151. Algunas de las políticas de seguridad más relevantes son:

- ¿Se permite la ejecución de aplicaciones no firmadas, o la instalación de ficheros .CAB no firmados?
- ¿Se solicita confirmación del usuario antes de ejecutar una aplicación no firmada?
- ¿El dispositivo móvil es one-tier o two-tier?
- ¿Qué privilegios tiene una aplicación de escritorio al invocar funciones de la librería RAPI (ActiveSync)?
- ¿Se permite la auto-ejecución (*autorun*) de las aplicaciones disponibles en tarjetas de almacenamiento externas?
- ¿Es obligatorio disponer de una clave de acceso (PIN o contraseña) para usar el dispositivo móvil?
- ¿Puede el usuario modificar la configuración para el cifrado de datos en tarjetas de almacenamiento externas?

- ¿Cuál es el modo Bluetooth empleado por el dispositivo móvil, visible u oculto?
 - ¿Se permite el acceso desde el dispositivo móvil a recursos ubicados en carpetas compartidas de Windows o en servidores SharePoint?
152. Por ejemplo, en dispositivos one-tier, para poder ejecutar una aplicación no firmada se comprueba la política de seguridad que define si se permite la ejecución de este tipo de aplicaciones (SECPOLICY_UNSIGNEDAPPS). En caso afirmativo, se comprueba la política de seguridad que define si se debe consultar al usuario antes de ejecutar la aplicación (SECPOLICY_UNSIGNEDPROMPT).
153. El término “configuración de seguridad” en Windows Mobile es empleado por Microsoft para designar las plantillas de seguridad de los dispositivos móviles, que engloban un conjunto de políticas de seguridad, es decir, un conjunto de parámetros de configuración individuales que afectan a la seguridad del dispositivo móvil, como por ejemplo, si se permite la ejecución de aplicaciones no firmadas digitalmente, o si RAPI está o no deshabilitada.
154. Los roles de seguridad determinan (permiten o deniegan) el nivel de acceso a los recursos del dispositivo móvil en función del origen de un mensaje y del tipo de firma digital asociada al mismo. Adicionalmente los roles son empleados junto a los certificados digitales para establecer las políticas de seguridad del dispositivo móvil.
155. Cada operación en Windows Mobile tiene asociado un role que determina el nivel de acceso disponible en función de quién origina la acción. Los orígenes pueden ser locales, como por ejemplo el interfaz de usuario (UI) y los almacenes de certificados, o remotos, como RAPI, los mensajes de configuración desde Microsoft Exchange o los mensajes WAP.
156. La lista de roles de seguridad definida por Microsoft [Ref.- 21] incluye, entre otros, el role privilegiado (SECROLE_MANAGER), de usuario autenticado (SECROLE_USER_AUTH) y del operador de telefonía móvil (SECROLE_OPERATOR).
157. Los roles aplican, entre otros, a mensajes remotos OTA (*Over-the-Air*) firmados (o no) de configuración y aprovisionamiento enviados mediante WAP por los operadores de telefonía móvil, mensajes de gestión desde Microsoft Exchange o mensajes RAPI. La configuración particular de los roles (aparte de los roles locales estándar MANAGER y USER_AUTH) está asociada principalmente a los operadores de telefonía móvil, ya que afecta fundamentalmente a mensajes de aprovisionamiento de tipo *push* enviados por estos desde su infraestructura. Los roles son empleados para determinar si se acepta un mensaje remoto, y el nivel de acceso al dispositivo que éste tendrá permitido.

5.7 SECURITY CONFIGURATION MANAGER POWERTOY

158. La utilidad “Security Configuration Manager PowerToy for Windows Mobile” [Ref.- 10] es una herramienta, diseñada para ser ejecutada en un ordenador que permite inspeccionar y analizar la configuración de seguridad de un dispositivo móvil basado en Windows Mobile, así como modificar dicha configuración y guardar una copia de la misma [Ref.- 11].

Nota: la página web de Microsoft para la descarga de la utilidad “Security Configuration Manager PowerToy for Windows Mobile” [Ref.- 10] referencia a la herramienta como

“Device Security Manager PowerToy for Windows Mobile 5.0”, aunque ésta es también la herramienta de referencia para Windows Mobile 6 (Versión 1.0.0.0 del año 2006), no existiendo ninguna actualización posterior de dicha herramienta entre las versiones 5.0 y 6.x de Windows Mobile.

159. El modelo de configuraciones de seguridad de Windows Mobile permite la combinación de diferentes parámetros de configuración de seguridad (políticas de seguridad) de forma flexible e independiente. Sin embargo, esta flexibilidad puede dar lugar a la creación de conjuntos de políticas de seguridad incoherentes e inconsistentes. Por este motivo, Microsoft proporciona una lista predefinida de seis configuraciones de seguridad estándar que pueden ser aprovisionadas en dispositivos Windows Mobile [Ref.- 12].

160. Las seis configuraciones de seguridad estándar son:

- Locked:

- Sólo se permite la ejecución de aplicaciones firmadas digitalmente. Únicamente las aplicaciones que han sido firmadas por el fabricante del dispositivo móvil (OEM) o el operador de telefonía móvil, tienen permisos de ejecución, ya que los certificados Mobile2Market han sido eliminados del dispositivo móvil.

- One-Tier Mobile2Market Locked:

- Sólo se permite la ejecución de aplicaciones firmadas digitalmente. Las aplicaciones firmadas digitalmente deben haber sido firmadas por un tercero fiable, como una autoridad certificadora (CA, Certification Authority) reconocida, cuyo certificado está disponible en el dispositivo móvil. Típicamente los dispositivos móviles disponen por defecto de certificados asociados al fabricante (OEM), al operador de telefonía móvil, a autoridades certificadoras (CA's) reconocidas y a Microsoft (Mobile2Market). Las aplicaciones disponen de permisos de ejecución con acceso completo a los recursos del sistema.

- One-Tier Prompt:

- Se consulta al usuario si permite la ejecución de aplicaciones no firmadas digitalmente, permitiendo, en caso afirmativo, su ejecución con acceso completo a los recursos del sistema. Las aplicaciones firmadas son ejecutadas con todos los privilegios sin consultar al usuario.

- Security Off: (configuración de tipo one-tier)

- Permite la ejecución de aplicaciones desde cualquier fuente, así como su ejecución con acceso completo a los recursos del sistema. En ningún caso se solicita confirmación por parte del usuario.

- Two-Tier Mobile2Market Locked:

- Sólo se permite la ejecución de aplicaciones firmadas digitalmente. Las aplicaciones firmadas digitalmente deben haber sido firmadas por un tercero fiable, como una autoridad certificadora (CA, Certification Authority) reconocida, cuyo certificado está disponible

en el dispositivo móvil. Típicamente los dispositivos móviles disponen por defecto de certificados asociados al fabricante (OEM), al operador de telefonía móvil, a autoridades certificadoras (CA's) reconocidas y a Microsoft (Mobile2Market). Las aplicaciones ejecutan con los privilegios otorgados por el certificado con el que han sido firmadas: privilegiado (Trusted) o no privilegiado (Normal). Ver apartado "5.5. Modelo de seguridad de Windows Mobile".

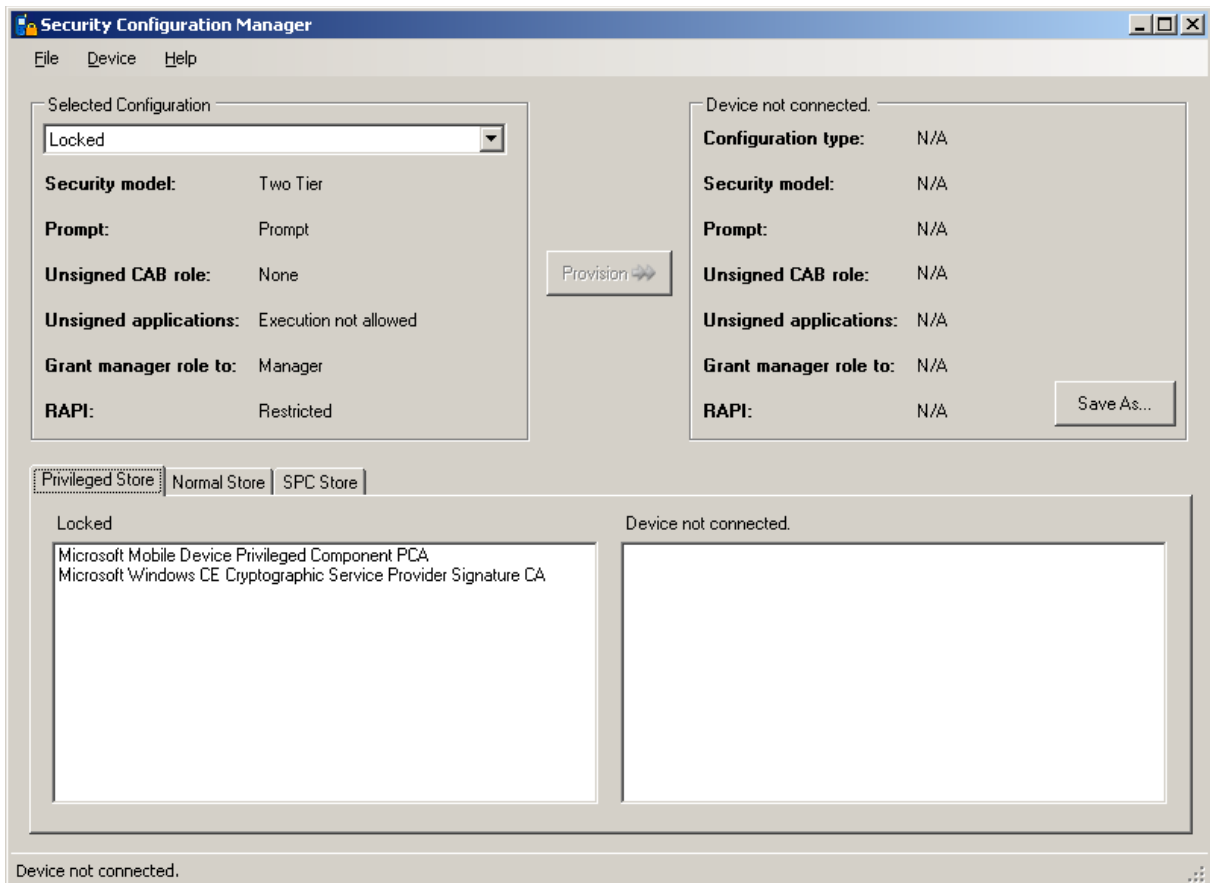
- Two-Tier Prompt:

- Se consulta al usuario si permite la instalación y ejecución de aplicaciones no firmadas digitalmente. En caso afirmativo, la aplicación ejecuta en modo "Normal". Las aplicaciones firmadas digitalmente ejecutan con los privilegios otorgados por el certificado con el que han sido firmadas sin consultar al usuario: privilegiado (Trusted) o no privilegiado (Normal). Ver apartado "5.5. Modelo de seguridad de Windows Mobile". Esta política es muy habitual en dispositivos móviles basados en Windows Mobile 6.x.

161. Desde el punto de vista de seguridad, en ningún caso se recomienda la activación de la configuración de seguridad "Security Off", ya que permite la instalación directa de aplicaciones no fiables en el dispositivo móvil, como por ejemplo, software malicioso (*malware*). Esta configuración es empleada principalmente en entornos de pruebas y no es habitual que los fabricantes y operadores de telefonía móvil incluyan esta configuración en los dispositivos móviles.
162. Las configuraciones de seguridad de tipo "Prompt" dejan en manos del usuario la decisión de si una aplicación debe o no ser instalada, escenario que facilita la realización de ataques de ingeniería social para convencer al usuario de la instalación de una aplicación maliciosa.
163. Cuando el usuario acepta la ejecución de una aplicación, Windows Mobile almacena un hash del binario, con el objetivo de que el usuario no vuelva a ser preguntado cada vez que se quiere ejecutar la misma aplicación.
164. Numerosos fabricantes de software han publicado aplicaciones no firmadas digitalmente para Windows Mobile, por lo que la configuración de seguridad de tipo "Prompt" favorece la utilización y compatibilidad con estas aplicaciones frente a la seguridad del dispositivo móvil.
165. En cualquier caso, en las configuraciones de seguridad de tipo "Prompt", el modelo two-tier es recomendado frente al one-tier ya que las aplicaciones para las que el usuario permite la instalación ejecutan en modo "Normal" (en lugar de "Trusted").
166. Las configuraciones de seguridad "Mobile2Market Locked" son las más recomendadas desde el punto de vista de seguridad, ya que fuerzan a la verificación e identificación del desarrollador de una determinada aplicación, eliminando el anonimato en la distribución de software malicioso. De nuevo, en las configuraciones de seguridad de tipo "Mobile2Market Locked" el modelo two-tier es recomendado frente al one-tier.
167. Finalmente, la configuración "Locked" no permite añadir y ejecutar aplicaciones de terceros, aparte de las seleccionadas por el fabricante u operador de telefonía móvil. Este modelo, poco habitual, es ideal en entornos donde los dispositivos móviles no son empleados como equipos de computación de propósito general, sino que tienen una función específica y no se desea extender sus capacidades. En este caso se limita el uso

del dispositivo móvil como equipo avanzado de comunicaciones personales y profesionales.

168. La herramienta “Security Configuration Manager PowerToy for Windows Mobile” muestra dos secciones en su pantalla principal: a la izquierda se ubica la configuración estándar de seguridad seleccionada, y a la derecha está la configuración de seguridad actual del dispositivo móvil, una vez éste ha sido conectado. Por otro lado, la parte superior ofrece los detalles de las políticas de seguridad, mientras que la inferior describe la información de los certificados digitales disponibles, y en concreto de tres *stores*: Privileged Certificate, Unprivileged Certificate y SPC.



169. El desplegable “Selected Configuration” de la izquierda permite seleccionar una de las seis configuraciones de seguridad estándar proporcionadas por Microsoft, y descritas previamente, facilitando sus detalles de configuración y sus certificados digitales asociados.
170. Los ficheros XML que contienen las configuraciones de seguridad estándar están disponibles en el directorio de instalación de la herramienta, y concretamente en Windows XP bajo “C:\Program Files\Microsoft\Security Configuration Manager\StandardConfigurations”.
171. Adicionalmente, la utilidad “Security Configuration Manager PowerToy for Windows Mobile” permite llevar a cabo tareas relacionadas con la gestión de los certificados digitales almacenados en el dispositivo móvil, como por ejemplo visualizar los certificados existentes, añadir un nuevo certificado de desarrollo para la instalación y

realización de pruebas de nuevas aplicaciones, firmar un fichero (o aplicación) con un certificado de desarrollo, o verificar la firma digital de un fichero (o aplicación).

172. Desde el punto de vista de seguridad, y no de desarrollo, esta última funcionalidad es muy útil a la hora de verificar la firma digital (o Authenticode), es decir, la autenticidad, de un fichero o aplicación para Windows Mobile antes de ser instalado en el dispositivo móvil.
173. Una firma digital correcta confirma que el contenido del fichero o aplicación no ha sido manipulado y/o modificado, y permite verificar quién es el autor de la aplicación.
174. A través del menú “File – Check file signature...” es posible seleccionar un fichero .EXE, .CAB o .CPF y visualizar la información del certificado digital utilizado para firmar el fichero o aplicación, así como los detalles de autenticación y permisos tanto para la configuración de seguridad estándar seleccionada actualmente en la herramienta, como para el dispositivo móvil actualmente conectado.

Nota: se han identificado escenarios donde la utilidad “Security Configuration Manager PowerToy for Windows Mobile”, ejecutando en Windows XP, no es capaz de detectar la existencia de dispositivos móviles basados en Windows Mobile 6.1 y 6.5. El mensaje que se obtiene en la utilidad es: "Querying device configuration".

En ese caso, es necesario obtener la funcionalidad proporcionada por esta utilidad a través de otras utilidades no gráficas, es decir, utilidades de línea de comandos como por ejemplo la utilidad *Desktop Configuration* (RapiConfig.exe; ver siguiente apartado).

5.8 MODIFICACIÓN LOCAL DE POLÍTICAS DE SEGURIDAD

175. Windows Mobile permite la creación y aplicación de políticas de seguridad manualmente en el dispositivo móvil desde un ordenador a través de ficheros XML (ficheros de aprovisionamiento) y la utilidad *Desktop Configuration* (RapiConfig.exe) [Ref.- 68], disponible en el directorio “Tools” del kit de desarrollo (SDK) de Windows Mobile (Professional y Standard), o en su defecto, en la “Microsoft Exchange Server ActiveSync Certificate-Based Authentication Tool” [Ref.- 72].
176. Este método local es similar al empleado por los operadores de telefonía móvil u organizaciones para aprovisionar dispositivos móviles con infraestructuras OTA (*Over-the-Air*) y WAP *push* - aprovisionamiento de clientes OMA, *Open Mobile Alliance* [Ref.- 70] -, y constituye una opción a considerar para organizaciones que deben preconfigurar múltiples dispositivos móviles y no disponen de infraestructura empresariales OTA.

Nota: los detalles de implementación y configuración para el aprovisionamiento de dispositivos móviles a través de OTA y WAP *push* están fuera del alcance de la presente guía. Más información en [Ref.- 70] y [Ref.- 104].

177. El fichero XML de aprovisionamiento puede ser usado tanto para modificar la configuración del dispositivo móvil, como para consultar parámetros de la configuración actual (paso recomendado antes de su modificación).

Nota: la modificación de las políticas de seguridad a través de este mecanismo puede requerir asignar previamente privilegios de manager al role de usuario autenticado [Ref.- 71], para la recepción de mensajes de Remote API (RAPI, 4097) que requieren privilegios de manager (valor de máscara 16).

178. Por ejemplo, el siguiente fichero permite consultar el estado actual de ciertas políticas de seguridad, en concreto, el acceso a RAPI (4097), la instalación de ficheros .CAB no firmados digitalmente (4101) y la ejecución de aplicaciones no firmadas digitalmente (4102):

```
<wap-provisioningdoc>
  <characteristic type="SecurityPolicy">
    <parm-query name="4097"/>
    <parm-query name="4101"/>
    <parm-query name="4102"/>
  </characteristic>
</wap-provisioningdoc>
```

179. Tras ejecutar el comando “RapiConfig.exe /P /M fichero.xml” la configuración actual de las políticas estará disponible en el fichero “RapiConfigOut.xml”:

```
<wap-provisioningdoc>
  <characteristic type="SecurityPolicy">
    <parm name="4097" value="1" datatype="integer" rw-access="3"/>
    <parm name="4101" value="16" datatype="integer" rw-access="3"/>
    <parm name="4102" value="1" datatype="integer" rw-access="3"/>
  </characteristic>
</wap-provisioningdoc>
```

180. Por ejemplo, el siguiente fichero permite modificar ciertas políticas de seguridad, en concreto, se permite acceso restringido a RAPI (4097 = “2”) [Ref.- 69], no se permite la instalación de ficheros .CAB no firmados digitalmente (4101 = “0”) y no se permite la ejecución de aplicaciones no firmadas digitalmente (4102 = “0”):

```
<wap-provisioningdoc>
  <characteristic type="SecurityPolicy">
    <parm name="4097" value="2"/>
    <parm name="4101" value="0"/>
    <parm name="4102" value="0"/>
  </characteristic>
</wap-provisioningdoc>
```

181. Tras ejecutar el comando “RapiConfig.exe /P /M fichero.xml” las políticas serán aplicadas en el dispositivo móvil, y el resultado es almacenado de nuevo en el fichero de salida “RapiConfigOut.xml”.

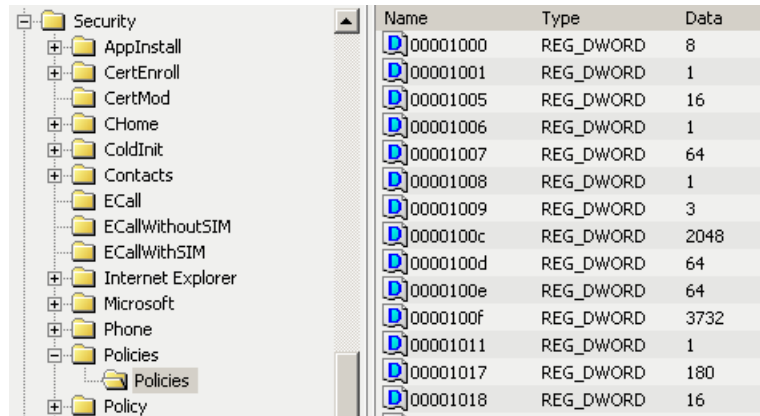
182. Mediante este método es posible provisionar una configuración de seguridad completa desde línea de comandos, como por ejemplo las configuraciones de seguridad estándar proporcionadas por la herramienta “Security Configuration Manager” en forma de ficheros XML (ver apartado “5.7. Security Configuration Manager PowerToy”).

183. Adicionalmente, las políticas de seguridad se verán reflejadas en el registro de Windows Mobile 6.5, tal como muestra el apartado “5.13. Eliminación de datos del dispositivo móvil” para la política “Password Required Policy” (4131). Es por tanto equivalente aprovisionar el valor de una política de seguridad a través de un fichero XML con RAPI que modificar la clave del registro asociada a la política de seguridad.

184. El identificador de política tiene un identificador numérico en decimal, por ejemplo 4097, que en hexadecimal corresponde a 0x1001. El valor hexadecimal es empleado para

identificar el nombre de la clave del registro, "00001001", dentro de la clave de las políticas de seguridad:

```
[HKEY_LOCAL_MACHINE\Security\Policies\Policies]
"00001001"=dword:00000002
```



Name	Type	Data
00001000	REG_DWORD	8
00001001	REG_DWORD	1
00001005	REG_DWORD	16
00001006	REG_DWORD	1
00001007	REG_DWORD	64
00001008	REG_DWORD	1
00001009	REG_DWORD	3
0000100c	REG_DWORD	2048
0000100d	REG_DWORD	64
0000100e	REG_DWORD	64
0000100f	REG_DWORD	3732
00001011	REG_DWORD	1
00001017	REG_DWORD	180
00001018	REG_DWORD	16

5.9 GESTIÓN EMPRESARIAL DE DISPOSITIVOS BASADOS EN WINDOWS MOBILE

185. La gestión de la configuración o aprovisionamiento de los dispositivos móviles se puede realizar directamente a través de ficheros XML, o mediante ficheros CPF (.CAB *Provisioning Format*), ficheros Cabinet especiales que contienen el fichero XML de aprovisionamiento, y que pueden ser distribuidos con infraestructuras OTA (*Over-the-Air*) o desde un ordenador local.
186. Microsoft ofrece principalmente dos métodos o herramientas a nivel empresarial para la gestión de los dispositivos móviles basados en Windows Mobile: Microsoft Exchange [Ref.- 39] (con Exchange ActiveSync) y Microsoft System Center Mobile Device Manager (SCMDM) [Ref.- 38], en sus diferentes versiones.
187. Como se analizará posteriormente a lo largo de la presente guía, las políticas de seguridad de Microsoft Exchange para dispositivos móviles (Exchange ActiveSync Mailbox Policy) permiten configurar diferentes parámetros de seguridad [Ref.- 79].
188. Asimismo, Microsoft Exchange posibilita la aplicación de diferentes políticas de seguridad a distintos usuarios (*mailboxes*) o grupos de usuarios, en función de su role (usuario, *manager*, etc) o departamento (dirección, contabilidad, ventas, etc) [Ref.- 80].
189. Las capacidades de Microsoft Exchange permiten a los administradores gestionar y configurar de forma centralizada los dispositivos móviles de la organización. Adicionalmente, a través de OWA (*Outlook Web Access*) se ofrecen capacidades de auto-gestión a los usuarios, pudiendo éstos llevar a cabo ciertas acciones de gestión y configuración sobre su dispositivo móvil sin necesidad de recurrir al administrador.
190. Las comunicaciones entre los dispositivos móviles y Exchange ActiveSync y OWA se realizan a través de conexiones HTTP sin cifrar (por defecto), aunque existe la posibilidad de cifrarlas mediante SSL/TLS [Ref.- 82].
191. La autenticación entre los dispositivos móviles y Exchange ActiveSync y OWA puede llevarse a cabo mediante autenticación HTTP "Basic" o empleando certificados digitales cliente [Ref.- 81].

192. Se recomienda emplear SSL/TLS para el cifrado de todas las comunicaciones entre el dispositivo móvil y Exchange ActiveSync [Ref.- 72], y emplear como mecanismo de autenticación para el acceso a Exchange ActiveSync certificados digitales cliente [Ref.- 72], para lo que es necesario importar un certificado digital personal (normalmente en formato PKCS12 o mediante *web enrollment*) en el dispositivo móvil (al igual que para la conexión a redes Wi-Fi basadas en EAP-TLS, o redes VPN basadas en IPSec/L2TP y certificados) [Ref.- 75].

Nota: los detalles de implementación y configuración de Microsoft Exchange o SCMDM para la gestión de dispositivos móviles basados en Windows Mobile están fuera del alcance de la presente guía. Sin embargo, a lo largo de la guía, en los diferentes apartados, se ofrecen recomendaciones de seguridad asociadas a la funcionalidad principal proporcionada por estas plataformas para incrementar la seguridad de los dispositivos móviles.

5.9.1 GESTIÓN DE SEGURIDAD DEL HARDWARE DEL DISPOSITIVO MÓVIL

193. Las soluciones de gestión empresarial de dispositivos móviles basados en Windows Mobile permiten definir políticas de disponibilidad de los diferentes elementos hardware del dispositivo móvil, como por ejemplo bloquear el acceso a tarjetas de almacenamiento, a la cámara o a las capacidades de comunicaciones.
194. Su configuración es posible a través de Microsoft Exchange (y en concreto de la Exchange Management Console), mediante múltiples opciones disponibles en la pestaña “Device” de la política de seguridad [Ref.- 34] [Ref.- 37]:
- *Allow removable storage*: permitir el uso de tarjetas de almacenamiento externas desde el dispositivo móvil.
 - *Allow camera*: permitir el uso de la cámara.
 - *Allow Wi-Fi*: permitir el uso de las capacidades de comunicación inalámbricas basadas en Wi-Fi, como por ejemplo, conectarse a una red Wi-Fi para disponer de acceso a Internet.
 - *Allow infrared*: permitir al dispositivo móvil conectar con otros dispositivos mediante infrarojos.
 - *Allow Internet sharing from the device*: permitir a otro ordenador el uso del dispositivo móvil como módem de conexión a Internet.
 - *Allow remote desktop from the device*: permitir el establecimiento de conexiones de escritorio remoto desde el dispositivo móvil hacia otros ordenadores o servidores.
 - *Allow synchronization from a desktop*: permitir al dispositivo móvil sincronizarse con un ordenador a través de ActiveSync o Windows Mobile Device Center.
 - *Allow Bluetooth (Disable, Handsfree Only, Allow)*: En el caso de Bluetooth, los administradores pueden definir si el usuario puede hacer uso de todas las capacidades de Bluetooth del dispositivo móvil (Allow), de ninguna (Disable) o conectar únicamente a dispositivos manos libres Bluetooth (Handsfree Only).

195. Las propiedades de la pestaña “Device” de la política de seguridad de Microsoft Exchange para dispositivos móviles constituyen capacidades avanzadas de configuración de Exchange ActiveSync, por lo que sólo están disponibles si se dispone de la licencia Exchange Enterprise Client Access License (CAL).

5.10 ACCESO FÍSICO AL DISPOSITIVO MÓVIL

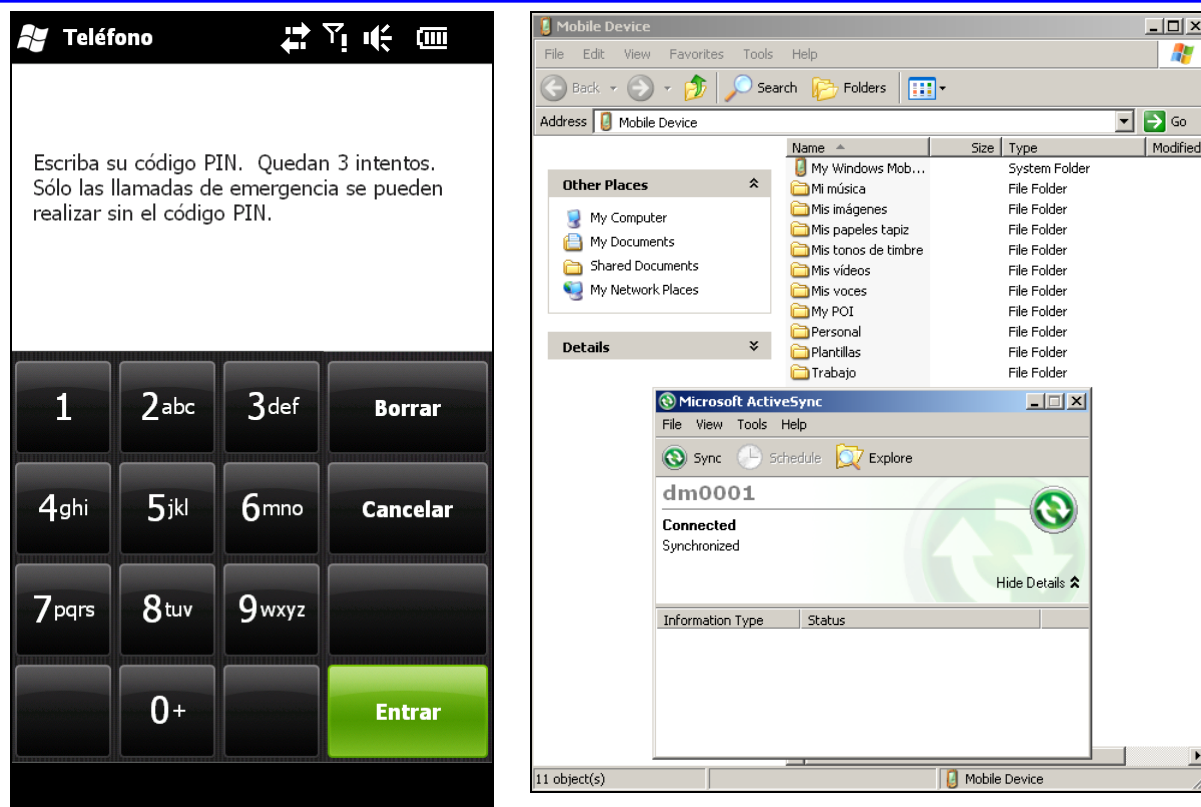
196. La posibilidad de disponer de acceso físico al dispositivo móvil permitiría a un potencial atacante acceder a los contenidos del mismo o hacer uso de los servicios de telefonía móvil disponibles.
197. Para evitar ambos tipos de acceso es posible fijar un PIN (Personal Identification Number) o clave de acceso tanto en la tarjeta SIM como en el propio dispositivo móvil.

Nota: independientemente de la protección del dispositivo móvil, es posible evitar que las aplicaciones que hacen uso del gestor de credenciales (*Credential Manager*) almacenen contraseñas en el dispositivo móvil mediante la siguiente clave del registro [Ref.- 59]:

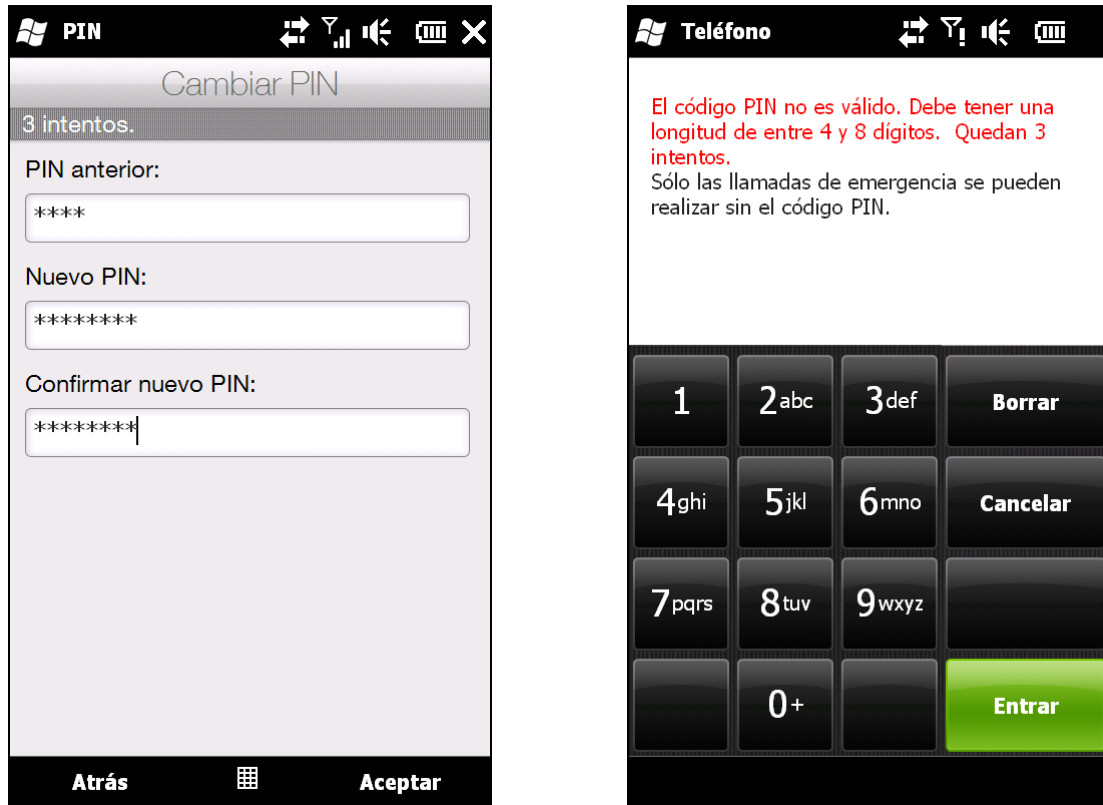
```
HKEY_LOCAL_MACHINE\Comm\Security  
"DisallowSavedNetworkPasswords"=dword:00000001
```

5.10.1 PIN DE LA TARJETA SIM

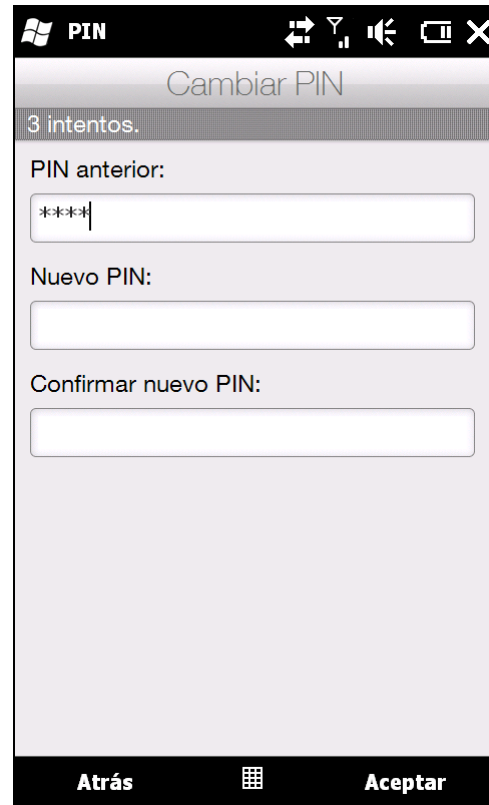
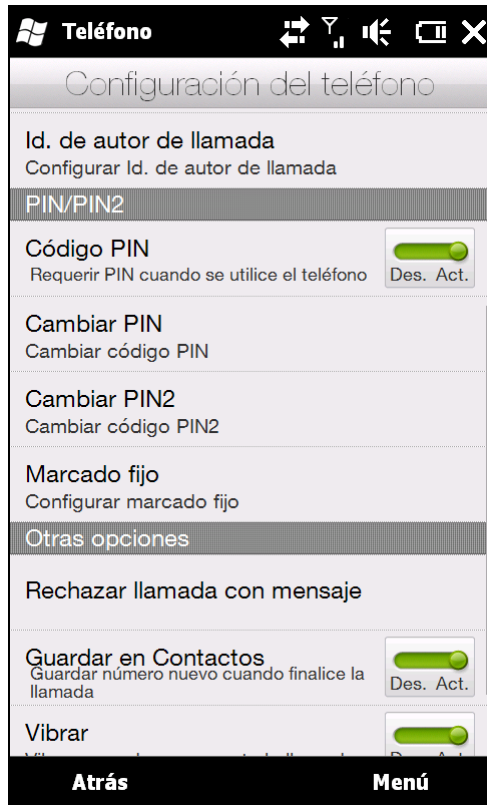
198. El PIN de la tarjeta SIM bloquea el acceso no autorizado a los servicios y capacidades de telefonía móvil asociados a la propia tarjeta SIM. Si la tarjeta SIM está bloqueada (se desconoce el código PIN), únicamente se permite la realización de llamadas de emergencia (112).
199. Sin embargo, si sólo se establece el PIN en la tarjeta SIM y no en el dispositivo móvil (ver apartado “5.10.2. PIN o contraseña de acceso del dispositivo móvil”), aún es posible para un potencial atacante acceder al terminal, incluyendo sus datos y aplicaciones, ya sea directamente (botón “Cancelar”) o, por ejemplo, a través de ActiveSync:



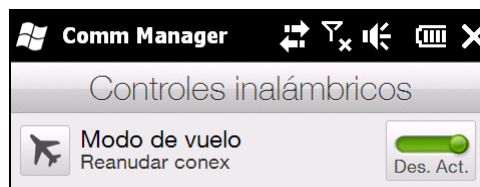
200. La disponibilidad de un PIN por defecto asociado a la tarjeta SIM depende del operador de telefonía móvil, siendo muy habitual que las tarjetas SIM tengan fijado un valor por defecto que es proporcionado en la documentación del operador de telefonía móvil facilitada al usuario al contratar sus servicios.
201. El estándar de la industria en la actualidad define un código de 4 dígitos (0-9) como PIN o clave de acceso para proteger la tarjeta SIM, sin embargo se recomienda hacer uso de un PIN de mayor longitud, en concreto, de 8 dígitos.
202. Windows Mobile 6.5 permite emplear un PIN con un valor de 4 a 8 dígitos:



203. Pese a la debilidad de un PIN de 4 dígitos frente a ataques de adivinación o fuerza bruta, los operadores de telefonía móvil y fabricantes de dispositivos móviles implementan otros mecanismos para evitar este tipo de ataques, como el bloqueo de la tarjeta SIM tras tres intentos de acceso fallidos. En ese caso, para poder desbloquear la tarjeta SIM es necesario emplear una segunda clave de acceso denominada PUK (PIN Unlock Key).
204. Los dispositivos móviles Windows Mobile 6.5 permiten forzar la utilización de un PIN para la tarjeta SIM, así como fijar o modificar el PIN (y PIN2) asociados a la tarjeta SIM a través del menú “Inicio – Configuración – Controles inalámbricos – Teléfono – PIN/PIN2 – Cambiar PIN“. El PIN2 es un segundo PIN asociado a la tarjeta SIM y fijado sólo por algunos operadores de telefonía móvil para proteger ciertos servicios de red, como llamadas a números restringidos.

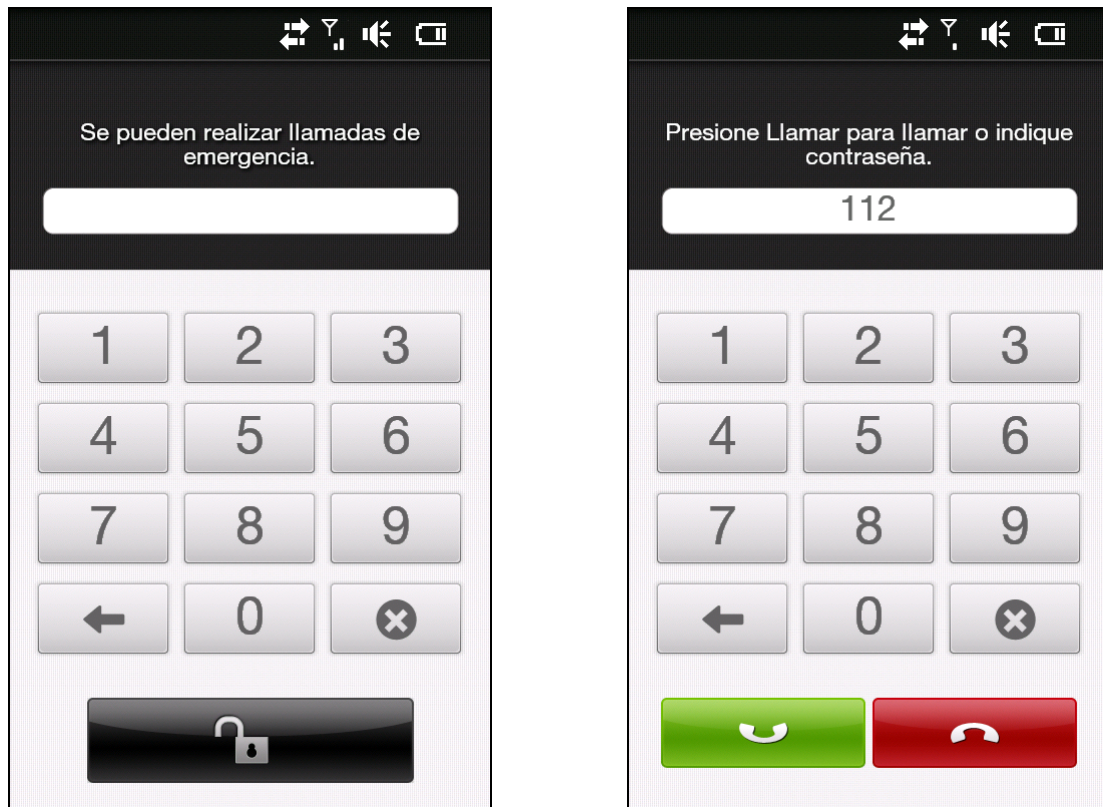


205. Se recomienda por tanto modificar el valor por defecto del PIN y fijar el PIN de la tarjeta SIM empleando un valor o secuencia de números que no sea fácilmente adivinable, es decir, excluyendo valores típicos como 0000, 1111 ó 1234.
206. Debe tenerse en cuenta que cada vez que el dispositivo móvil sale del “Modo de vuelo” (este modo es desactivado), solicitará el PIN de la tarjeta SIM al usuario al activar de nuevo los servicios de telefonía móvil:



5.10.2 PIN O CONTRASEÑA DE ACCESO DEL DISPOSITIVO MÓVIL

207. El PIN del dispositivo móvil bloquea el acceso no autorizado al terminal, incluyendo sus datos, capacidades de comunicación y aplicaciones.
208. Una vez el dispositivo móvil está bloqueado, únicamente se permite la realización de llamadas de emergencia (112) sin el código PIN del terminal. Para ello es necesario marcar el número de teléfono de emergencias en el campo de entrada del PIN.



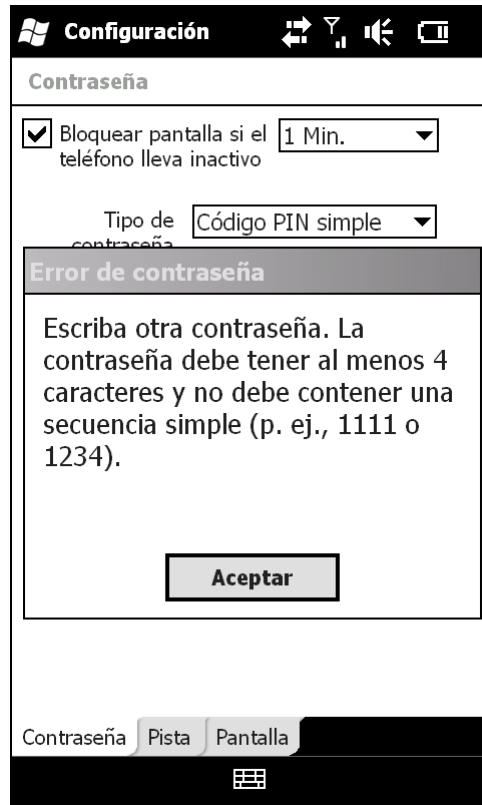
209. Sin embargo, si únicamente se establece el PIN en el dispositivo móvil y no en la tarjeta SIM (ver apartado “5.10.1. PIN de la tarjeta SIM”), aún es posible para un potencial atacante acceder al terminal, extraer la tarjeta SIM y hacer uso de la misma en otro terminal, incluidos sus servicios y capacidades de telefonía móvil asociados.
210. Por defecto, los dispositivos móviles basados en Windows Mobile 6.5 no disponen de un PIN o clave de acceso para bloquear accesos no autorizados al terminal.
211. Se recomienda por tanto establecer el PIN de acceso al dispositivo móvil a través del menú “Inicio – Configuración – Seguridad – Bloqueo del Teléfono”.
212. Windows Mobile 6.5 permite establecer dos tipos de clave de acceso. El PIN más tradicional o simple (opción “Código PIN simple”), compuesto por cuatro dígitos (0-9), o una contraseña (opción “Contras. segura alfanumérica”), compuesta por caracteres alfanuméricos (incluyendo símbolos de puntuación), y por tanto, opción más segura y recomendada:



213. El tamaño máximo de la contraseña alfanumérica en Windows Mobile 6.5 es de 40 caracteres.
214. El tipo de clave de acceso a emplear, PIN o contraseña, está especificado por la siguiente clave del registro, cuyos valores pueden ser “0” (contraseña alfanumérica), “1” (PIN) ó “2” (sin restricción – ambas alternativas son posibles y están disponibles para el usuario; opción por defecto):

```
[HKEY_LOCAL_MACHINE\Comm\Security\Policy\LASSD\LAP\lap_pw]
"PasswordComplexity"=dword:00000002
```

215. Tras confirmar el PIN de acceso, Windows Mobile 6.5 solicitará confirmación por parte del usuario antes de fijar el nuevo PIN en el dispositivo móvil, y en el caso de que el PIN elegido sea una secuencia simple de dígitos, como por ejemplo secuencias que se repiten o que siguen un patrón entre sus dígitos, como 1111, 1234, 2468, 1357, etc, el terminal no lo utilizará como clave de acceso y obligará al usuario a elegir otro valor (una secuencia de números más difícilmente adivinable):

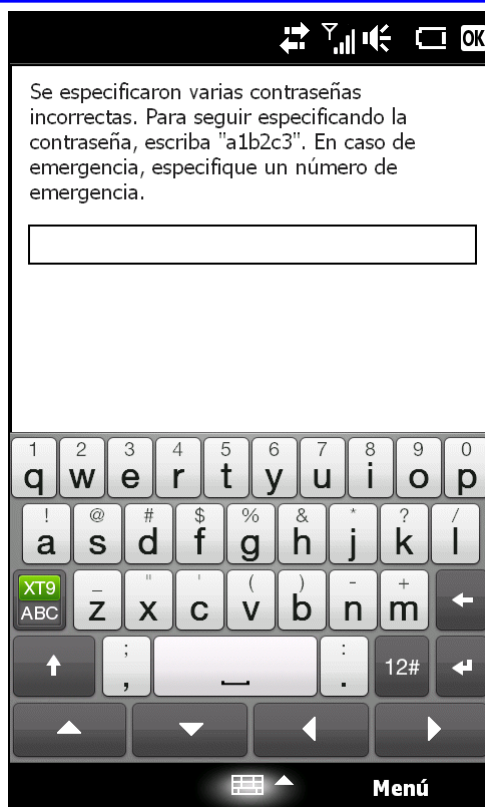


216. El uso de un PIN con secuencia simple (1111, 1234, etc) como clave de acceso al dispositivo móvil está especificado por la siguiente clave del registro, cuyos valores pueden ser “0” (el PIN no puede ser una secuencia fácilmente adivinable; configuración por defecto) ó “1” (se permite el uso de un PIN simple):

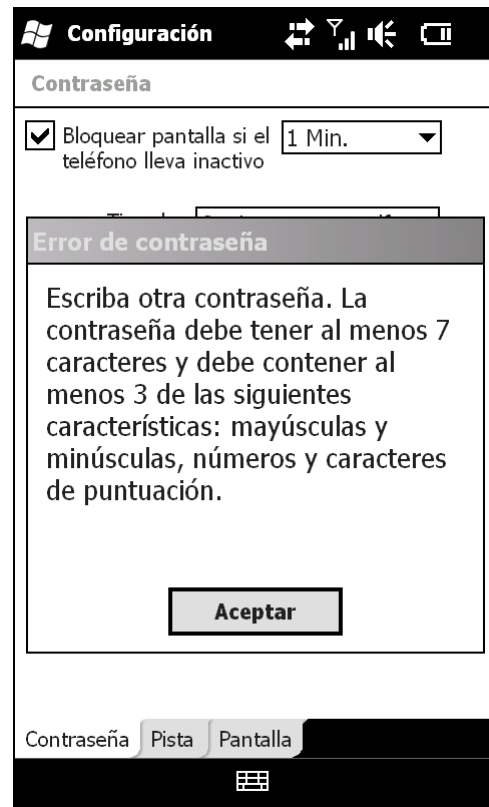
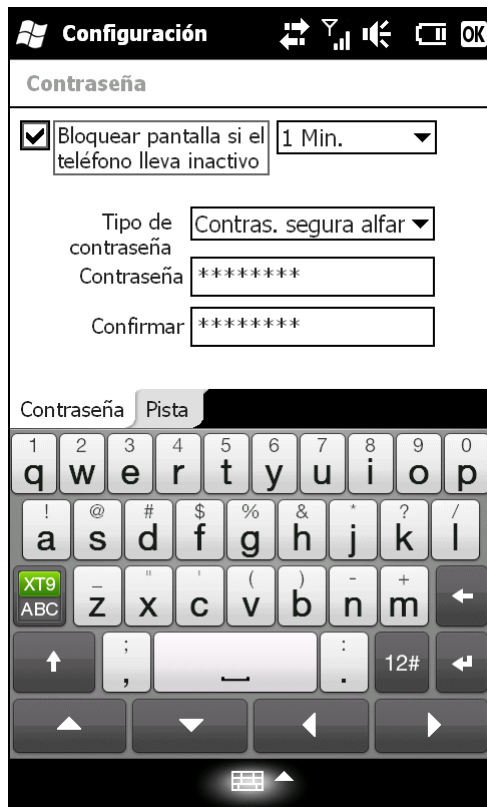
```
[HKEY_LOCAL_MACHINE\Comm\Security\Policy\LASSD\LAP\lap_pw]
"AllowSimplePIN"=dword:00000000
```

217. Pese a la debilidad de un PIN de 4 dígitos frente a ataques de adivinación o fuerza bruta, Windows Mobile 6.5 implementa un mecanismo que hace que cada vez que se introduzca un PIN (o contraseña) incorrecta, el tiempo que el dispositivo móvil tarda en responder será cada vez mayor hasta que parezca que éste no responde al pulsar el botón de desbloqueo [Ref.- 40].
218. Adicionalmente, Windows Mobile 6.5 implementa un mecanismo tipo CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) dónde el usuario debe teclear una secuencia proporcionada por el terminal (*codeword* en terminología Microsoft) para poder seguir intentando desbloquear el dispositivo móvil tras varios intentos de acceso fallidos [Ref.- 40].
219. La siguiente clave del registro, “CodeWordFrequency”, especifica el número de intentos de acceso fallido tras los que se mostrará el *codeword* (el valor por defecto es cada 8 intentos), siendo el valor del *codeword* el especificado por la clave “CodeWord” (el valor por defecto es “a1b2c3”):

```
[HKEY_LOCAL_MACHINE\Comm\Security\LASSD]
"CodeWordFrequency"=dword:00000008
"CodeWord"="a1b2c3"
```



220. El objetivo del *codeword* es evitar que la interacción del usuario con el teclado del dispositivo móvil de forma inadvertida active acciones como la eliminación de los datos del dispositivo móvil (*wipe*). Por este motivo, el valor del número de intentos fallidos necesario para mostrar el *codeword* siempre debería ser menor que el valor del número de intentos fallidos que dan lugar a la eliminación de los datos, dando la oportunidad al usuario de introducir el PIN (o contraseña) correcta antes de proceder al borrado de datos.
221. En el caso de emplear una contraseña alfanumérica (opción recomendada), por defecto debe tener un número mínimo de 7 caracteres y contener valores en tres categorías de las cuatro siguientes: letras minúsculas, letras mayúsculas, números y símbolos de puntuación [Ref.- 29]:



222. El número de categorías diferentes para las que la contraseña debe contener caracteres para ser considerada suficientemente robusta está especificado por la siguiente clave del registro, cuyo valor es el número de categorías (tres por defecto):

```
[HKEY_LOCAL_MACHINE\Comm\Security\Policy\LASSD\LAP\lap_pw]
"ComplexElements"=dword:00000003
```

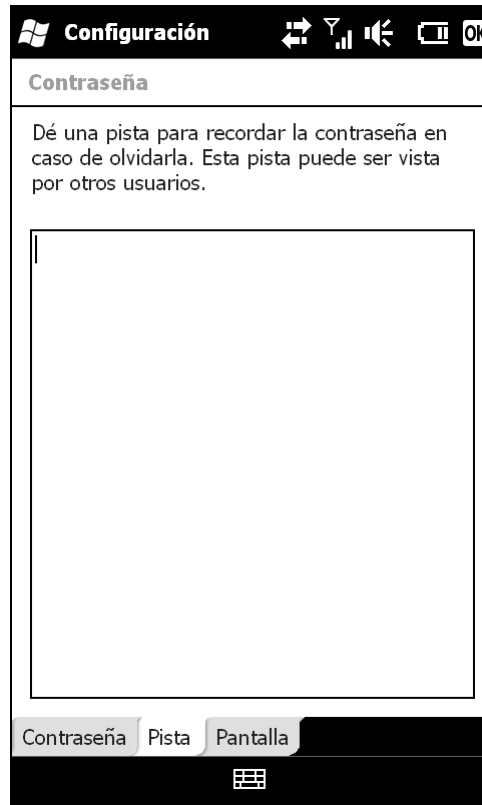
223. Para proceder a modificar el PIN (o contraseña) de acceso al dispositivo móvil, en caso de disponer de un valor ya fijado, es necesario introducir el PIN (o contraseña) actual.
224. Una vez ha sido establecido el PIN (o contraseña), el dispositivo móvil solicitará al usuario el PIN (o contraseña) para desbloquear el acceso al terminal cada vez que esté bloqueado, como por ejemplo al encender el terminal o tras un tiempo de inactividad.
225. Se recomienda por tanto establecer el bloqueo del dispositivo móvil tras un tiempo de inactividad, como por ejemplo 1 minuto (opción seleccionada en todas las pantallas de configuración previas). El rango razonable debería estar entre 1 y 5 minutos, pero debe ser definido por la política de seguridad de la organización propietaria del terminal.
226. La opción de "0 minutos" podría ser empleada para no establecer el bloqueo del terminal tras un periodo de inactividad, pero se desaconseja su utilización.
227. La siguiente clave del registro permite establecer el tiempo de bloqueo de la pantalla del dispositivo móvil en minutos (5 minutos en el ejemplo inferior):

```
[HKEY_LOCAL_MACHINE\Comm\Security\LASSD\AE\{50C13377-C66D-400C-889E-C316FC4AB374}]
"AEFrequencyValue"=dword:00000005
"AEFrequencyType"=dword:00000001
```

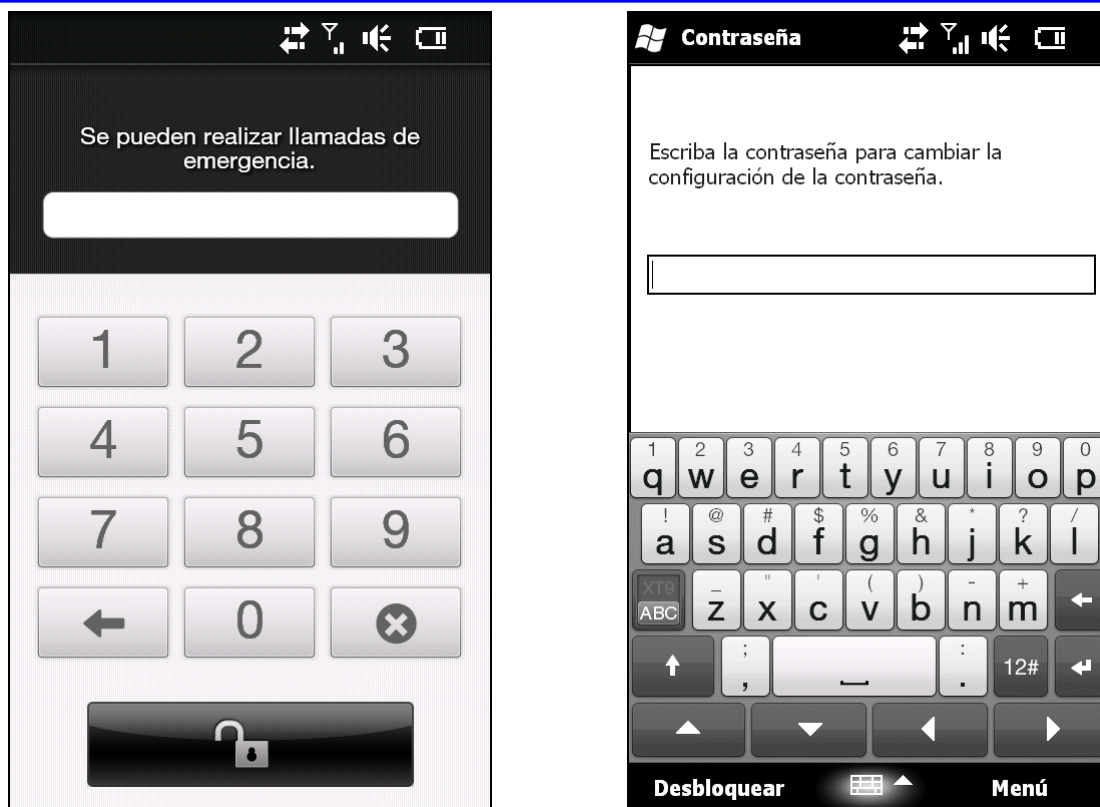
Al habilitar dicho parámetro se crea automáticamente la siguiente clave en el registro:

```
[HKEY_LOCAL_MACHINE\Comm\Security\Policy\LASSD\AE\{50C13377-C66D-400C-889E-C316FC4AB374}]
```

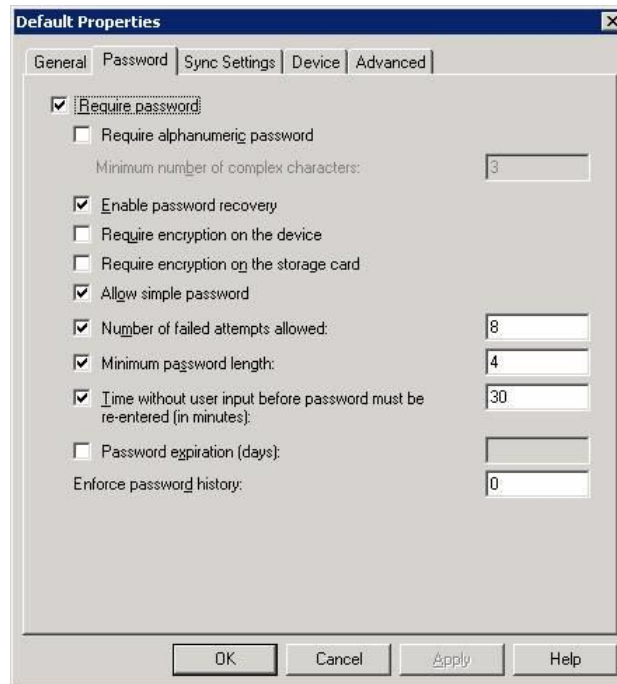
228. En ningún caso se recomienda establecer una pista que proporcione información respecto a la posible contraseña del dispositivo móvil en el caso de olvidarla, opción disponible a través de la pestaña “Pista” (del menú “Inicio – Configuración – Seguridad – Bloqueo del Teléfono”):



229. Por defecto, la pista asociada a la clave de acceso se mostrará tras 5 intentos de acceso fallidos al dispositivo móvil, valor no modificable y establecido de fábrica por Microsoft.
230. Como se puede apreciar en las siguientes dos imágenes, la pantalla de desbloqueo de Windows Mobile 6.5 permite diferenciar visualmente entre ambas configuraciones de desbloqueo del terminal, PIN simple o contraseña segura, lo que puede facilitar a un potencial atacante una primera aproximación al nivel de seguridad existente en el dispositivo móvil:



231. Adicionalmente, es posible establecer éstos y otros parámetros de configuración asociados al proceso de desbloqueo del dispositivo móvil a través de Microsoft Exchange, como por ejemplo el tamaño mínimo de la clave o el periodo de expiración de la misma [Ref.- 31].
232. Su configuración es posible a través de Microsoft Exchange (y en concreto de la Exchange Management Console), mediante las siguientes opciones de la pestaña "Password" de la política de seguridad [Ref.- 34] [Ref.- 37] (se describen únicamente las asociadas a la gestión de contraseñas, detallándose el resto en los apartados correspondientes):



- *Require password*: Forzar el uso de un PIN o contraseña para el acceso al dispositivo móvil. Esta opción habilita el resto de opciones.
- *Require alphanumeric password*: Forzar el uso de una contraseña alfanumérica, más segura que un PIN de 4 dígitos.
- *Minimum number of complex characters*: Número de categorías de las que la contraseña debe contener caracteres para ser considerada suficientemente robusta.
- *Allow simple password*: Permitir el uso de un PIN cuya secuencia de dígitos es simple o fácilmente adivinable (1111, 1234, etc).
- *Minimum password length*: Longitud mínima de la contraseña.
- *Time without user input before password must be re-entered (in minutes)*: Tiempo de inactividad tras el que se producirá el bloqueo del dispositivo móvil y el usuario deberá introducir la contraseña de acceso para su uso.
- *Password expiration (days)*: Número de días para la expiración de la contraseña, tras el cual será necesario cambiar su valor.
- *Enforce password history*: Número de contraseñas almacenadas en el histórico de contraseñas y que, por tanto, el usuario no podrá reutilizar.

Nota: las políticas de seguridad en Microsoft Exchange (y Exchange ActiveSync) están disponibles a través de la Exchange Management Console (EMC), y en concreto, dentro del árbol de Microsoft Exchange en la rama “Organization Configuration → Client Access”, bajo la pestaña “Exchange ActiveSync Mailbox Policies” de la ventana principal. Los parámetros de configuración pueden ser accedidos mediante el menú “Properties” (botón derecho) de la política de seguridad a configurar.

233. La longitud mínima de la contraseña está especificada por la siguiente clave del registro, cuyo valor es la longitud en número de caracteres del PIN o contraseña (el valor por defecto es de 4 dígitos para el PIN):

```
[HKEY_LOCAL_MACHINE\Comm\Security\Policy\LASSD\LAP\lap_pw]  
"MinimumPasswordLength"=dword:00000004
```

234. El periodo de expiración de la contraseña, tras el cual es necesario cambiar la misma, está especificado por la siguiente clave del registro, cuyo valor por defecto es cero días de expiración, indicando que la contraseña no expira:

```
[HKEY_LOCAL_MACHINE\Comm\Security\Policy\LASSD\LAP\lap_pw]  
"ExpirationPeriod"=dword:00000000
```

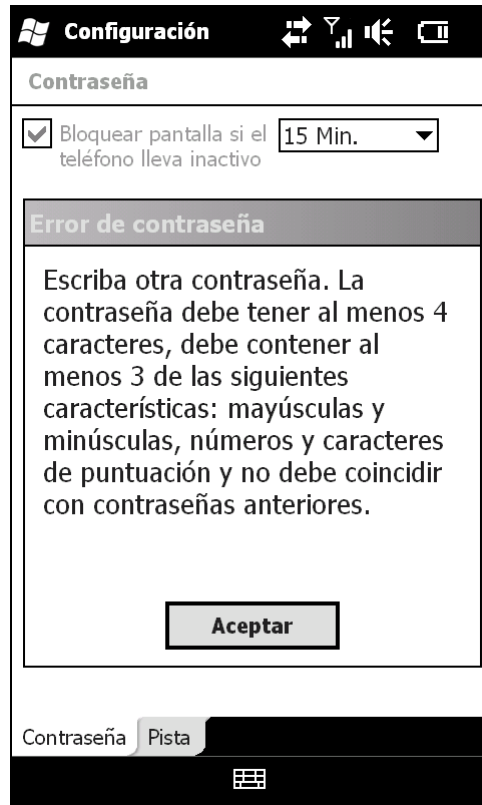
235. Una vez la contraseña ha expirado, Windows Mobile 6.5 notifica al usuario de este hecho y fuerza a su modificación:

The screenshot shows the 'Contraseña' (Password) settings screen on a Windows Mobile 6.5 device. At the top, there are icons for settings, search, volume, and a keyboard icon. The screen is divided into two main sections. The top section, titled 'Contraseña', contains a checkbox labeled 'Bloquear pantalla si el teléfono lleva inactivo' (Lock screen if phone is inactive) which is checked, and a dropdown menu set to '15 Min.'. Below this, there is a 'Tipo de contraseña' (Password type) dropdown set to 'Código PIN simple' (Simple PIN code), and a 'Contraseña' (Password) field showing eight asterisks. The bottom section, titled 'Contraseña caducada' (Password expired), has a grey background and contains the text 'La contraseña ha caducado. Cámbiela ahora.' (The password has expired. Change it now.) and an 'Aceptar' (Accept) button. At the very bottom, there are three tabs: 'Contraseña' (selected), 'Pista' (Hint), and 'Pantalla' (Screen). Below the tabs are 'Cancelar' (Cancel) and a keyboard icon.

236. El número de contraseñas a almacenar en el histórico con el objetivo de evitar su reutilización está especificado por la siguiente clave del registro, cuyo valor por defecto es cero, indicando que no se almacena ningún histórico de contraseñas:

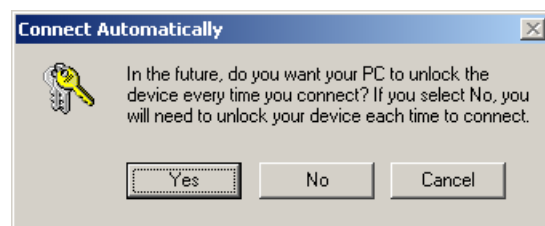
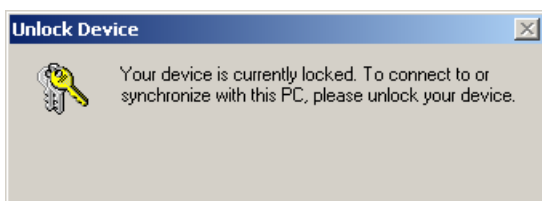
```
[HKEY_LOCAL_MACHINE\Comm\Security\Policy\LASSD\LAP\lap_pw]  
"NumberOfPasswords"=dword:00000000
```

237. En el caso de habilitar el histórico de contraseñas, al proceder a modificar la misma y reutilizar una contraseña previamente empleada, Windows Mobile 6.5 notifica al usuario de este hecho y fuerza a la elección de otra contraseña diferente:



238. Cuando se establece un PIN o contraseña de acceso al dispositivo móvil, ActiveSync notifica el nuevo estado del terminal y advierte al usuario de la necesidad de desbloquear el dispositivo móvil para tener acceso al mismo y poder realizar las tareas de sincronización (imagen inferior izquierda).

239. Adicionalmente, ActiveSync ofrece al usuario la opción de poder desbloquear el dispositivo móvil automáticamente en el futuro (imagen inferior derecha), evitando así que el usuario tenga que desbloquearlo manualmente cada vez que éste se conecta y antes de poder llevar a cabo las tareas de sincronización.



240. En el caso de responder afirmativamente, la clave de acceso al dispositivo móvil es almacenada por ActiveSync en el registro de Windows del ordenador de forma cifrada (y en binario), y concretamente bajo la siguiente clave del registro (dónde “<deviceid>” es un identificador del dispositivo móvil de 8 caracteres asociado al vínculo creado en ActiveSync entre el ordenador y el dispositivo móvil):

```
HKEY_CURRENT_USER\Software\Microsoft\Windows CE Services\Partners\  
<deviceid>\Password
```

241. Una vez fijados tanto el PIN en la tarjeta SIM como en el dispositivo móvil, al encender el terminal, el dispositivo móvil solicitará el PIN del terminal y después el de la tarjeta SIM, en este orden:



242. Pese a que la obligatoriedad de introducir dos PIN's diferentes puede suponer una molestia para el usuario, cuyos valores desde el punto de vista de seguridad se recomienda sean distintos, es necesario establecer ambos niveles de seguridad para que, tanto la tarjeta SIM y sus servicios asociados, como el dispositivo móvil y sus datos asociados, estén protegidos.
243. Adicionalmente, y con el objetivo de mejorar globalmente la seguridad de los servicios asociados al dispositivo móvil, se recomienda modificar a la mayor brevedad posible el PIN de acceso al buzón de voz proporcionado por el operador de telefonía móvil al activar este servicio. Su valor debe ser diferente al valor del PIN (o contraseña) de acceso al terminal y de la tarjeta SIM.

5.10.3 RECUPERACIÓN DE LA CONTRASEÑA DE ACCESO

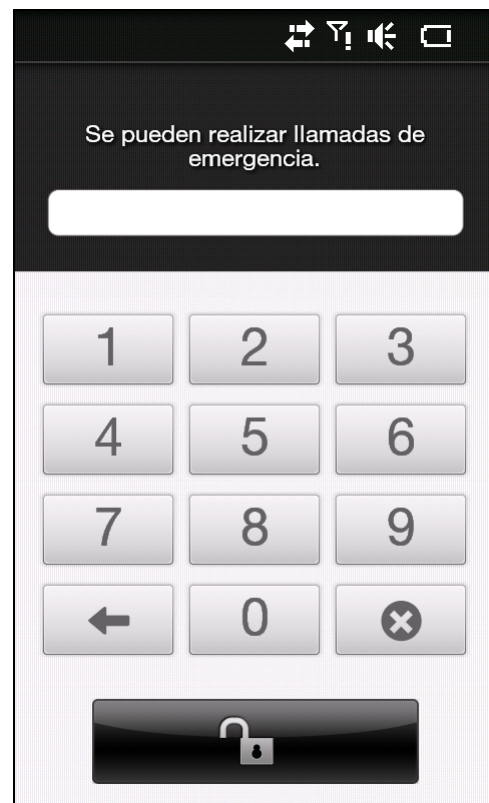
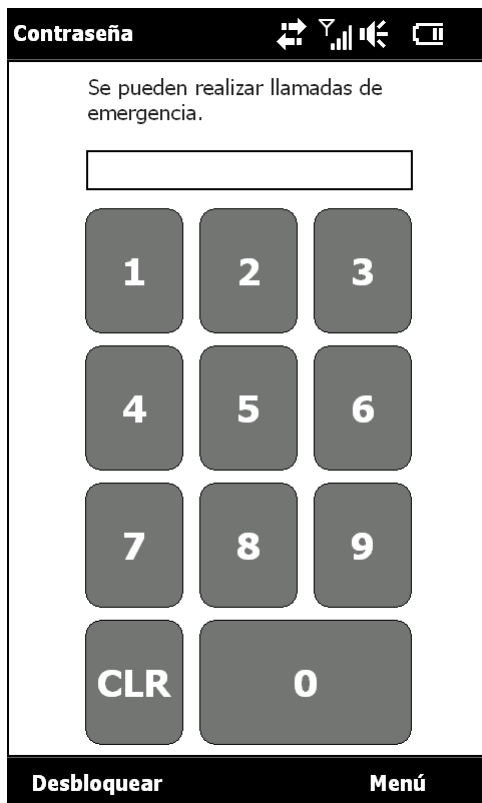
244. Microsoft Exchange (o SCMDM 2008 SP1 [Ref.- 45]) permite la generación de una clave para disponer de acceso al dispositivo móvil, por ejemplo, cuando el acceso al dispositivo móvil está protegido por PIN (o contraseña) y el usuario olvida dicho PIN (o contraseña), en adelante clave de recuperación (de acceso).
245. El proceso se basa en la generación y utilización de una clave de recuperación que permita al usuario desbloquear el dispositivo móvil y establecer una nueva clave de acceso (PIN o contraseña) sin tener que eliminar los datos del dispositivo móvil (*wipe*).
246. La clave de recuperación es un valor numérico de 20 dígitos que es generado automáticamente durante el proceso de configuración del dispositivo móvil, y es transmitido de forma transparente para el usuario al servidor Microsoft Exchange (o SCMDM), donde es almacenado.

247. La configuración de esta opción de recuperación es posible a través de Microsoft Exchange (y en concreto de la Exchange Management Console), mediante la opción “Enable password recovery” de la pestaña “Password” de la política de seguridad [Ref.-34].

Nota: con carácter informativo, ya que la activación de esta funcionalidad debe llevarse a cabo a través del servidor empresarial empleado para la gestión de dispositivos móviles, Microsoft Exchange o SCMDM, la siguiente clave del registro define si se permite la obtención de una clave de recuperación (proceso conocido como “Authentication Reset”), y sus valores pueden ser “0” (deshabilitado) ó “1” (habilitado):

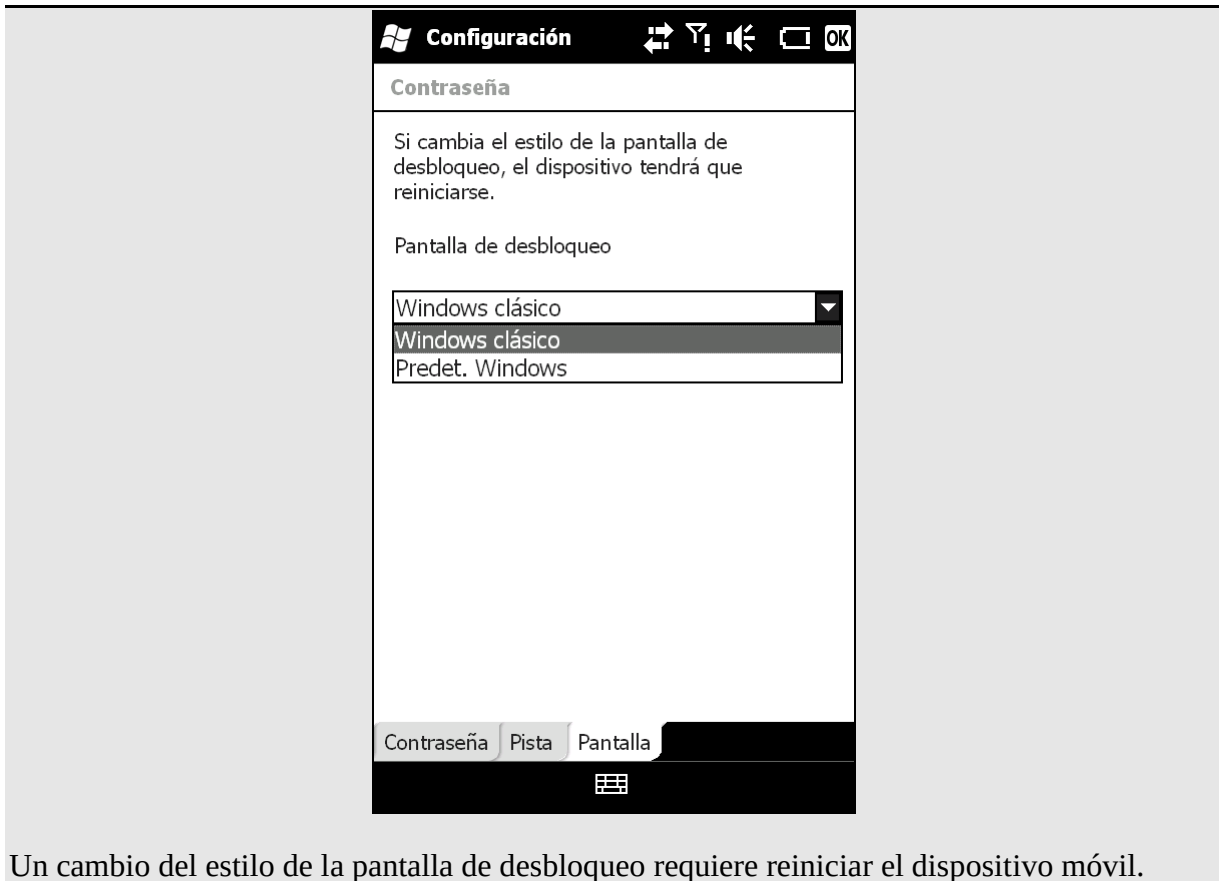
```
[HKEY_LOCAL_MACHINE\Comm\Security\Policy\LASSD\AuthReset]
"AuthenticationReset"=dword:00000001
```

248. Una vez la funcionalidad ha sido habilitada, el usuario dispondrá de la opción “Restablecer contraseña” desde el botón “Menú” disponible (abajo a la derecha) en la pantalla de desbloqueo del dispositivo móvil (cuando se emplea la versión “Windows clásico”):



Nota: Windows Mobile 6.5 permite hacer uso de dos tipos de pantalla de desbloqueo diferentes, empleadas para procesar la clave de acceso (PIN o contraseña) por parte del usuario, “Predet. Windows” (“Predeterminada de Windows”, pantalla por defecto) o “Windows clásico”, mostradas en las imágenes superiores.

La opción de selección del tipo de pantalla de desbloqueo está disponible en el menú “Inicio – Configuración – Seguridad – Bloqueo del teléfono”, a través de la pestaña “Pantalla”:



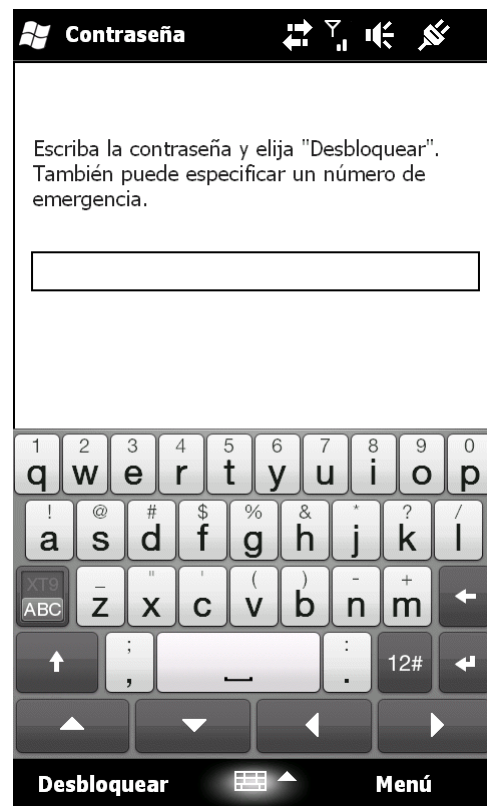
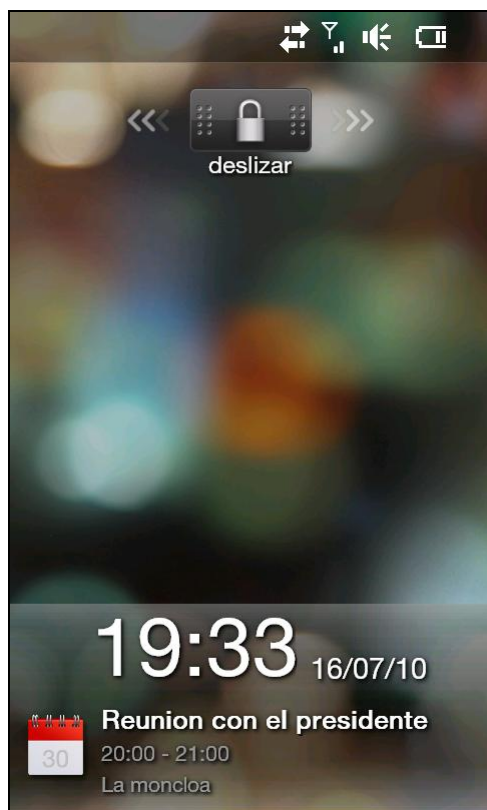
249. Los mensajes mostrados al usuario durante el proceso de recuperación de la clave de acceso también pueden ser configurados a través del registro de Windows Mobile 6.5 [Ref.- 40].
250. Los usuarios desde OWA (Outlook Web Access) pueden obtener la clave de recuperación y desbloquear su dispositivo móvil a través de la sección “Options”, y en concreto la sección “Mobile Devices”. Una vez seleccionado el dispositivo móvil, debe usarse la opción “Display Recovery Password”.

Nota: la sección “Mobile Devices” sólo estará disponible si ActiveSync ha sido habilitado para ese usuario en Microsoft Exchange [Ref.- 46].

251. Los administradores, desde la Exchange Management Console, pueden igualmente obtener la clave de recuperación de un dispositivo móvil a través de la rama “Recipient Configuration → Mailbox”. La clave de recuperación puede ser visualizada mediante el menú “Manage Mobile Device” (botón derecho) del mailbox asociado al dispositivo móvil.
252. Tras completar el proceso se genera una nueva clave de recuperación que es de nuevo transmitida por el dispositivo móvil al servidor Microsoft Exchange [Ref.- 44], y que será empleada en procesos de recuperación de acceso futuros.

5.11 PANTALLA DE DESBLOQUEO: PREVISUALIZACIÓN DE DATOS

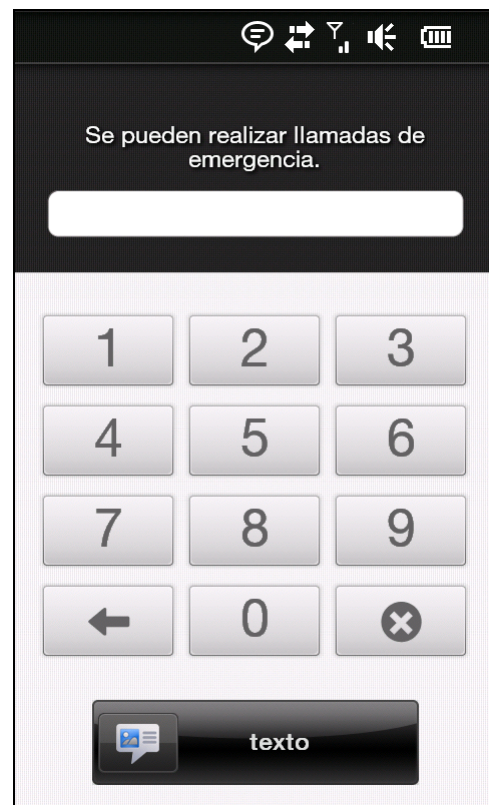
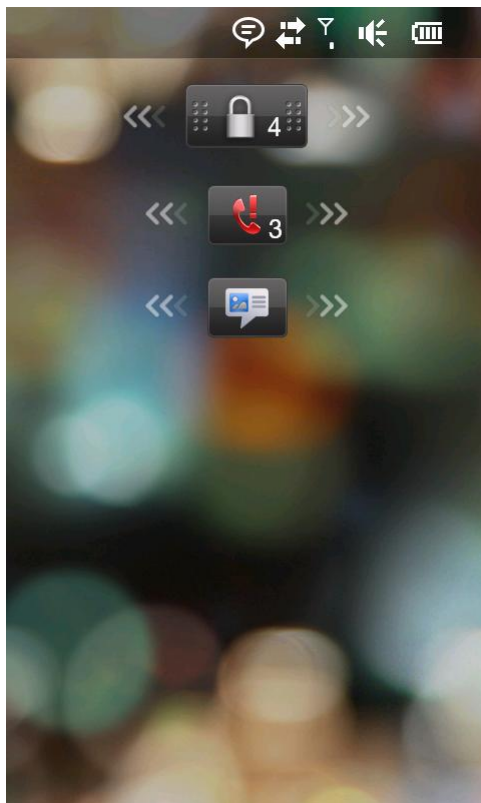
253. La nueva pantalla de desbloqueo del terminal (*lock screen*) en Windows Mobile 6.5 permite, junto a la hora y la fecha, la previsualización de la próxima cita de calendario sin necesidad de introducir el PIN o contraseña de acceso y, por tanto, sin necesidad de desbloquear el teléfono.
254. La pantalla de bloqueo puede desvelar por tanto información potencialmente confidencial a un potencial atacante. La información de cita mostrada incluye la fecha, tramo horario, descripción o título de la misma, y ubicación.
255. La pantalla de desbloqueo permite visualizar esa información sólo si el dispositivo móvil está configurado con un PIN simple para su protección. En el caso de emplear una contraseña segura alfanumérica, la pantalla de desbloqueo no dispone de capacidades de previsualización y únicamente muestra la pantalla para introducir la contraseña de acceso.



256. Desde el punto de vista de seguridad, esta nueva funcionalidad de previsualización permitiría a un potencial atacante la lectura de citas de calendario simplemente con poder tener acceso visual a la pantalla del dispositivo móvil antes de que tengan lugar.
257. Asimismo, debe considerarse que en numerosas ocasiones las citas de calendario pueden contener información sensible y confidencial, que en el caso de ser accedida por un potencial atacante, podrían dar lugar a incidentes de seguridad de mayor relevancia.
258. Desde el punto de vista de seguridad, se recomienda deshabilitar esta previsualización mediante la utilización de una contraseña alfanumérica de acceso al dispositivo móvil (ver apartado “5.10.2. PIN o contraseña de acceso del dispositivo móvil”).
259. La nueva pantalla de desbloqueo muestra adicionalmente otras notificaciones, como la recepción de nuevos mensajes de texto, llamadas perdidas, mensajes del buzón de voz, e-

mails, etc. Concretamente, el botón de desbloqueo indica el número total de notificaciones pendientes.

260. Si en lugar de deslizar el botón de desbloqueo, el usuario patea sobre él, obtendrá un nuevo conjunto de botones asociados a las notificaciones pendientes, cada uno de ellos indicando el número de notificaciones pendientes de ese tipo.
261. Es posible deslizar cualquiera de estos botones para acceder directamente a la aplicación asociada al tipo de notificación (sistema de mensajes de texto, teléfono, lector de correo electrónico, etc), sin embargo, Windows Mobile 6.5 protege la información de forma adecuada desde el punto de vista de seguridad, ya que es necesario introducir el PIN (o contraseña) de acceso para desbloquear el dispositivo móvil antes de tener acceso al contenido de la notificación (desvelándose únicamente el número de notificaciones de cada tipo):

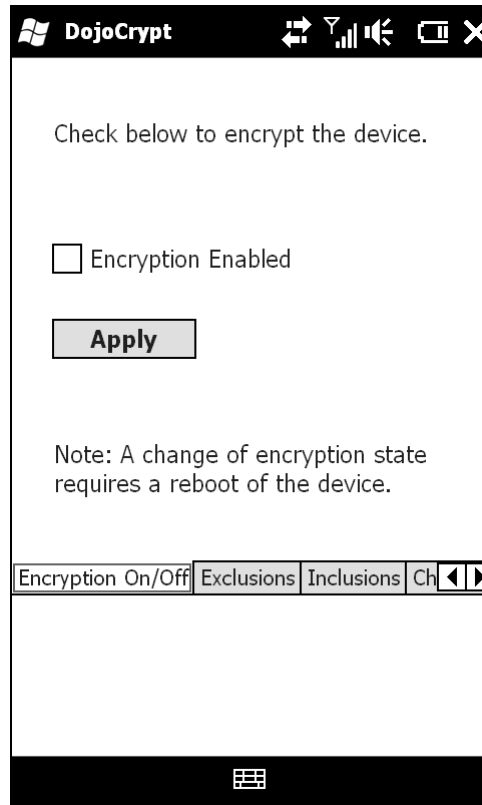


5.12 CIFRADO DE DATOS EN WINDOWS MOBILE

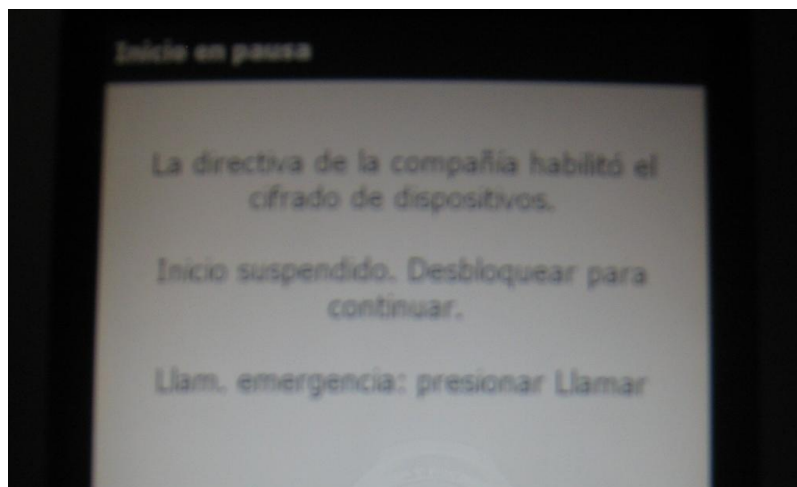
5.12.1 CIFRADO DEL DISPOSITIVO MÓVIL

262. Windows Mobile 6.5 permite el cifrado de los datos almacenados en el dispositivo móvil de forma nativa mediante el algoritmo AES de 128 bits (funcionalidad disponible desde Windows Mobile 6.1 y denominada “On Device Encryption”), con un impacto bajo en el rendimiento del terminal.
263. Para ello se emplea el subsistema DPAPI (Data Protection API), que tiene asociadas dos claves maestras (en el modelo two-tier) generadas por el dispositivo móvil automáticamente, la clave SYSTEM (sólo accesible para aplicaciones “Trusted”) y la clave USER. Al disponer sólo de dos claves, no es posible limitar que una aplicación descifre los datos de otra del mismo nivel de ejecución.

264. La clave empleada para el cifrado está protegida por el PIN (o contraseña) de acceso al dispositivo móvil, y el cifrado funciona de forma transparente una vez el terminal ha sido activado. Durante el proceso de inicio del terminal, se solicita el PIN al usuario, y mediante el mismo, se procede a descifrar e iniciar el sistema operativo. En caso de no proporcionar el PIN, el proceso de inicio queda suspendido, pudiéndose únicamente realizar llamadas de emergencia.
265. Por defecto, no se cifra todo el dispositivo móvil, sino se cifran únicamente los datos contenidos en la carpeta “\My Documents”, los datos de sincronización y contenidos de e-mails (incluidas las tareas, calendario, notas y los adjuntos de e-mails; “pim.vol”), o la caché temporal de navegación en Internet [Ref.- 32].
266. El cifrado del dispositivo móvil sólo puede ser gestionado a través de una política de seguridad específica, no existiendo ninguna opción disponible en el interfaz de usuario de Windows Mobile 6.5, al considerarse una configuración de seguridad empresarial que no se desea pueda ser manipulada por el usuario final.
267. La configuración del cifrado es posible a través de Microsoft Exchange (y en concreto de la Exchange Management Console), mediante la opción “Require encryption on device” de la pestaña “Password” de la política de seguridad (ya que disponer de un PIN o contraseña para el bloqueo del terminal es requisito necesario para el cifrado del mismo).
268. Mediante políticas de grupo (Group Policy Object, GPO) es posible la configuración de cifrado desde SCMDM, disponiendo incluso de la capacidad para excluir ciertos ficheros según su tipo, como por ejemplo evitar el cifrado de ficheros multimedia, audio y video, normalmente de mayor tamaño.
269. En el caso de querer verificar o modificar el estado del cifrado del dispositivo móvil en Windows Mobile 6.5 sin hacer uso de las opciones de gestión empresariales mencionadas, existe una utilidad denominada “DojoCrypt” [Ref.- 33] que permite gestionar este parámetro de configuración: habilitar o deshabilitar el cifrado, excluir ficheros o carpetas individuales o según su tipo, e incluir ficheros o carpetas a cifrar.
270. Por defecto, y salvo que el fabricante o el operador de telefonía móvil que proporcionan el dispositivo móvil hayan realizado alguna configuración de seguridad específica, el cifrado del dispositivo móvil estará deshabilitado, tal y como se refleja mediante DojoCrypt en la siguiente imagen:



271. Se recomienda por tanto habilitar el cifrado del dispositivo móvil con el objetivo de evitar ataques de acceso a los datos en caso en el que un potencial atacante disponga de acceso físico al dispositivo móvil y desconozca el PIN (o contraseña) de acceso. Tras modificar este parámetro de configuración, es necesario reiniciar el dispositivo móvil para que el cifrado sea activado.
272. Si el cifrado del dispositivo móvil está activado, al iniciar, Windows Mobile 6.5 mostrará un mensaje indicando este hecho, y reflejando que el inicio del sistema operativo ha sido suspendido y que es necesario desbloquear el terminal para continuar con el proceso de inicio. Tras desbloquear el dispositivo móvil con el PIN (o contraseña) de acceso, Windows Mobile 6.5 se iniciará normalmente:



273. En dicho estado sólo es posible realizar llamadas de emergencia (112) tras pulsar el botón de llamada físico del dispositivo móvil.

5.12.2 CIFRADO DE LAS TARJETAS DE ALMACENAMIENTO EXTERNAS

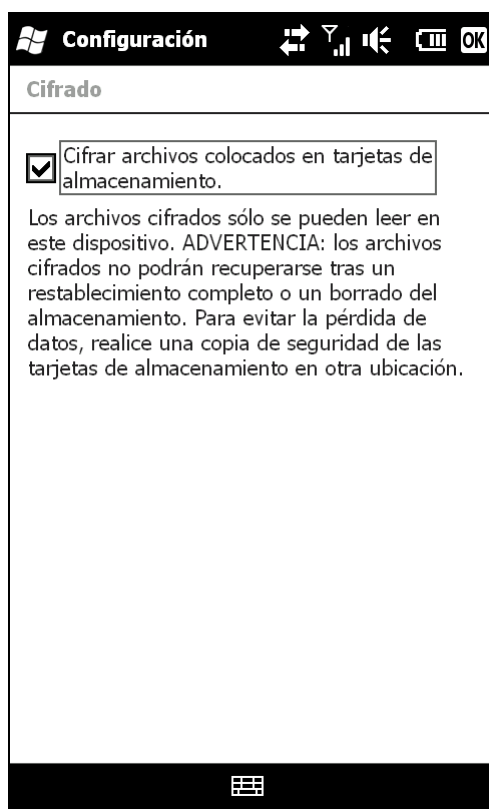
274. Adicionalmente, Windows Mobile 6.5 permite cifrar los datos que vayan a ser guardados en tarjetas de almacenamiento externas mediante AES de 128 bits (funcionalidad disponible desde Windows Mobile 6.0 y denominada “SD Card Encryption”) [Ref.- 30].

275. Para ello es necesario habilitar la opción “Cifrar archivos colocados en tarjetas de almacenamiento”, disponible en el menú “Inicio – Configuración – Seguridad – Cifrado” (deshabilitada por defecto).

Nota: Windows Mobile no permite exportar (o recuperar) las claves empleadas para el cifrado. Antes de realizar una actualización completa del sistema operativo del dispositivo móvil (ver apartado “5.1. Actualización del sistema operativo: Microsoft”), si la opción “Cifrar archivos colocados en tarjetas de almacenamiento” está activa, es necesario hacer una copia de seguridad de todos los datos disponibles en la tarjeta de almacenamiento.

276. Con el objetivo de evitar el acceso a los datos almacenados en tarjetas externas por parte de un potencial atacante, se recomienda habilitar esta opción de configuración.

277. La disponibilidad de una tarjeta de almacenamiento en el dispositivo móvil (así como la memoria total, usada y libre) puede ser confirmada a través del menú “Inicio – Configuración – Almacenamiento”, y concretamente bajo la sección “Tarjeta SD”:



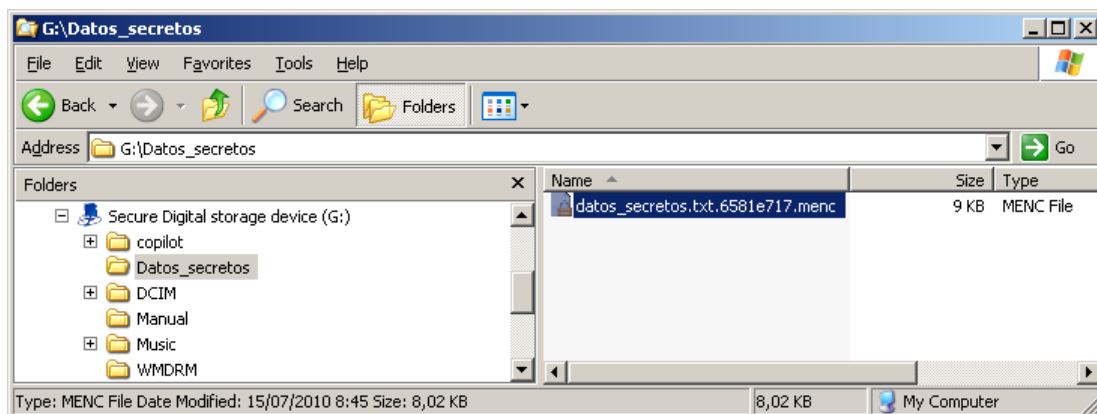
278. La opción de cifrado de las tarjetas de almacenamiento externas está especificada por la siguiente clave del registro, cuyos valores pueden ser “0” (cifrado deshabilitado; opción por defecto) ó “1” (cifrado habilitado):

```
[HKEY_LOCAL_MACHINE\System\StorageManager\Filters\ENCFilt]
"EncryptByDefault"=dword:00000001
```

Nota: adicionalmente, la activación del cifrado en las tarjetas de almacenamiento externas activa el servicio de monitorización de cifrado a nivel del registro de Windows Mobile 6.5:

```
[HKEY_LOCAL_MACHINE\Services\App\Tasks\MonitorEncryption]
"EncryptionTrace"=dword:00000001
```

279. La configuración de este parámetro también es posible a través de Microsoft Exchange (y en concreto de la Exchange Management Console), mediante la opción “Require encryption on the storage card” de la pestaña “Password” de la política de seguridad.
280. La clave de cifrado es generada por DPAPI (tras un *hard reset* o restablecimiento de fábrica del dispositivo móvil) y almacenada en la memoria interna (*flash*) del dispositivo móvil, por lo que los datos cifrados sólo pueden ser accedidos desde el terminal empleado originalmente para su almacenamiento. Adicionalmente, la clave está sólo disponible para aplicaciones privilegiadas, “Trusted”.
281. La extracción de los datos desde la tarjeta de almacenamiento externa ubicada en el dispositivo móvil puede llevarse a cabo a través de ActiveSync, proceso durante el cual los datos son descifrados y enviados al ordenador sin cifrar.
282. Tras activar la opción de cifrado, los datos escritos en la tarjeta de almacenamiento a partir de ese momento serán cifrados, pero no así los datos previamente almacenados.
283. Si la tarjeta de almacenamiento es utilizada en un equipo externo, es posible identificar los ficheros cifrados a través de la extensión “.menc”, siendo completamente transparente al usuario su nombrado cuando la tarjeta es utilizada desde el dispositivo móvil:



5.13 ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL

284. Windows Mobile 6.5 proporciona capacidades, locales y remotas, para la eliminación de todos los datos almacenados en el dispositivo móvil en caso de que el mismo se encuentre en manos de un potencial atacante, proceso conocido como *wipe* (limpieza de datos).
285. El proceso de eliminación de los datos es equivalente a un *hard reset*, es decir, al restablecimiento del dispositivo móvil a la configuración de fábrica. Durante el proceso además se eliminarán los programas instalados, los datos y las configuraciones realizadas por el usuario.
286. La eliminación de datos de forma local se activa tras un número fallido de intentos de acceso al dispositivo móvil cuando éste está bloqueado.

287. Esta característica, no habilitada por defecto para evitar la pérdida de datos no deseada por desconocimiento de la existencia de este mecanismo de seguridad, puede ser configurada tras habilitar la política de seguridad “Password Required Policy” (ID 4131), que fuerza la utilización de una clave de acceso (PIN o contraseña) en el dispositivo móvil (política deshabilitada por defecto).

288. La siguiente clave del registro habilita la política de seguridad “Password Required Policy” (ID 4131), que fuerza la utilización de una clave de acceso. El identificador de política es el 4131 en decimal, que en hexadecimal corresponde a 0x1023 (ver apartado “5.6. Políticas de seguridad, configuraciones de seguridad y roles de seguridad en Windows Mobile”). El valor hexadecimal es empleado para identificar el nombre de la clave del registro: “00001023”. Su valor debe ser “0” si la política está habilitada (se requiere una clave de acceso) y “1” se está deshabilitada:

```
[HKEY_LOCAL_MACHINE\Security\Policies\Policies]
"00001023"=dword:00000000
```

Nota: debe tenerse en cuenta que el valor “1” de la clave del registro **deshabilita** esta política de seguridad, en lugar de habilitarla, como indicaría el sentido común.

289. La activación de esta política de seguridad deshabilita la posibilidad por parte del usuario de no utilizar una clave de acceso al dispositivo móvil, apareciendo en color gris y no seleccionable dicha opción (imagen inferior izquierda):

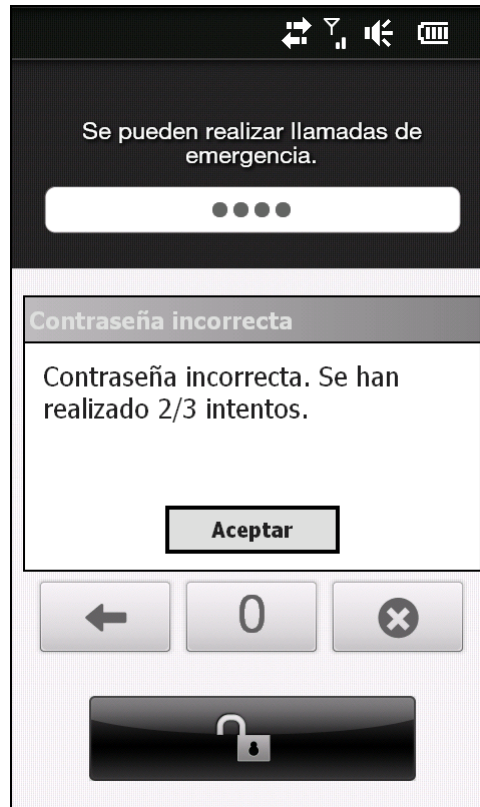


290. La siguiente clave del registro habilita la eliminación local de datos y permite especificar el número de intentos de acceso fallidos que activarán dicho borrado. Su valor debe ser un número decimal positivo, como por ejemplo, 10 intentos (y “0” ó “0xFFFFFFFF” si se desea deshabilitar):

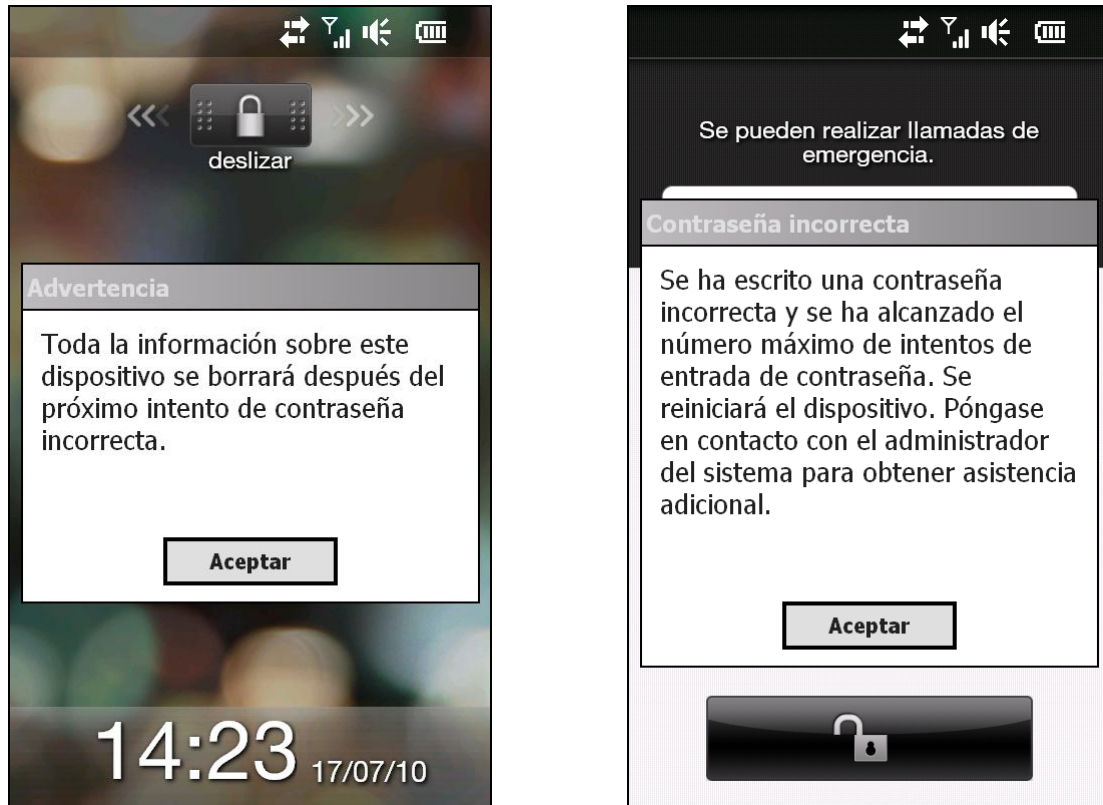
```
[HKEY_LOCAL_MACHINE\Comm\Security\Policy\LASSD]
```

"DeviceWipeThreshold"=dword:00000000A

291. Si se configura el valor "DeviceWipeThreshold" a tres intentos (valor utilizado como ejemplo, pero no recomendado en un entorno real), tras realizar uno o más intentos de acceso fallidos, el dispositivo móvil notificará al usuario al introducir un PIN (o contraseña) incorrecto el número de intentos realizados hasta el momento y el número de intentos totales (por ejemplo, "Se han realizado 2 de 3 (2/3) intentos").



292. Tras realizar el penúltimo intento de acceso fallido (por ejemplo, "9/10"), el dispositivo móvil avisará al usuario; si el siguiente intento de acceso es fallido, se eliminará toda la información del dispositivo móvil (imagen inferior izquierda).
293. En caso de realizarse el último intento de acceso fallido, Windows Mobile 6.5 notificará la situación al usuario (imagen inferior derecha), procederá a eliminar toda la información y reiniciar el dispositivo móvil, llevando a cabo un *hard reset* (restablecimiento de fábrica):



294. Los datos guardados en tarjetas de almacenamiento externas serán también eliminados por completo durante el proceso de eliminación de datos. Debe tenerse en cuenta que esta funcionalidad no estaba disponible hasta la versión 6 de Windows Mobile.

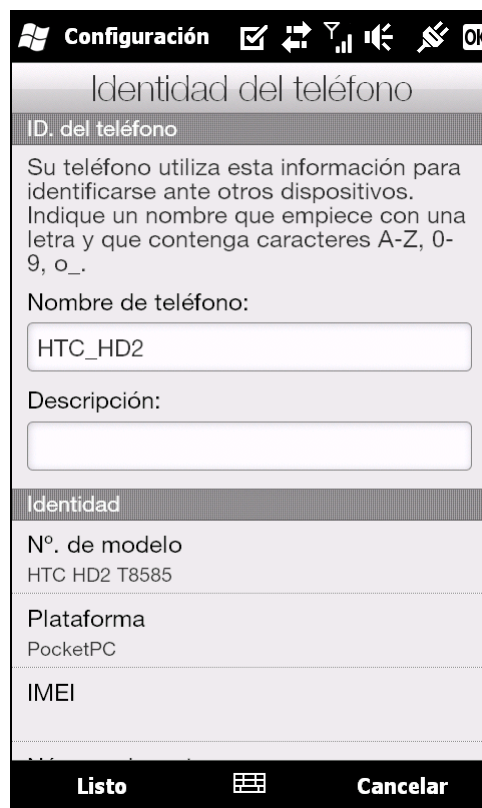
Nota: tras la eliminación de los datos, el único fichero que permanece en la tarjeta de almacenamiento externo es “EncFiltLog.menc”, pero sin ningún contenido relevante. Este fichero es creado al activar el cifrado en tarjetas de almacenamiento externas (ver apartado “5.12.2. Cifrado de las tarjetas de almacenamiento externas”), por lo que está asociado a, y evidencia, el uso previo de cifrado en la tarjeta de almacenamiento externa.

295. La configuración de la funcionalidad de eliminación local de datos es posible a través de Microsoft Exchange (y en concreto de la Exchange Management Console), mediante la opción “Number of failed attempts allowed” de la pestaña “Password” de la política de seguridad [Ref.- 34], y su valor por defecto es 8 intentos.
296. Si el dispositivo móvil ha sido perdido o robado, el administrador puede proceder a la eliminación de los datos de forma remota en cualquier momento (no tras un número de intentos de acceso fallidos) a través de Microsoft Exchange (disponible desde la versión 2007, y en versiones posteriores, como nuevos Service Packs, o Microsoft Exchange 2010 [Ref.- 35]) a través de la Exchange Management Console.
297. También se puede activar la eliminación de datos por parte de su propietario (usuario del dispositivo móvil) desde la sección “Options”, y en concreto la sección “Mobile Devices”, de OWA (Microsoft Office *Outlook Web Access*, 2007). Una vez seleccionado el dispositivo móvil, la eliminación se puede llevar a cabo mediante la opción “Wipe All Data from Device...” [Ref.- 34].

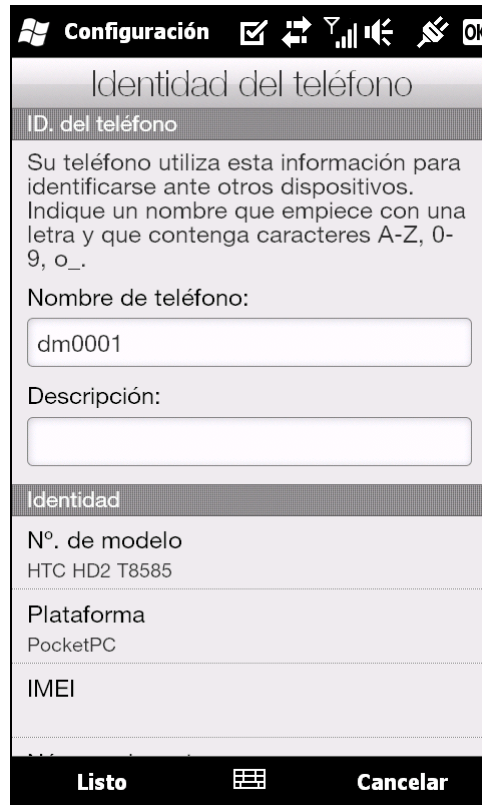
298. La siguiente vez que el dispositivo móvil realice una sincronización con el servidor Microsoft Exchange, obtendrá la política de eliminación de datos y procederá a borrar todos los datos.

5.14 CONFIGURACIÓN POR DEFECTO DEL DISPOSITIVO MÓVIL

299. El dispositivo móvil está configurado por defecto con valores fijados por el fabricante del sistema operativo, el fabricante del hardware o el operador de telefonía móvil, que pueden desvelar detalles del terminal o de su propietario.
300. Para evitar la revelación de información sensible, se recomienda modificar esos valores existentes por defecto por valores elegidos por su propietario.
301. El nombre del dispositivo móvil se fija a través del menú “Inicio”, y en concreto desde la opción “Configuración – Acerca del teléfono – Identidad del teléfono”:



302. En el ejemplo superior asociado al dispositivo móvil empleado para la elaboración de la presente guía, el nombre (“HTC_HD2”) desvela tanto el fabricante del dispositivo móvil, HTC, como el modelo del terminal, HD2, ambos datos muy útiles para un potencial atacante interesado en explotar vulnerabilidades en ese tipo concreto de dispositivo móvil.
303. El nombre del dispositivo móvil debe ser modificado a través del campo “Nombre de teléfono” por uno que no revele detalles ni del dispositivo móvil (fabricante o modelo) ni del propietario (evitando tanto referencias al nombre de la persona como de la organización asociadas al mismo), como por ejemplo “dm0001” (dispositivo móvil 0001) en la imagen inferior, y que será establecido tras pulsar el botón “Listo”:



304. La misma recomendación aplica a la descripción del dispositivo móvil (campo “Descripción”). La descripción del terminal puede no contener un valor, no así el nombre del teléfono, que obligatoriamente debe contener un nombre que empiece con una letra y contenga caracteres A-Z, 0-9 o subrayado (_).

305. El nombre del dispositivo móvil fijado por Microsoft, el fabricante del terminal o el operador de telefonía móvil, está especificado por la siguiente clave del registro (“OrigName”; por defecto “WinCE” para Microsoft), almacenándose el nombre del dispositivo móvil configurado a través del interfaz de usuario en “Name”:

```
[HKEY_LOCAL_MACHINE\Ident]
"Name"="dm0001"
"OrigName"="HTC_HD2"
```

306. La descripción del dispositivo móvil está especificada por la siguiente clave del registro:

```
[HKEY_LOCAL_MACHINE\Ident]
"Desc"="Descripción del dispositivo móvil"
```

307. El nombre del dispositivo móvil puede ser empleado igualmente en otros servicios y tecnologías, como por ejemplo Bluetooth (ver apartado “5.17. Comunicaciones Bluetooth”) o las comunicaciones en redes Microsoft, como por ejemplo en las conexiones de escritorio remoto (ver apartado “5.22. Comunicaciones en entornos de red Microsoft”).

308. Adicionalmente, Windows Mobile 6.5 emplea el nombre del dispositivo móvil, si el parámetro “Name” es distinto al parámetro “OrigName”, en las tramas de anuncio de nombre de NetBIOS (*NetBIOS Name Service*, UDP/137, con el nombre todo en mayúsculas) y en el campo nombre de las peticiones DHCP a la hora de obtener una dirección IP [Ref.- 62].

309. Se recomienda modificar por tanto ambos parámetros del registro para que contengan el mismo valor con el objetivo de no revelar el nombre en el tráfico de comunicaciones mencionado, e incluso evitar así la generación de tráfico NetBIOS desde el terminal:

```
[HKEY_LOCAL_MACHINE\Ident]
"Name"="dm0001"
"OrigName"="dm0001"
```

5.15 LOCALIZACIÓN GEOGRÁFICA

310. Las capacidades de localización del dispositivo móvil a través de GPS están disponibles y son empleadas por aplicaciones como “Google Maps for mobile” (<http://m.google.com/maps>), que en el caso del dispositivo móvil empleado para la elaboración de la presente guía, está disponible como aplicación por defecto a través del menú “Inicio – Google Maps”.
311. Desde “Google Maps” (aplicación que requiere disponer de una conexión de datos) es posible habilitar o deshabilitar el dispositivo GPS, en concreto, desde el botón “Menú” y la opción “Usar GPS”:



312. Adicionalmente “Google Maps” tiene capacidades para localizar la ubicación del dispositivo móvil incluso cuando no se dispone de GPS (o éste no está activo), a través del servicio denominado “My Location” (invocado manualmente mediante la tecla “0”), que emplea la información de localización disponible sobre torres de telefonía móvil y redes Wi-Fi.
313. El servicio de ubicación de Google Maps, “My Location”, emplea conexiones HTTP (no cifradas) desde el dispositivo móvil hacia “mobilemaps.clients.google.com” (“/glm/mmap”) y envía a Google información de las redes inalámbricas (incluyendo el nombre de red, SSID, y su dirección MAC, BSSID) y de las torres de telefonía

(incluyendo el identificador de torre, y los códigos de área (LAC), operador de telefonía móvil (MNC) y país (MCC)) [Ref.- 57] existentes en el área de cobertura del dispositivo móvil.

314. Adicionalmente, la petición incluye información detallada del dispositivo móvil. Por ejemplo, el idioma (español, “es”), la plataforma (Windows Mobile, “winm”), la versión de SO (“PocketPCv5.2.21869”), el modelo (“HTC HD2”), la aplicación empleada (Google Maps for mobile de HTC, “gmm-htc”) y su versión (“3.2.116.1”). Ver apartado “4. Entorno de aplicación de esta guía” para contrastar la información del dispositivo móvil empleado para la elaboración de la presente guía:

```
es.-winm-PocketPCv5.2.21869-HTC HD2 T8585/gmm-htc..3.2.116.1
```

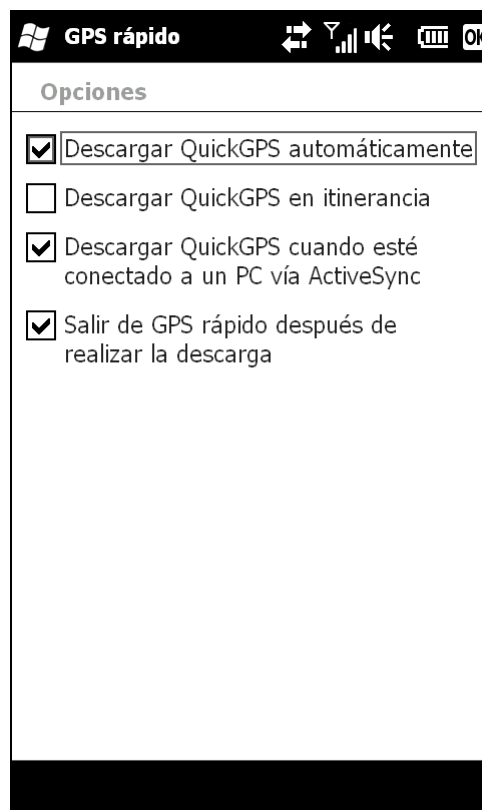
Nota: la información detallada de versiones de las diferentes aplicaciones disponibles en el dispositivo móvil, fundamental a la hora de contrastar si se dispone de una aplicación afectada por una vulnerabilidad de seguridad, está disponible en la siguiente clave del registro (se muestra como ejemplo la versión asociada a “Google Maps for mobile”):

```
[HKEY_LOCAL_MACHINE\Software\OEM\MASD]  
"GPS_GMM"="3_2_116_1"
```

315. Estas peticiones de información hacia Google desvelan información de las redes, Wi-Fi y de telefonía, existentes en el área de cobertura del dispositivo móvil, así como otros detalles relevantes del terminal, a cualquiera que esté capturando el tráfico de datos generado desde el dispositivo móvil. Las respuestas, en formato binario, contienen información de la ubicación estimada del dispositivo móvil.
316. Se recomienda limitar el uso del servicio “Google Maps”, y específicamente su utilización sin emplear el GPS, ya que el servicio de ubicación a través de torres de telefonía y redes Wi-Fi desvela detalles privados del dispositivo móvil y su ubicación.
317. Debe tenerse en cuenta que pese a que el uso del GPS esté seleccionado, hay escenarios en los que no es posible obtener señal de GPS (por ejemplo, en el interior de edificios), por lo que “Google Maps” hará uso de las capacidades de ubicación sin GPS, no siendo posible deshabilitar esta funcionalidad por completo.
318. La modificación de las siguientes dos claves del registro (activas por defecto con el valor “1”) permite reducir la información enviada a Google, tanto de las torres de telefonía (RIL, *Radio Interface Layer*) como de las redes Wi-Fi, reduciendo la precisión de la ubicación del dispositivo móvil:
- ```
[HKEY_LOCAL_MACHINE\Software\Google\GoogleMaps]
"supports_extended_wifi"="0"
"supports_extended_ril"="0"
```
319. La información de localización se integra con las aplicaciones de acceso a redes sociales y Web 2.0, siendo posible la publicación de la ubicación del usuario a través por ejemplo de Twitter (mediante la opción “Actualizar ubicación” del cliente HTC Peep).
320. Se recomienda no hacer pública la ubicación en la que se encuentra el usuario en redes sociales con el objetivo de proteger su privacidad.

### 5.15.1 QUICKGPS

321. Con el objetivo de agilizar el proceso de localización de coordenadas del GPS y su precisión, el dispositivo móvil dispone de la aplicación QuickGPS, disponible desde el menú “Inicio – Herramientas (Herram.) – GPS rápido”.
322. Esta aplicación se conecta a un servidor web de “gpsonextra.net” (xtra1, xtra2 ó xtra3) para descargar la información semanal de la localización de los satélites GPS alrededor del planeta. Por defecto, la descarga automática de esta información está habilitada.
323. Se recomienda deshabilitar la descarga automática de QuickGPS desde el botón “Menú – Opciones” de la aplicación, no seleccionando las opciones “Descargar QuickGPS automáticamente” (habilitada por defecto), “Descargar QuickGPS en itinerancia” y “Descargar QuickGPS cuando esté conectado a un PC vía ActiveSync” (habilitada por defecto):



324. Las siguientes claves del registro permiten configurar (activo = “1”; inactivo = “0”) los cuatro parámetros de la pantalla de opciones respectivamente. Se recomienda fijar todos los valores a “0” (inactivos):

```
[HKEY_LOCAL_MACHINE\Software\HTC\QuickGPS]
"auto"=dword:00000000
"roaming"=dword:00000000
"actSync"=dword:00000000
"autoClose"=dword:00000000
```

### 5.15.2 A-GPS

325. *Assisted GPS* (A-GPS) es un sistema de ayuda para mejorar la obtención de información de localización mediante GPS, y utiliza las torres de telefonía móvil para disponer de una estimación de la ubicación del dispositivo móvil más rápidamente.

326. El módulo A-GPS está disponible en dispositivos móviles Windows Mobile 6.5 con GPS, pero que está deshabilitado por defecto en dispositivos móviles como el empleado para la elaboración de la presente guía, tal y como indican las siguientes claves del registro:

```
[HKEY_LOCAL_MACHINE\Software\HTC\SUPL AGPS]
"EnableAGPS"= dword:00000000
"ServerPort"=dword:00001C6B
"ServerIP"="10.1.101.63"
```

327. La funcionalidad A-GPS envía tráfico hacia los servidores y puerto (por defecto TCP/7275; 0x1C6B) de A-GPS configurados en el registro. El fabricante HTC por defecto fija un servidor de pruebas interno, 10.1.101.63.

328. Los servidores pueden ser proporcionados por los operadores de telefonía móvil ("agps.operador.es" o "supl.operador.es"), que normalmente sólo ofrecen su servicio A-GPS a través de la red de datos de telefonía móvil, para limitar su uso a sus clientes, y no permitir el acceso por parte de cualquiera desde Internet. Adicionalmente, algunos fabricantes de terminales proporcionan servidores A-GPS usando el estándar SUPL, arquitectura "Secure User Plane Location":

```
"ServerURL"="supl.operador.es"
```

329. En el caso de que A-GPS esté habilitado por defecto ("EnableAGPS" con valor "1"), y se disponga de valores asociados a servidores A-GPS reales, se recomienda deshabilitar la funcionalidad A-GPS salvo que se quiera hacer uso explícito de estas capacidades, con el objetivo de evitar desvelar información de la ubicación del dispositivo móvil (por ejemplo, torre de telefonía a la que está asociado) a través del tráfico de datos destinado a los servidores A-GPS.

330. El parámetro "GPSPMode" (con valor "2" por defecto) indica las fuentes a emplear para obtener la estimación del GPS (torres de telefonía móvil, GPS, etc). Por defecto, cuando el valor es "2" ó "4" el dispositivo móvil contactará con los servidores configurados para intercambiar información de su ubicación y mejorar así la precisión de la localización.

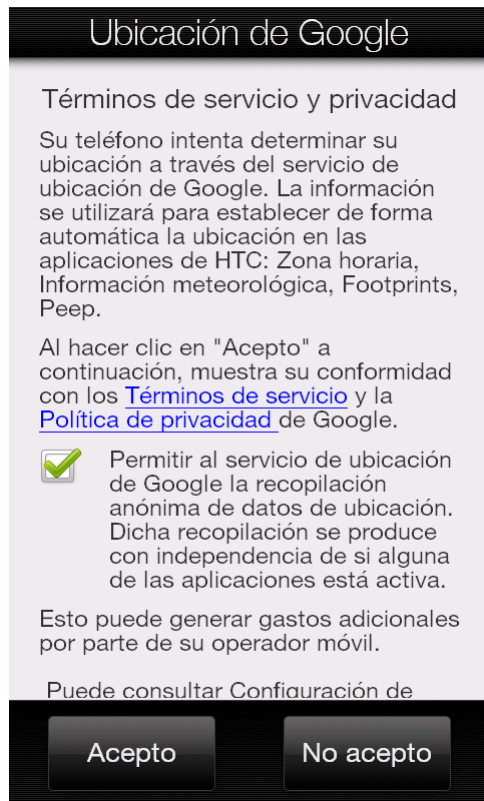
331. En el caso de hacer uso de A-GPS se recomienda incrementar la privacidad de los datos intercambiados mediante cifrado a través de SSL/TLS, para lo que es necesario fijar los parámetros "EnabledPrivacyMethod" ("1"), "PrivacyMethod" ("3") y "TLSHostName". Sin embargo, debe tenerse en cuenta que no todos los proveedores ni todos los dispositivos móviles soportan SSL/TLS para las comunicaciones A-GPS.

### 5.15.3 SERVICIOS DE LOCALIZACIÓN: GOOGLE Y HTC

332. El servicio de ubicación de Google pretende conocer la ubicación del dispositivo móvil a través de la información de localización disponible sobre torres de telefonía móvil y redes Wi-Fi, y la señal recibida en cada momento por el dispositivo móvil para ambas tecnologías (telefonía móvil y Wi-Fi), en lugar de emplear información más precisa como la proporcionada por el dispositivo GPS.

333. Este servicio de ubicación sin GPS es utilizado también por "Google Maps for mobile" (analizado previamente en el apartado "5.15. Localización geográfica").

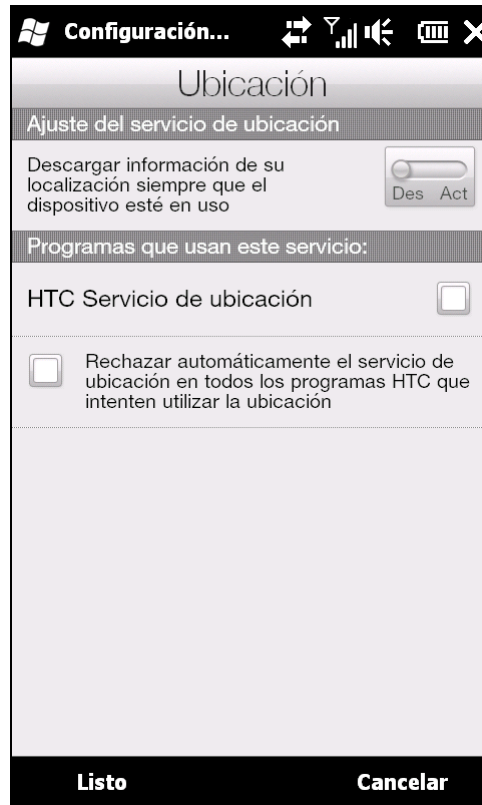
334. Algunas aplicaciones propias de los fabricantes, como HTC, utilizan las capacidades de ubicación de Google, como por ejemplo la aplicación de meteorología accesible a través del acceso directo "Clima" (Información meteorológica; imagen inferior derecha). El servicio es también empleado por otros programas como "Zona horaria", Footprints y Peep:



**Nota:** durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía (activado automáticamente la primera vez que se enciende el terminal), se muestra el mensaje de aceptación del servicio de “Ubicación de Google” (imagen superior izquierda), debiendo el usuario seleccionar la configuración deseada. Se recomienda desactivar la opción “Permitir al servicio de ubicación de Google la recopilación...” y seleccionar el botón “No acepto”.

Este comportamiento, centrado en consultar al usuario acerca de la configuración inicial deseada, es el recomendado desde el punto de vista de seguridad, con el objetivo de no disponer de funcionalidad habilitada por defecto en la que el usuario no está interesado, evitándose así configuraciones por defecto inseguras.

335. Mediante la pantalla de aceptación (imagen superior izquierda) es posible decidir si se permite a Google recopilar información de ubicación, incluso cuando no hay aplicaciones que hagan uso del servicio. Se recomienda no permitir a Google la recopilación de dicha información.
336. Si se acepta el uso del servicio, la recopilación de información será activada y se permitirá su utilización por defecto por parte del programa “HTC Servicio de ubicación” (analizado posteriormente).
337. Es posible deshabilitar el servicio de ubicación de Google (recopilación de información) en cualquier momento desde el menú “Inicio”, y en concreto desde la opción “Configuración – Ubicaciones”, a través del botón deslizante:



338. Adicionalmente, existe la posibilidad de habilitar qué programas pueden hacer uso de este servicio, como por ejemplo el programa “HTC Servicio de ubicación”. Por otro lado, se puede rechazar de forma automática el uso del servicio para todos los programas HTC que requieren conocer la ubicación del usuario, de forma que no pregunten al usuario si desea hacer uso del servicio de ubicación y no se muestren los términos de uso y privacidad del mismo (imagen superior izquierda mostrada anteriormente).
339. El registro de Windows Mobile 6.5 almacena la configuración del servicio de ubicación en las siguientes claves del registro. El parámetro “idle\_collection” permite activar el servicio de descarga o recopilación de información de localización, cuando el valor es “1”. El valor asociado a cada programa, por ejemplo “services.exe” (HTC Servicio de ubicación), permite seleccionar qué programas pueden usar el servicio; cuando el valor es “1” el programa está permitido. El parámetro “tos\_accepted” (Terms of Service, ToS) define si la pantalla de aceptación de uso del servicio ha sido aceptada (si el valor es “1”):

```
[HKEY_LOCAL_MACHINE\Software\Google\cll]
"idle_collection"=dword:00000000
"tos_accepted"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\Software\Google\cll\permission list\services.exe]
"services.exe"=dword:00000000
```

Ninguno de estos parámetros tiene un valor por defecto; debe recordarse que el usuario establece su valor según sus preferencias durante el proceso de configuración inicial.

340. La siguiente clave del registro permite configurar si se rechaza el servicio de ubicación automáticamente para todos los programas, no mostrándose el mensaje de aceptación si el valor es “1”:

```
[HKEY_LOCAL_MACHINE\Software\HTC\HTCGeoService]
"DontShowAgreement"=dword:00000001
```

341. El servicio de ubicación de Google, si está activo, es accedido a través de conexiones HTTP (no cifradas) desde el dispositivo móvil hacia “www.google.com” (“/m/appreq/cllwinm”) y envía a Google información de las redes inalámbricas (incluyendo el nombre de red, SSID, y su dirección MAC, BSSID) y de las torres de telefonía disponibles desde el dispositivo móvil.

342. Adicionalmente, la petición incluye información detallada del dispositivo móvil. Por ejemplo, la plataforma (Windows Mobile, “winm” y “Icllwinm”), la versión de SO (“PocketPCv5.2.21869”) y el modelo (“HTC HD2”), el idioma (español, “es”) y el programa que accede al servicio (“services.exe”); ver apartado “4. Entorno de aplicación de esta guía”:

```
Icllwinm,1.0,winm-PocketPC-HTC HD2 T85855.2.21869/Google-hTC,Google-hTC,es ... services.exe
```

343. Estas peticiones de información hacia Google desvelan información de las redes, Wi-Fi y de telefonía, existentes en el área de cobertura del dispositivo móvil, así como otros detalles relevantes del terminal, a cualquiera que esté capturando el tráfico de datos generado desde el dispositivo móvil. Las respuestas, en formato binario, contienen información de la ubicación estimada del dispositivo móvil.

344. El servicio de ubicación de HTC proporciona información de localización a diferentes aplicaciones del terminal en función de la ubicación del dispositivo móvil.

345. El servicio de ubicación de HTC (“HTC Servicio de ubicación”), si está activo y en concreto para la aplicación de “Clima”, realiza peticiones HTTP (no cifradas) desde el dispositivo móvil hacia “htc.accuweather.com” con información de la ubicación actual (latitud y longitud), y recibe la información meteorológica asociada a la ubicación proporcionada.

346. Las actualizaciones de ubicación conllevan una actualización horaria mediante peticiones de información a “time.nist.gov” y “time-nw.nist.gov” (TCP/13), en función de la configuración de sincronización de hora del dispositivo móvil (ver apartado “5.25. Servicios de datos”).

347. Estas peticiones de información meteorológica desvelan la ubicación del dispositivo móvil a cualquiera que esté capturando el tráfico de datos generado desde el mismo:

```
/widget/htc/lat-lon-search.asp?ac=TR9cra0U&lat=-4.35817&lon=55.839357
```

348. Se recomienda limitar el uso de los servicios de localización o ubicación de Google y de HTC, configurables de forma independiente, y necesarios para hacer uso de las capacidades de ubicación asociadas a algunas aplicaciones y programas, pero que pueden desvelar detalles privados de la ubicación del dispositivo móvil (y del tipo de dispositivo).

349. Es posible deshabilitar la funcionalidad encargada de mostrar la información meteorológica (“Clima”) para la ubicación actual del dispositivo móvil (almacenada en el parámetro “Weather.CurLocInfo”) a través de la siguiente clave del registro:

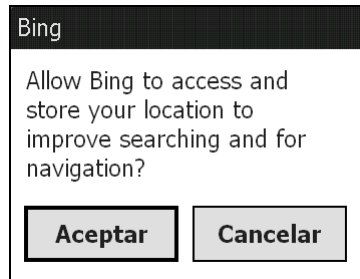
```
[HKEY_CURRENT_USER\Software\HTC\Manila]
"Weather.EnableCurrentLocation"=dword:00000000
```

#### 5.15.4 SERVICIOS DE LOCALIZACIÓN: BING

350. La información de localización de GPS es empleada por los servicios de localización de Bing (buscador de Microsoft), aceptados al confirmar el acuerdo de licencia y uso del

servicio, permitiendo a Microsoft recoger, almacenar y utilizar los datos de localización del dispositivo móvil. Se recomienda evaluar en detalle el uso del cliente Bing y de estos servicios, ya que afectan directamente a la privacidad del usuario.

351. La última versión disponible (Bing Mobile versión 5.1.2010.6280) solicita confirmación del usuario para hacer uso de los servicios de localización la primera vez que se ejecuta:



352. La utilización de los servicios de localización puede ser gestionada a través de la opción de configuración "GPS Tracking" disponible desde el botón "Menu", opción "Settings" (como en otros servicios de localización; ver apartado "5.15. Localización geográfica").
353. Los servicios de localización de Bing generan peticiones HTTP (TCP/80), sin cifrar, hacia el servidor "api.tiles.virtualearth.net".

#### 5.15.5 INFORMACIÓN GEOGRÁFICA EN FOTOGRAFÍAS

354. Windows Mobile 6.5 permite añadir información de la localización geográfica a las fotografías realizadas con la cámara del dispositivo móvil. Al realizar la fotografía se añaden las coordenadas GPS en el momento de tomar la instantánea a la cabecera EXIF de la imagen.
355. Esta funcionalidad puede ser utilizada a través del menú de configuración de la cámara, seleccionando el "Modo Captura" (segundo botón de la izquierda) denominado "Foto GPS", en lugar de la opción "Foto" (estándar).
356. Por defecto, las fotografías tomadas con el dispositivo móvil no incluyen la información del GPS. Es necesario utilizar "Foto GPS", indicado con un icono tras la obtención de coordenadas por el GPS, para almacenar esta información.
357. Se recomienda no hacer uso de la funcionalidad que incluye la información del GPS en fotografías, especialmente para su publicación o distribución, salvo que se quiera hacer uso explícito de estas capacidades. En caso contrario, las imágenes revelarán los detalles exactos de dónde han sido tomadas.
358. Es posible incluso deshabilitar por completo esta funcionalidad ocultando el botón de "Foto GPS" mediante la siguiente clave del registro:

```
[HKEY_LOCAL_MACHINE\Software\HTC\Camera\P10]
"Enable"=dword:00000000
```

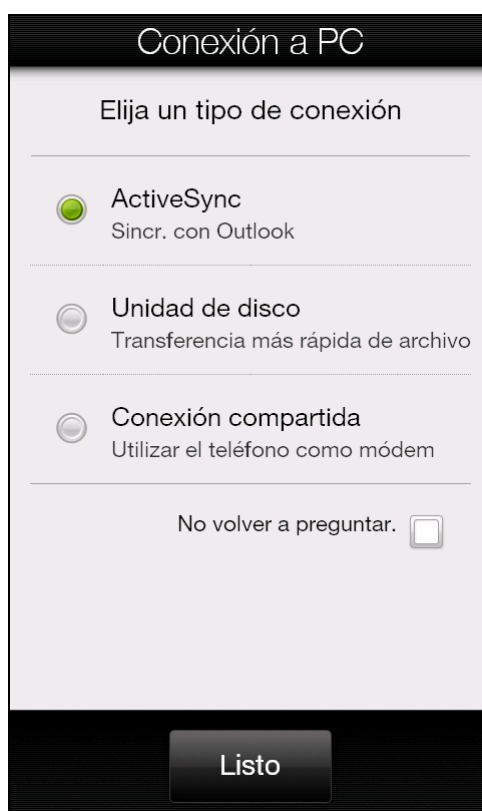
359. Además de la información de localización almacenada en imágenes, la aplicación HTC Footprints (aplicación basada en la localización) permite añadir metadatos adicionales a las fotografías (información extra asociada) y clasificarlas en categorías. Entre los datos que pueden ser vinculados a una fotografía está la ubicación exacta del GPS, zona geográfica, anotaciones, sonidos, número de teléfono, o un sitio web asociado.

360. Se recomienda analizar desde el punto de vista de la privacidad del usuario que tipo de información es añadida a las fotografías, con el objetivo de limitar los detalles facilitados.

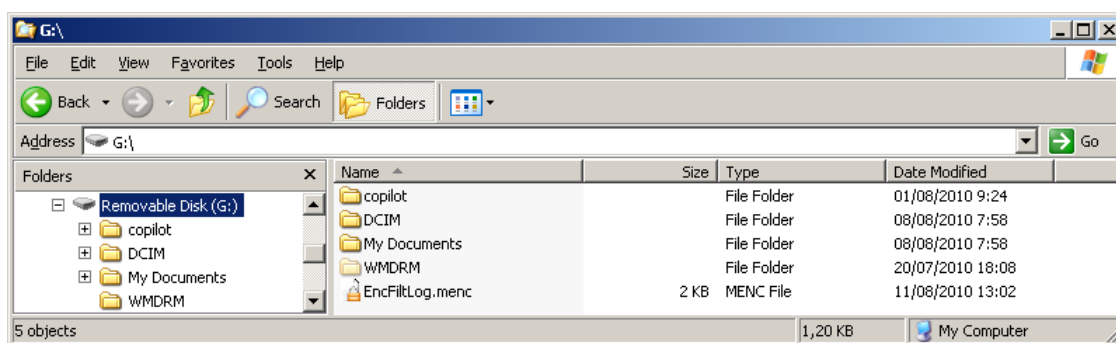
## 5.16 COMUNICACIONES USB

361. La conexión USB del dispositivo móvil a un ordenador proporciona tres funcionalidades o tipos de conexiones diferentes (la opción por defecto mostrada es la utilizada en la última conexión realizada):

- ActiveSync (opción por defecto inicialmente, analizada en detalle en el apartado “5.3. Microsoft ActiveSync”).
- Unidad de disco.
- Conexión compartida, o *tethering*.



362. La opción de unidad de disco, también conocida como modo de almacenamiento USB, permite el acceso a la tarjeta de almacenamiento externa del dispositivo móvil directamente desde el ordenador a través del puerto USB:



363. Debe prestarse especial atención a la configuración de seguridad del ordenador, y en concreto a los mecanismos de auto-ejecución de Windows (*autorun* y *autoplay*), para evitar la propagación de software malicioso (como el troyano Ambler) desde la tarjeta de almacenamiento externa del dispositivo móvil al ordenador [Ref.- 1].
364. La opción de conexión compartida, o *tethering*, permite compartir la conexión de datos de telefonía móvil del terminal con el ordenador. Las recomendaciones de seguridad para esta funcionalidad se describen en el apartado Bluetooth “5.17.9. Red de área Personal (PAN)”, aunque desde el punto de vista de seguridad se recomienda hacer uso de *tethering* mediante USB, en lugar de mediante Bluetooth.

## 5.17 COMUNICACIONES BLUETOOTH

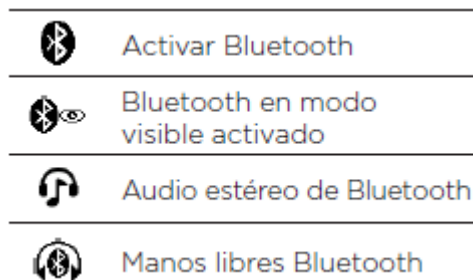
### 5.17.1 DESACTIVACIÓN DE LAS COMUNICACIONES BLUETOOTH

365. La principal recomendación de seguridad asociada a las comunicaciones Bluetooth (802.15) en dispositivos móviles es no activar el interfaz inalámbrico Bluetooth salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Bluetooth, incluyendo los perfiles Bluetooth disponibles [Ref.- 51].
366. El interfaz inalámbrico Bluetooth puede ser desactivado en Windows Mobile 6.5 a través del menú “Inicio – Configuración – Controles inalámbricos” (que proporciona acceso al “Comm Manager”), mediante el botón deslizante de activación y desactivación asociado a la sección “Bluetooth”:



367. El estado del interfaz Bluetooth puede ser verificado de forma rápida y sencilla por el usuario del dispositivo móvil a través de la barra superior de estado.

368. Windows Mobile 6.5 proporciona información en la barra superior de estado sobre el estado del interfaz Bluetooth, su modo (visible u oculto), y el uso de audio estéreo o manos libres Bluetooth, a través del siguiente conjunto de iconos:



**Nota:** el interfaz Bluetooth en Windows Mobile 6.5 no puede ser deshabilitado en tiempo real únicamente a través de la manipulación del registro. Las siguientes cuatro claves del registro forman parte del proceso de desactivación de las capacidades Bluetooth, pero tras aplicarlas, el estado del interfaz sigue siendo activo, tal como muestran tanto el “Comm Manager” como la pestaña de configuración de Bluetooth (analizada posteriormente):

```
[HKEY_CURRENT_USER\Software\Microsoft\Bluetooth\Settings]
"ScanMode"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\General]
"StackMode"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Platform\PowerMode]
"ActiveProfileMask"=dword:80000000
```

```
Cambios de estado en el interfaz Bluetooth: activación, conexión...
Sólo cambia el icono de estado del interfaz Bluetooth en la barra de
título:
```

```
(Su valor es 9 en activo y 8 en inactivo)
```

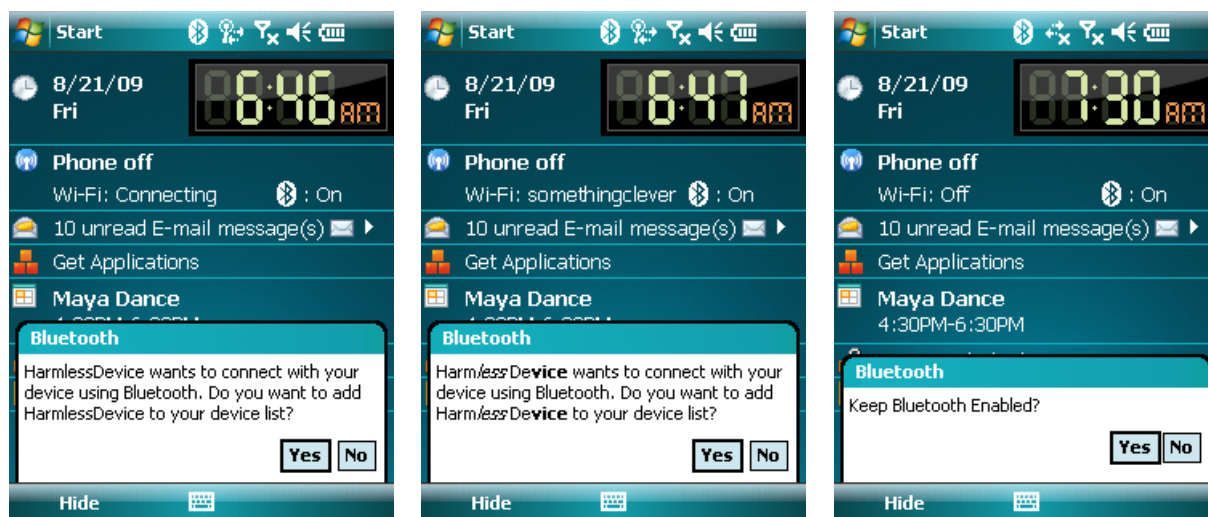
```
[HKEY_LOCAL_MACHINE\System\State\Hardware]
"Bluetooth"=dword:00000008
```

Sin embargo, tras modificar estos valores en el registro y proceder a reiniciar el dispositivo móvil (incluso tras un restablecimiento software o *soft reset*), el interfaz Bluetooth permanecerá deshabilitado.

369. Windows Mobile 6.5 mantiene el estado del interfaz Bluetooth tras reiniciar el dispositivo móvil (incluso tras un restablecimiento de software o *soft reset*), es decir, si el interfaz Bluetooth estaba activo al apagar el terminal, al encender el dispositivo móvil seguirá activo. Sin embargo, la activación inicial del interfaz Bluetooth no se llevará a cabo hasta que se desbloquee por primera vez el dispositivo móvil tras encenderlo (no así el interfaz Wi-Fi; ver apartado “5.17.12. Ataques Blueline”)

370. Windows Mobile emplea el lenguaje HTML (contenidos web) para mostrar los mensajes y avisos de diferentes componentes del interfaz gráfico, incluidas las notificaciones de acceso generadas por el interfaz Bluetooth (ver apartado “5.19.1. Ejecución de contenido web en mensajes de texto”).

371. Cuando los mecanismos de autorización de Bluetooth están activos, el dispositivo solicita confirmación al usuario antes de permitir el acceso desde otros dispositivos, mostrando en la notificación el nombre Bluetooth del otro dispositivo.
372. Debido a la ausencia de mecanismos de validación de dicho nombre, éste puede incluir etiquetas HTML. Pese a que un atacante no puede eliminar la existencia de los botones de confirmación o el título, las etiquetas HTML pueden ser empleadas para desplazar el texto mostrado por defecto en el mensaje de notificación [Ref.- 108]. Este ataque Bluetooth es conocido como Blueline.
373. Mediante el desplazamiento de dicho texto, un atacante puede llevar a cabo ataques de ingeniería social, mostrar en la notificación cualquier mensaje que potencialmente será aceptado positivamente por el usuario, como por ejemplo “¿Desea que el interfaz Bluetooth continúe activo?”.
374. Si el usuario víctima responde afirmativamente a dicho mensaje, estará aceptando la conexión con el dispositivo Bluetooth externo controlado por el atacante.



NOTA: Imágenes de ejemplo obtenidas de “<http://pauldotcom.com/wiki/index.php/Episode209>”.

**Nota:** la existencia de esta vulnerabilidad Blueline en Windows Mobile está condicionada a las capacidades añadidas por ciertos fabricantes de dispositivos móviles. Si las capacidades de notificación existentes por defecto en el interfaz gráfico de Bluetooth en Windows Mobile han sido reemplazadas por el fabricante, la vulnerabilidad podría ser eliminada o incluso ser más crítica, permitiendo ataques de Cross-Site Scripting (XSS).

En el caso del dispositivo móvil empleado como referencia en la presente guía, la vulnerabilidad no está presente, ya que HTC proporciona un subsistema de notificaciones propietario que no interpreta el nombre de otros dispositivos Bluetooth como HTML.

### 5.17.2 DOS EN EL NOMBRE BLUETOOTH

375. Windows Mobile 6 es vulnerable frente a una denegación de servicio (DoS) asociada al procesamiento de nombres Bluetooth malformados de otros dispositivos.

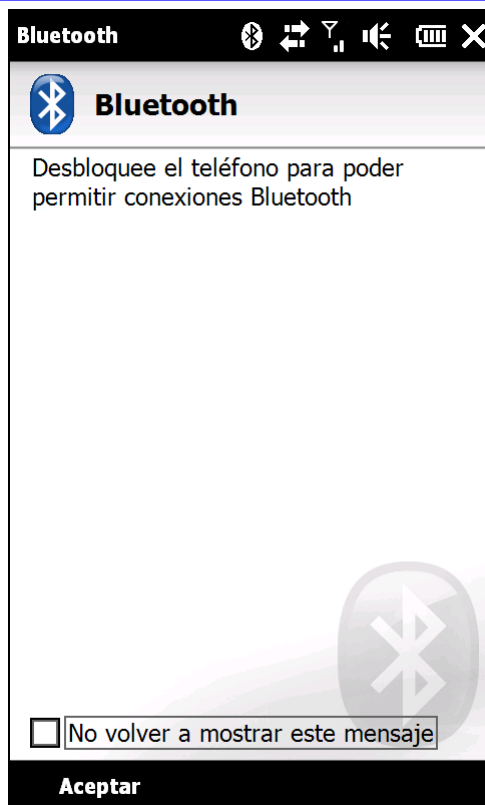
376. En septiembre de 2008 [Ref.- 109] se anunció la vulnerabilidad en el driver de Bluetooth, indicando que tras la recepción de un nombre Bluetooth de elevada longitud (por ejemplo, 248 caracteres, el máximo definido por la especificación Bluetooth), el dispositivo móvil fallará y se reiniciará.
377. La vulnerabilidad puede ser explotada tanto durante el proceso de descubrimiento de otros dispositivos, como al recibir conexiones de otros dispositivos Bluetooth.
378. En el momento de elaboración de la presente guía no hay disponible ninguna actualización que resuelva esta vulnerabilidad.

**Nota:** el dispositivo móvil empleado como referencia en la presente guía no es vulnerable a esta denegación de servicio en el nombre Bluetooth.

379. Comunicaciones Wi-Fi”).
380. Igualmente, al salir del modo de vuelo el estado del interfaz Bluetooth será restaurado, activándose en el caso de haber estado activo previamente (al activar el modo de vuelo).
381. El interfaz Bluetooth permanece activo cuando el dispositivo móvil está en espera o *stand-by*, es decir, encendido pero con la pantalla apagada y bloqueado.

**Nota:** tras un restablecimiento de fábrica, o *hard-reset*, el dispositivo móvil empleado para la elaboración de la presente guía no responde a peticiones SDP ni a intentos de conexión en los diferentes perfiles Bluetooth. La activación completa de la pila Bluetooth se lleva a cabo tras cambiar a modo visible y recibir una petición SDP o intento de conexión a uno de los perfiles en ese estado. Por tanto, si el dispositivo móvil nunca cambia a modo visible no podrá recibir ataques a través de Bluetooth.

382. El bloqueo del teléfono constituye un primer nivel de protección frente a las conexiones Bluetooth entrantes, ya que pese a estar el interfaz Bluetooth activo, no se aceptarán conexiones en ese estado, generándose el siguiente mensaje de advertencia para el usuario:



383. La dirección de Bluetooth, BD\_ADDR (*Bluetooth Device Address*) está disponible a través del menú “Inicio – Configuración – Acerca del teléfono – Información de hardware”, y en concreto, en el campo “Dirección Bluetooth”:



384. Adicionalmente, el campo “Versión Bluetooth” proporciona los detalles de la versión de la especificación Bluetooth soportada por el dispositivo móvil, por ejemplo, “2.1+EDR”.

**Nota:** el dispositivo móvil empleado para la elaboración de la presente guía hace uso de la pila de comunicaciones Bluetooth WIDCOMM (Broadcom), en lugar de emplear la pila de Microsoft. Por tanto, algunas de las recomendaciones de seguridad descritas en esta sección, especialmente referencias a claves del registro, podrían variar para aquellos dispositivos móviles basados en Windows Mobile 6.5 que hacen uso de la pila Bluetooth de Microsoft.

385. La dirección Bluetooth del dispositivo móvil se almacena en tres claves del registro, en formato hexadecimal (REG\_BINARY):

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\General]
"BDAddr"=hex:\
 00,23,76,01,02,03

[HKEY_LOCAL_MACHINE\Software\WIDCOMM\Version]
"BDAddress"=hex:\
 00,23,76,01,02,03

[HKEY_LOCAL_MACHINE\Software\OEM\Bluetooth]
"BTAddress"=hex:\
 00,23,76,01,02,03
```

**Nota:** la parte de la dirección Bluetooth (BD\_ADDR) asociada al fabricante, NAP+UAP, puede permitir identificar el tipo de dispositivo móvil. En el ejemplo analizado, el valor “00:23:76” está asignado por el IEEE (<http://standards.ieee.org/regauth/oui/index.shtml>) a “HTC”:

|                  |                           |
|------------------|---------------------------|
| 00-23-76 (hex)   | HTC Corporation           |
| 002376 (base 16) | HTC Corporation           |
|                  | No.23 Hsin Hua Rd.        |
|                  | Taoyuan Taiwan 330        |
|                  | TAIWAN, REPUBLIC OF CHINA |

### 5.17.3 DISPOSITIVOS BLUETOOTH EMPAREJADOS

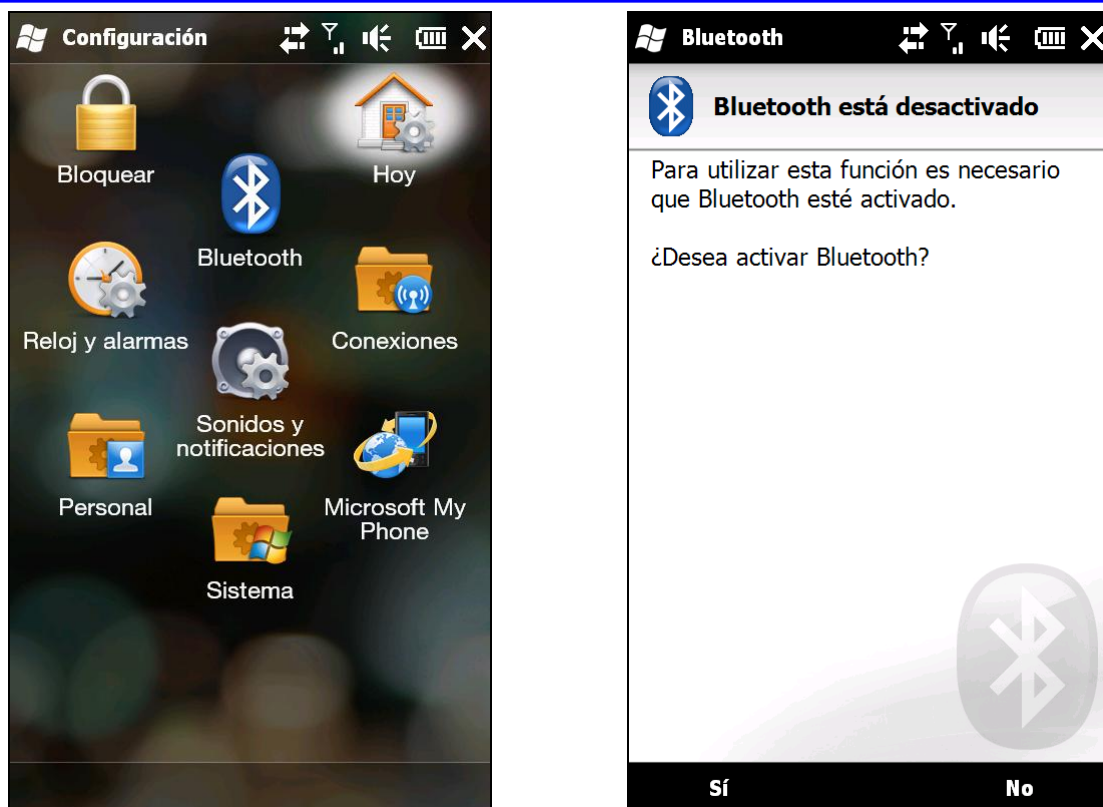
386. A través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, el icono “Bluetooth” permite gestionar y configurar el interfaz Bluetooth, comenzando por la visualización de la lista de dispositivos emparejados (y sus perfiles asociados – seleccionados durante el emparejamiento), pudiendo agregar nuevos dispositivos a la lista desde la pestaña central (mostrada por defecto de entre las tres pestañas disponibles):



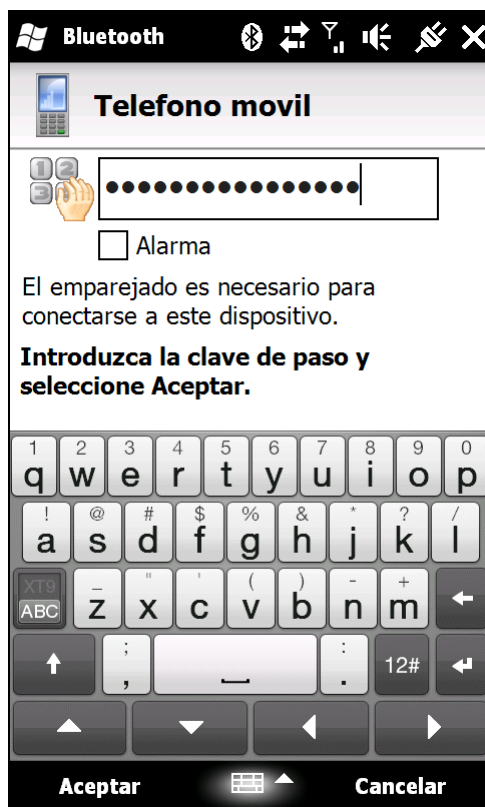
387. Los perfiles de los otros dispositivos Bluetooth registrados durante el emparejamiento con el dispositivo móvil (imagen superior derecha), denominados conexiones en nomenclatura Microsoft, están definidos en la siguiente clave del registro, junto a los mecanismos de seguridad a emplear (autenticación, autorización y cifrado):

HKEY\_LOCAL\_MACHINE\Software\WIDCOMM\Connections

388. Debe tenerse en cuenta que para poder llevar a cabo la configuración de la pila de comunicaciones Bluetooth a través del interfaz de usuario del dispositivo móvil es obligatorio activar el interfaz, como se muestra en la siguiente imagen, por lo que se recomienda activar el interfaz y realizar las modificaciones de la configuración en un entorno seguro, o en su defecto, llevar a cabo los cambios de configuración a través del registro de Windows Mobile 6.5, para evitar potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados:



389. Windows Mobile 6.5 permite la utilización de claves de paso o PIN Bluetooth formados por caracteres alfanuméricos y símbolos, de hasta 16 caracteres de longitud, durante el emparejamiento con otros dispositivos (tal como define la especificación Bluetooth):



390. Se recomienda hacer uso de contraseñas alfanuméricas robustas para el emparejamiento con otros dispositivos Bluetooth (compuestas por números, letras y símbolos, y de al menos 8 caracteres), en lugar de emplear un PIN de cuatro dígitos (valor común por defecto y empleado de forma estándar en el emparejamiento de dispositivos Bluetooth).
391. Para cada dispositivo con el que se ha realizado el emparejamiento, es posible obtener su dirección Bluetooth (BD\_ADDR), muy útil a la hora de reconocer otros dispositivos asociados al terminal, así como modificar el nombre empleado para identificarlos en el dispositivo móvil y determinar si las conexiones con el dispositivo móvil están autorizadas, a través de la opción “Conexiones autorizadas”. Estas opciones están disponibles a través del botón “Propiedades” (abajo a la izquierda) de la pestaña central que muestra la lista de dispositivos emparejados:

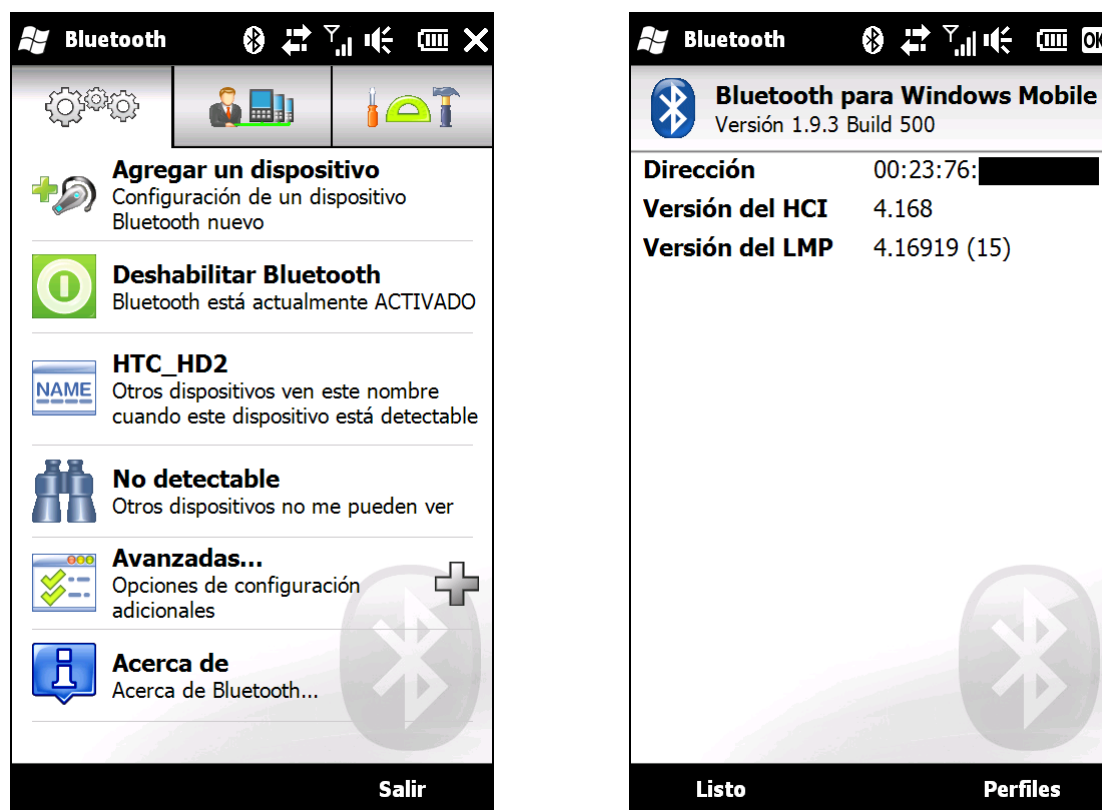


392. Se recomienda no seleccionar la opción de “Conexiones autorizadas” para ninguno de los dispositivos emparejados con el dispositivo móvil.
393. La opción de “Conexiones autorizadas” es analizada en detalle en el apartado “5.17.6. OBEX File Transfer”, al estar relacionada con la opción “Acepte todas las conexiones que provengan de este dispositivo” de los mensajes de autorización mostrados durante el establecimiento de conexiones Bluetooth. Este parámetro define el nivel de autorización otorgado a otros dispositivos Bluetooth y gestiona las notificaciones que son mostradas al usuario para solicitar confirmación de las operaciones realizadas a través de Bluetooth.

#### 5.17.4 CONFIGURACIÓN GENERAL DE BLUETOOTH

394. La pestaña de configuración de la izquierda (imagen inferior izquierda) permite múltiples acciones, como agregar nuevos dispositivos (al igual que la pestaña central), habilitar y deshabilitar el interfaz Bluetooth, configurar el nombre del dispositivo móvil empleado para las conexiones Bluetooth, configurar el estado del interfaz Bluetooth (oculto o

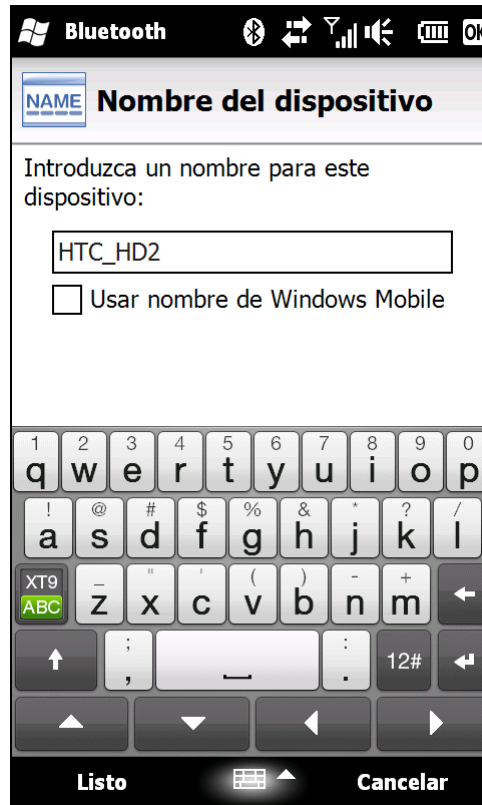
visible), además de otras tareas avanzadas y poder obtener información detallada del interfaz Bluetooth y versiones (imagen inferior derecha). Aquellas acciones con implicaciones de seguridad son analizadas a continuación:



395. Los detalles de versiones de la pila de comunicaciones Bluetooth y de los componentes HCI y LMP están disponibles en los parámetros de la siguiente clave del registro:

```
HKEY_LOCAL_MACHINE\Software\WIDCOMM\Version
```

396. El nombre empleado por el dispositivo móvil para las conexiones Bluetooth (modificable a través de la tercera opción de la pestaña de configuración) puede ser igual al nombre del dispositivo móvil (parámetro "Usar nombre de Windows Mobile") o diferente:

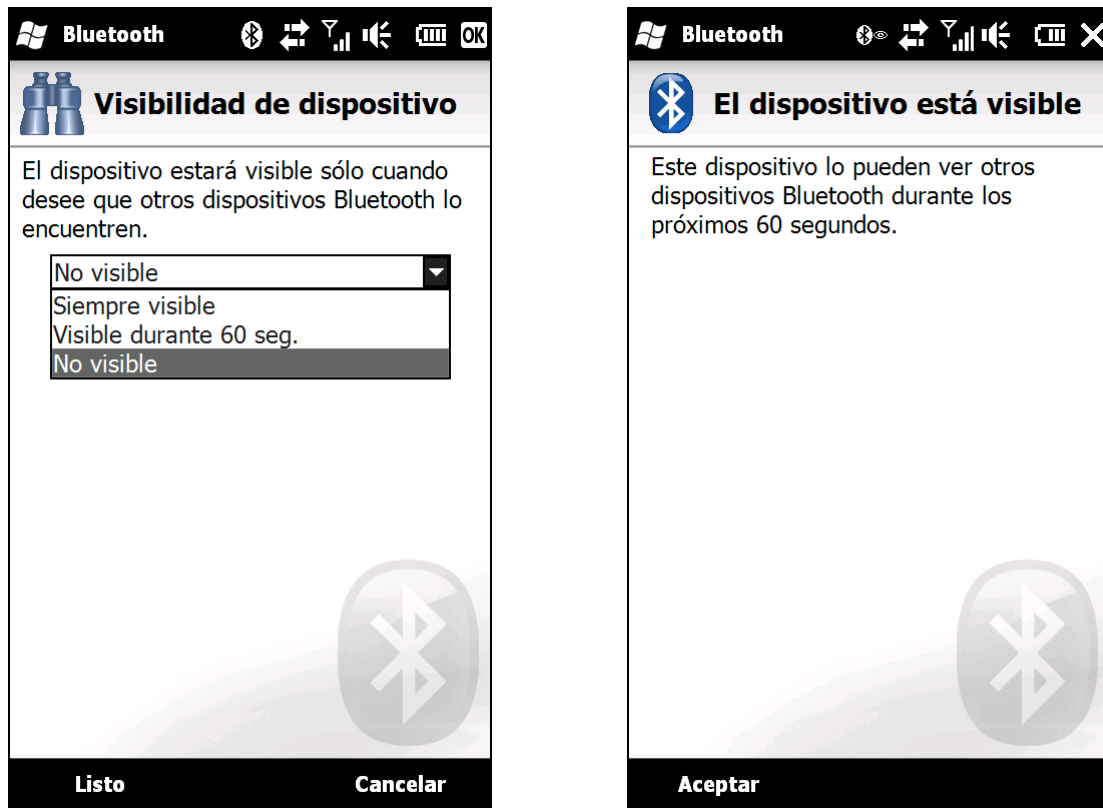


397. En caso de ser igual, el nombre del dispositivo móvil almacenado en la clave del registro “HKEY\_LOCAL\_MACHINE\Ident\Name” (ver apartado “5.14. Configuración por defecto del dispositivo móvil”), es copiado automáticamente a la clave del registro especificada a continuación. En caso de ser diferente, el nombre del dispositivo móvil empleado por las tecnologías Bluetooth se almacena en la siguiente clave del registro

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\General]
"DeviceName"="bt0001"
```

398. Se recomienda modificar el nombre configurado por defecto (ej. “HTC\_HD2”) con el objetivo de no desvelar información sobre su propietario o la marca y modelo del dispositivo móvil (ej. “bt0001”).
399. Adicionalmente, se recomienda emplear un nombre para el dispositivo móvil (por ejemplo, “dm0001”) y otro distinto para las conexiones Bluetooth (por ejemplo, “bt0001”), con el objetivo de no desvelar a través de Bluetooth el nombre real del dispositivo móvil, que podría ser usado para otro tipo de comunicaciones, como las comunicaciones en redes Microsoft (ver apartado “5.14. Configuración por defecto del dispositivo móvil”).
400. En el caso de activar el interfaz Bluetooth para hacer uso de esta tecnología, se recomienda configurar el mismo en modo oculto o no visible, con el objetivo de no desvelar su presencia frente a las operaciones de búsqueda de otros dispositivos Bluetooth.
401. Para ello, desde la pestaña de configuración de la izquierda (accesible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Bluetooth”) debe seleccionarse la cuarta opción. Por defecto, al activar el interfaz Bluetooth éste se encuentra en modo oculto o no visible, estado identificado por el texto “No detectable” (opción recomendada desde el punto de vista de seguridad). El interfaz

Bluetooth puede configurarse adicionalmente en estado visible permanente (estado identificado por el texto “Detectable”), o visible únicamente durante el próximo minuto (60 segundos) tras seleccionar esta opción:



402. La siguiente clave del registro define el estado del interfaz Bluetooth, oculto (valor igual a “0” y recomendado) o visible (valor igual a “1”):

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Filters]
"AllowOthersToDiscover"=dword:00000000
```

**Nota:** la política de seguridad 4135 (0x00001027), bajo la rama del registro [HKEY\_LOCAL\_MACHINE\Security\Policies\Policies], determina si el dispositivo móvil puede ser utilizado en modo visible (“1”) u oculto (“0”) para ser buscado por otros dispositivos. Si se selecciona la opción “0” (oculto), el usuario no podrá activar la visibilidad del terminal a otros dispositivos.

403. Al encontrarse el interfaz Bluetooth del dispositivo móvil en modo oculto, todas las conexiones Bluetooth y operaciones de emparejamiento con otros dispositivos deberán iniciarse desde el dispositivo móvil, siendo necesario que el otro dispositivo Bluetooth se encuentre en modo visible.

**Nota:** en el caso de requerir, de forma excepcional, disponer del interfaz Bluetooth en modo visible para realizar el emparejamiento con otro dispositivo, siempre debería usarse la opción “Visible durante 60 seg.”, y en ningún caso la opción “Siempre visible”, con el objetivo de volver al estado oculto tras la operación de emparejamiento.

### 5.17.5 CONFIGURACIÓN AVANZADA DE BLUETOOTH

404. Las opciones de configuración avanzadas, identificadas por el botón desplegable “Avanzadas” (quinta opción de la pestaña de configuración), permiten establecer restricciones de conectividad, obtener información de los puertos serie empleados, y configurar opciones de transferencia de archivos, el audio en dispositivos manos libres, el intercambio de objetos y el perfil de acceso a la tarjeta SIM. A continuación se detallan aquellas opciones de configuración avanzadas con implicaciones de seguridad.
405. La configuración de qué dispositivos pueden establecer conexiones con el dispositivo móvil está disponible a través de las opciones “Avanzadas” de configuración, y en concreto, de la opción “Conectividad”:



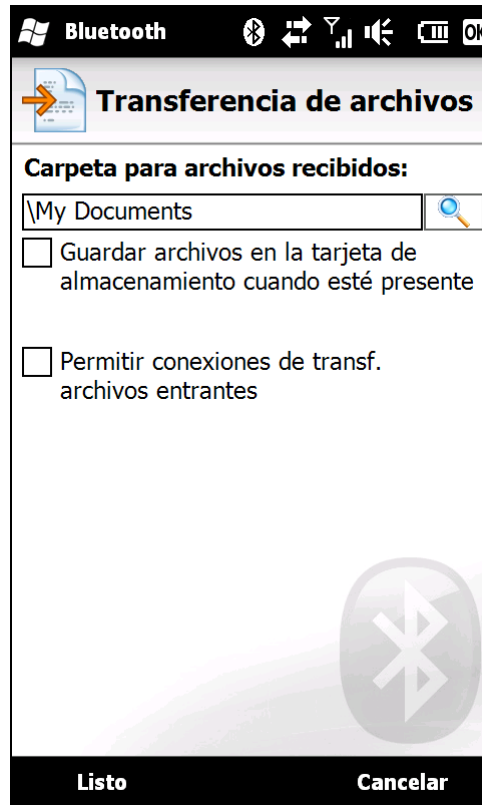
406. Es posible habilitar la posibilidad de aceptar conexiones desde cualquier dispositivo (opción por defecto), o sólo desde aquellos dispositivos indicados en “Mis dispositivos”. La lista de “Mis dispositivos” referencia a todos aquellos dispositivos Bluetooth que han sido emparejados con el dispositivo móvil previamente (disponibles en la pestaña central de Bluetooth, analizada anteriormente).
407. La siguiente clave del registro define qué dispositivos se pueden conectar al terminal. El valor de “WhoAllowedToConnect” puede ser “1” (valor por defecto), indicando que cualquiera puede conectarse, ó “2”, indicando que sólo pueden hacerlo los dispositivos disponibles en “Mis dispositivos”:
- ```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Filters]
"WhoAllowedToConnect"=dword:00000002
```
408. Se recomienda habilitar la opción que sólo permite conexiones desde los dispositivos indicados en “Mis dispositivos”, es decir, previamente emparejados. Esta restricción implica que si un dispositivo Bluetooth no ha sido emparejado previamente con Windows Mobile 6.5, los intentos de conexión a cualquiera de los perfiles Bluetooth del dispositivo

- móvil serán rechazados. Este mecanismo de seguridad es aplicado antes de los mecanismos de seguridad particulares de cada perfil de Bluetooth.
409. En caso de no habilitar la restricción, los intentos de conexión a un perfil Bluetooth que requiere autenticación (mecanismo de seguridad analizado posteriormente en el apartado “5.17.6. OBEX File Transfer”) desencadenan el proceso de emparejamiento que, una vez completado, permite continuar con la conexión original asociada al perfil. Los intentos de conexión sobre perfiles que no requieren autenticación serán permitidos directamente.
410. En caso de habilitar la restricción, los intentos de emparejamiento originados desde cualquier dispositivo Bluetooth hacia Windows Mobile 6.5 también serán rechazados, no siendo posible establecer ninguna comunicación desde dispositivos desconocidos. En este escenario, para iniciar el emparejamiento desde un nuevo dispositivo Bluetooth es necesario desactivar la restricción temporalmente, o iniciar el emparejamiento desde Windows Mobile 6.5 hacia el otro dispositivo (opción recomendada).
411. Las opciones de configuración avanzadas de los perfiles de transferencia de archivos son analizadas en detalle posteriormente en el apartado “5.17.6. OBEX ”, mientras que las del perfil de intercambio de objetos se analizan en el apartado “5.17.7. OBEX Object Push”, las de audio en el apartado “5.17.8. Manos libres Bluetooth” y las de el perfil de acceso a la tarjeta SIM en el apartado “5.17.9. SAP: SIM Access Profile”.

5.17.6 OBEX FILE TRANSFER (Y MECANISMOS DE SEGURIDAD)

412. El menú de configuración de transferencia de archivos, asociadas al perfil Bluetooth estándar *OBEX File Transfer*, u OBEX FTP, permite especificar la carpeta en la que se copiarán los archivos recibidos mediante Bluetooth, por defecto “\My Documents” (carpeta por defecto), así como la posibilidad de guardar los archivos en una tarjeta de almacenamiento externa si está presente, y definir si se permiten conexiones entrantes de transferencia de archivos (deshabilitada por defecto):

Nota: el menú de configuración de transferencia de archivos está ubicado en las opciones de configuración avanzadas de Bluetooth, quinta opción de la pestaña de configuración de Bluetooth de la izquierda, accesible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Bluetooth”.



413. Las claves del registro asociadas a los perfiles Bluetooth (o servicios, en nomenclatura Microsoft) de transferencia de archivos, donde se definen los diferentes parámetros de configuración mencionados, están asociadas tanto al perfil “OBEX Object Push” (0002) como al perfil “File Transfer” (0003), correspondiente al perfil Bluetooth estándar “OBEX File Transfer”, ambos ubicados bajo la siguiente clave del registro:

```
HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services
```

414. El permitir conexiones de transferencia de archivos entrantes (es decir, habilitar el perfil OBEX FTP) está definido por la siguiente clave del registro, que afecta únicamente al servicio “File Transfer” (0003). El parámetro de configuración “Auto” activa o desactiva el perfil OBEX FTP, con un valor de “1” si se permiten las conexiones y de “0” (valor por defecto) si no se permiten:

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services\0003]
"Name"="File Transfer"
"Auto"=dword:00000000
```

Nota: los dispositivos móviles que hacen uso de la pila Bluetooth de Microsoft pueden deshabilitar las capacidades de OBEX a través de la siguiente clave del registro (<http://msdn.microsoft.com/en-us/library/aa916361.aspx>):

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Obex
"IsEnabled"=dword:00000000
```

415. La carpeta definida en el interfaz de usuario para almacenar los archivos recibidos se refleja en las dos siguientes claves del registro (por defecto, “My Documents”):

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services\0002]
"InboxDirectory"="\My Documents"
"Name"="OBEX Object Push"
```

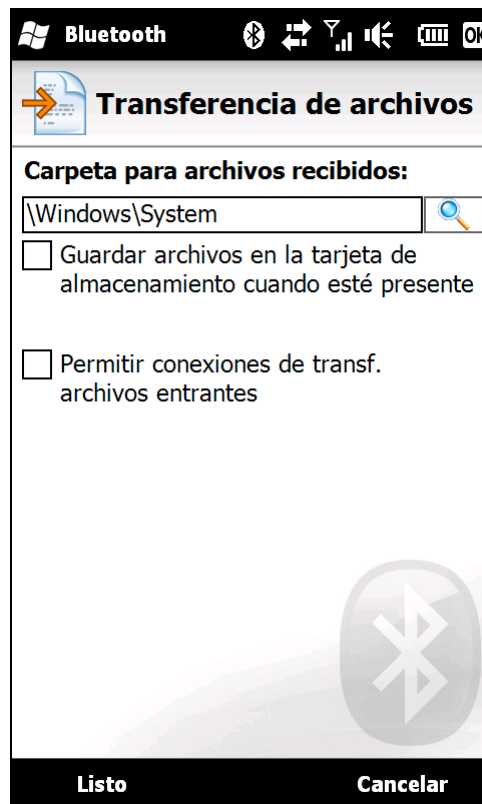
```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services\0003]
"Root"="\My Documents"
"Name"="File Transfer"
```

416. La preferencia de almacenar los archivos en una tarjeta de almacenamiento externa si está presente (asociada al valor “1”) viene definida por las siguientes dos claves del registro (no existentes por defecto hasta que se activa el perfil OBEX FTP):

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services\0002]
"Name"="OBEX Object Push"
"PreferStorageCardForFTP"=dword:00000001

[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services\0003]
"Name"="File Transfer"
"PreferStorageCardForFTP"=dword:00000001
```

417. Desde el punto de vista de seguridad se recomienda dejar las opciones disponibles por defecto, salvo que se quiera almacenar los archivos recibidos en otra carpeta o en una tarjeta de almacenamiento externa y, principalmente, con el perfil deshabilitado.
418. Debe prestarse especial atención a la carpeta especificada para la transferencia de archivos, ya que la pila de comunicaciones Bluetooth WIDCOMM no impone ninguna restricción sobre la misma, siendo posible seleccionar cualquier carpeta del dispositivo móvil, como por ejemplo “\Windows\System”. Un potencial atacante podría disponer de acceso a la totalidad del sistema de ficheros de Windows Mobile 6.5, y por tanto, a todos los archivos e información almacenada en el dispositivo móvil:



419. En el caso de requerir permitir conexiones entrantes de transferencia de archivos, se recomienda habilitar el perfil temporalmente, para volver a deshabilitarlo una vez se ha completado la transferencia. Para ello no es necesario reiniciar el interfaz Bluetooth, sino que basta con habilitar la opción de configuración y pulsar el botón “Listo”.

420. La pila de comunicaciones Bluetooth WIDCOMM, empleada por el dispositivo móvil utilizado para la elaboración de la presente guía, ofrece diferentes niveles de seguridad para los perfiles Bluetooth disponibles según la especificación Bluetooth estándar: autenticación, autorización y cifrado. Otras pilas de comunicaciones Bluetooth, como la de Microsoft, pueden presentar un comportamiento diferente desde el punto de vista de seguridad [Ref.- 52].

Nota: las modificaciones de los mecanismos de seguridad de Bluetooth (autenticación, autorización y cifrado) a través del registro requieren reiniciar el interfaz Bluetooth para que los cambios sean aplicados sobre los perfiles.

421. Por ejemplo, el perfil OBEX FTP dispone de los tres mecanismos de seguridad habilitados por defecto (ver apartado “5.17.11. Otros perfiles Bluetooth”).

422. Los intentos de conexión a un perfil Bluetooth que requiere autenticación llevan implícita la verificación de emparejamiento del dispositivo Bluetooth que origina la petición con Windows Mobile 6.5, es decir, se comprueba que la petición se origina desde un dispositivo previamente emparejado. En caso de no haber sido emparejado anteriormente, el intento de conexión desencadena automáticamente el proceso de emparejamiento que, una vez completado, permite continuar con la conexión original al perfil.

423. La siguiente clave del registro, asociada al perfil OBEX FTP tomado como ejemplo, define si el mecanismo de autenticación es requisito para establecer conexiones con este perfil:

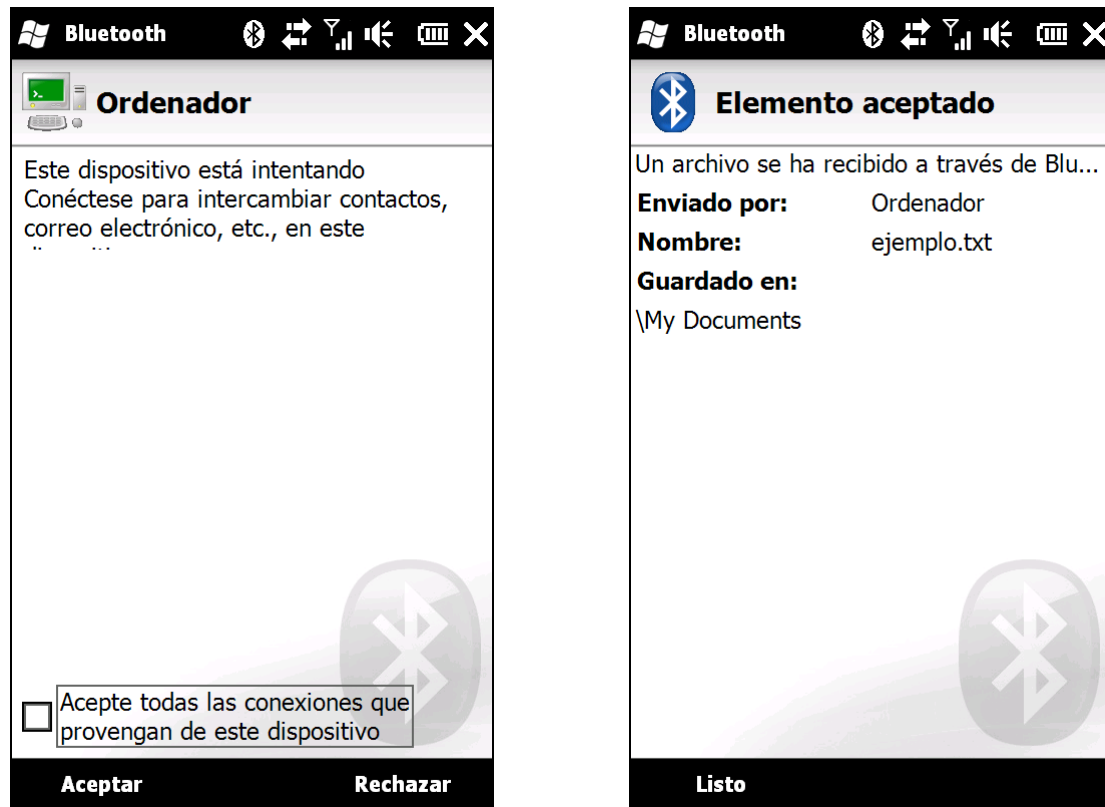
```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services\0003]
"Name"="File Transfer"
"Authentication"=dword:00000001
```

424. Por otro lado, es posible definir si se habilita un mecanismo de autorización para el perfil, de forma que cada vez que se realice un intento de conexión al perfil, el dispositivo móvil muestre un aviso para que el usuario autorice dicha conexión.

425. La siguiente clave del registro, asociada al perfil OBEX FTP tomado como ejemplo, define si el mecanismo de autorización es requisito para establecer conexiones con este perfil:

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services\0003]
"Name"="File Transfer"
"Authorization"=dword:00000001
```

426. Durante la transferencia de archivos entrantes a través de Bluetooth, por defecto, el dispositivo móvil solicita autorización (o confirmación) al usuario para que el intercambio de información se lleve a cabo (imagen inferior izquierda). El dispositivo móvil solicitará autorización cada vez que se intercambie un fichero, indicando el dispositivo Bluetooth involucrado en el título de la pantalla, y generará un mensaje de confirmación de la transferencia en el caso de realizarse con éxito (imagen inferior derecha):



Nota: el mensaje de confirmación de transferencia generado tras el intercambio de datos es muy útil desde el punto de vista de seguridad para que el usuario tenga constancia de que la transferencia ha tenido éxito, incluyendo todos sus detalles. El mensaje permanece en pantalla hasta que el usuario pulsa el botón “Listo”.

Sin embargo, si mientras el mensaje permanece en pantalla el usuario recibe otra transferencia desde el mismo o desde otro dispositivo Bluetooth, el mensaje se perderá y únicamente se mostrará en pantalla el mensaje asociado a la última transferencia realizada. La ausencia de capacidades para almacenar todos los mensajes de transferencia realizados, esperando la aceptación por parte del usuario de cada uno de ellos, es una limitación significativa de la funcionalidad de notificación de Bluetooth de Windows Mobile 6.5. Esta situación se presenta tanto si se aceptan, como si no, todas las conexiones del dispositivo que realiza la transferencia (opción analizada a continuación).

427. Por último, el tercer mecanismo de seguridad disponible para los perfiles Bluetooth es el de cifrado, asociado al modo de seguridad 3 de la especificación Bluetooth, que requiere que todas las transferencias de datos desde y hacia el perfil se cifren a nivel de enlace (LMP) para protegerlas frente a la captura de las comunicaciones Bluetooth por parte de un potencial atacante [Ref.- 51].

428. La siguiente clave del registro, asociada al perfil OBEX FTP tomado como ejemplo, define si el mecanismo de cifrado es requisito para establecer conexiones con este perfil:

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services\0003]
"Name"="File Transfer"
"Encryption"=dword:00000001
```

429. Los mecanismos de autenticación, autorización y cifrado en la pila de comunicaciones Bluetooth WIDCOMM son independientes, pudiendo habilitarse y deshabilitarse por separado para cada uno de los perfiles disponibles.

Nota: en resumen, si un perfil tiene habilitado el mecanismo de autenticación, será necesario disponer de (o establecer) un emparejamiento con el otro dispositivo (imagen inferior izquierda); si tiene habilitado el mecanismo de autorización, se mostrará un mensaje de confirmación al usuario (imagen inferior derecha); y si tiene habilitado el mecanismo de cifrado, será también necesario disponer de (o establecer) un emparejamiento con el otro dispositivo (imagen inferior izquierda), al emplearse las claves de enlace del emparejamiento para cifrar los datos transmitidos:



430. Por otro lado, se recomienda no seleccionar la opción “Acepte todas las conexiones que provengan de este dispositivo” disponible en la parte inferior del mensaje de autorización (o confirmación) mostrado durante la transferencia de datos o acceso al perfil (sólo cuando el mecanismo de autenticación está también habilitado), con el objetivo de recibir siempre notificación de las operaciones realizadas a través de Bluetooth, incluso con dispositivos de confianza ya emparejados (autenticados), ya que hay escenarios dónde éstos podrían ser suplantados por un potencial atacante [Ref.- 51].
431. Se recomienda, por tanto, no aceptar de forma permanente todas las conexiones para ninguno de los dispositivos Bluetooth con los que se ha emparejado el dispositivo móvil, equivalente a deshabilitar el mecanismo de autorización para un dispositivo concreto.
432. Incluso en el caso de haber seleccionado la opción para aceptar todas las conexiones provenientes de un dispositivo, se generará el mensaje de confirmación de la transferencia si ésta se realiza con éxito, avisando al usuario de dicha operación.

Desafortunadamente, en este escenario, el fichero ya habría sido transferido al dispositivo móvil (pudiendo haber explotado una vulnerabilidad en el terminal).

433. La siguiente clave del registro especifica si se aceptan todas las conexiones que provengan de un dispositivo específico con el que se ha emparejado Windows Mobile 6.5. La clave del registro incluye la dirección Bluetooth (BD_ADDR) del dispositivo emparejado con el dispositivo móvil (por ejemplo, 00:10:60:05:06:07). El valor de "Trusted Mask" es "0" si no se confía en el otro dispositivo y se desea mostrar el mensaje de confirmación al usuario y "0xFFFFFFFF" si se aceptan todas las conexiones que provengan de este dispositivo:

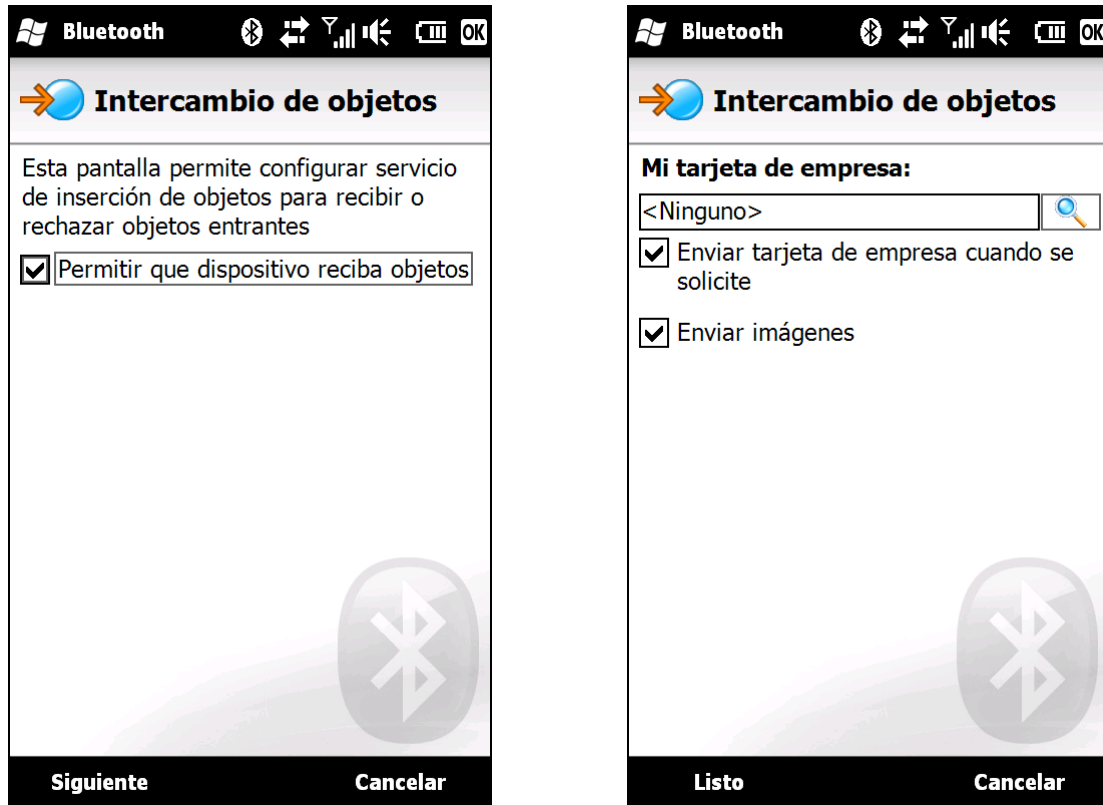
```
[HKLM\Software\WIDCOMM\BTConfig\Devices\00:10:60:05:06:07]
"TrustedMask"=dword:00000000
```

434. Si por error se aceptaron todas las conexiones asociadas a un dispositivo, se recomienda modificar la clave del registro y fijar su valor a "0". Para que el cambio de configuración surta efecto, es necesario deshabilitar y volver a habilitar el interfaz Bluetooth en el dispositivo móvil.
435. Adicionalmente es posible revocar (o habilitar) la autorización de todas las conexiones con un dispositivo Bluetooth concreto a través del botón "Propiedades" disponible en la pestaña central que muestra la lista de dispositivos emparejados (ver apartado "5.17.3. Dispositivos Bluetooth emparejados").

5.17.7 OBEX OBJECT PUSH

436. El menú de configuración de intercambio (o inserción) de objetos, asociadas al perfil Bluetooth estándar *OBEX Object Push*, define si se permite la recepción de objetos (OBEX, *Object Exchange*) a través de Bluetooth, opción habilitada por defecto, y (tras pulsar el botón "Siguiente") la ubicación de la tarjeta de empresa (o negocios) del usuario, si ésta será enviada automáticamente al ser solicitada y si se permite el envío de imágenes:

Nota: el menú de configuración de intercambio de objetos está ubicado en las opciones de configuración avanzadas de Bluetooth, quinta opción de la pestaña de configuración de Bluetooth de la izquierda, accesible a través del menú "Inicio – Configuración", mediante el botón "Menú" y la opción "Más", y el icono "Bluetooth".



437. Se recomienda deshabilitar la recepción de objetos a través de Bluetooth, así como el resto de opciones mencionadas (todas ellas habilitadas por defecto), salvo que se quiera hacer uso explícito de esta funcionalidad.
438. En el caso de requerir permitir conexiones entrantes de intercambio de objetos, se recomienda habilitar el perfil temporalmente, para volver a deshabilitarlo una vez se ha completado el intercambio. Para ello no es necesario reiniciar el interfaz Bluetooth, sino que basta con habilitar la opción de configuración y pulsar el botón “Siguiente - Listo”.
439. El perfil OBEX Object Push se activa (valor igual a “1”) y desactiva (valor igual a “0”) mediante la siguiente clave del registro (parámetro “Auto”). El resto de parámetros especifican la tarjeta de empresa a enviar (“DefaultBusinessCard”), su envío si se solicita (“SendBusinessCardOnRequest”) y si se envían imágenes (“PictureHandling”, con valor “3” si está activo y “0” si no lo está):
- ```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services\0002]
"Name"="OBEX Object Push"
"Auto"=dword:00000000
"DefaultBusinessCard"="80000001"
"SendBusinessCardOnRequest"=dword:00000000
"PictureHandling"=dword:00000000
```
440. El perfil OBEX Object Push no dispone del mecanismo de autenticación habilitado por defecto en el registro (ver apartado “5.17.11. Otros perfiles Bluetooth”), debido a su modelo de uso, en el que no es necesario emparejarse con el otro dispositivo para transferir datos. Sin embargo, en la implementación del dispositivo móvil empleado para la elaboración de la presente guía, los intentos de conexión sí requieren llevar a cabo el emparejamiento con el otro dispositivo.
441. Si se activa el mecanismo de autenticación en el perfil OBEX Object Push a través de la siguiente clave del registro, forzando teóricamente a que sea necesario realizar un

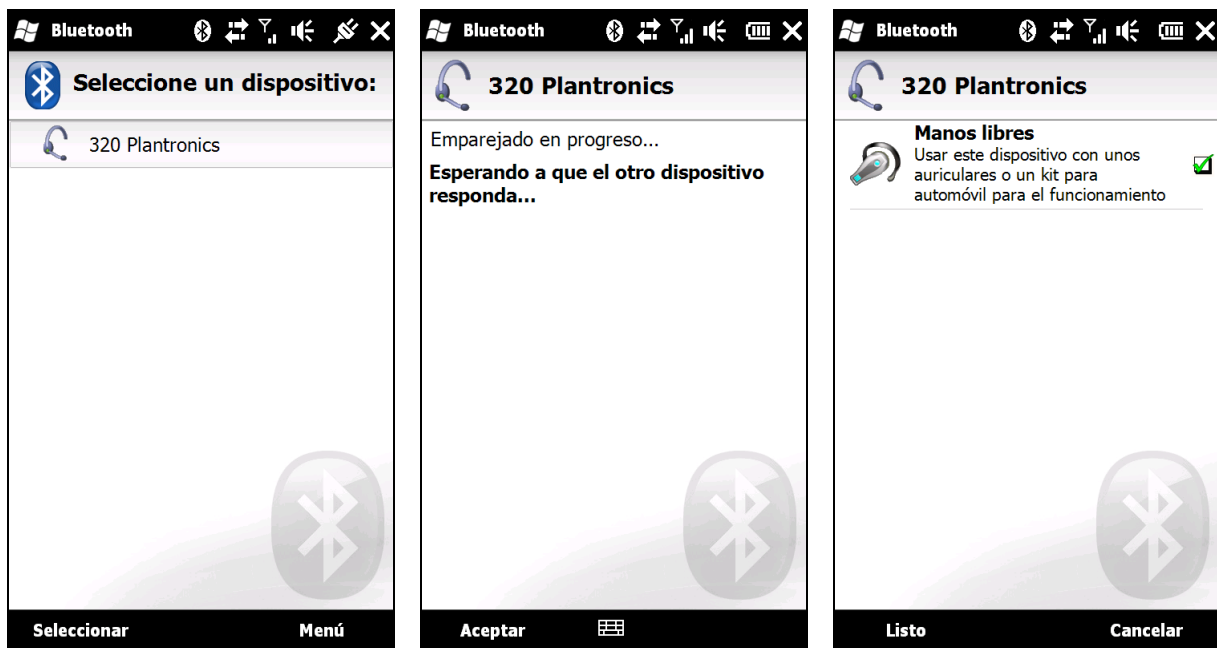
emparejamiento antes de transferir datos con otro dispositivo, el comportamiento no cambia:

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Services\0002]
"Name"="OBEX Object Push"
"Authentication"=dword:00000001
```

442. La transferencia de datos a través del perfil OBEX Object Push es similar a la empleada en el perfil OBEX FTP (ver apartado “5.17.6. OBEX File Transfer (y mecanismos de seguridad)”). Tras aplicarse los mecanismos de autenticación y autorización, se establece la conexión cifrada, y si la transferencia tiene éxito, se indica con una pantalla de confirmación que incluye el remitente, el nombre los datos transferidos, y dónde se han almacenado (carpeta destino en el caso de ficheros, contactos en el caso de tarjetas de visita, calendario en el caso de citas, etc).

### 5.17.8 MANOS LIBRES BLUETOOTH

443. El emparejamiento con dispositivos Bluetooth manos libres puede no requerir el introducir ningún PIN o clave de paso, proceso conocido como emparejamiento automático o *auto pairing*, debido a que Windows Mobile 6.5 dispone de conocimiento de los PIN's empleados por defecto (no modificables) por los fabricantes de manos libres Bluetooth:



**Nota:** si se elimina el emparejamiento con el dispositivo manos libres Bluetooth, por ejemplo a través del botón “Menú-Eliminar”, sucesivos emparejamientos tampoco requerirán introducir un PIN.

La información obtenida durante el emparejamiento inicial se mantiene en el registro (no es eliminada realmente, salvo la clave de enlace: *LinkKey*). La información de emparejamiento del dispositivo móvil está disponible en la siguiente clave del registro, dónde el último valor corresponde a la dirección (BD\_ADDR) del dispositivo manos libres:

```
HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Devices\00:03:89:01:02:03
```

El escenario de emparejamiento puede variar en función de la información que quedó previamente almacenada en el dispositivo manos libres durante el emparejamiento inicial, pudiendo éste iniciar los intentos de emparejamiento hacia el dispositivo móvil.

**Nota:** las claves de enlace (*link keys*) de Bluetooth generadas durante el emparejamiento entre el dispositivo móvil Windows Mobile 6.5 y cualquier otro dispositivo Bluetooth son almacenadas en la siguiente clave del registro, donde “00:10:60:05:06:07” es la dirección (BD\_ADDR) del otro dispositivo:

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Devices\00:10:60:05:06:07]
"LinkKey"=hex:\
 96,2F,D9,68,02,70,53,F8,41,B5,90,CF,79,CA,FE,F2
```

Esta información es crítica desde el punto de vista de seguridad, y el acceso a la misma por parte de un potencial atacante permitiría la suplantación del otro dispositivo y el establecimiento de conexiones Bluetooth con el dispositivo móvil con sus permisos asociados.

444. El comportamiento del emparejamiento automático queda reflejado en el parámetro “AutoPair”, que indica si el emparejamiento con un dispositivo, identificado por su dirección (BD\_ADDR), fue realizado de forma automática (“1”) o no (“0”):

```
[HKLM\Software\WIDCOMM\BTConfig\Devices\00:03:89:01:02:03]
"AutoPair"=dword:00000001
```

445. El PIN más común empleado por defecto en Bluetooth es “0000”, tal como define la siguiente entrada del registro, que incluye los valores “0000” (0x30303030) y “8888” (0x38383838):

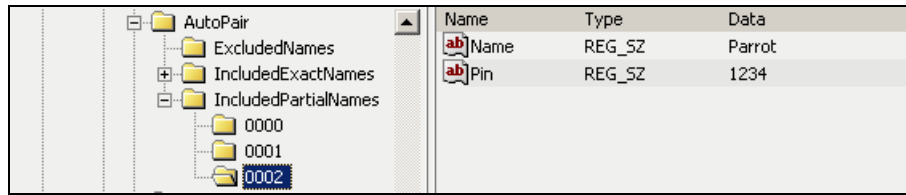
```
[HKEY_LOCAL_MACHINE\ControlPanel\Bluetooth]
"PinEntries"=hex(7):\
 30,30,30,30,00,38,38,38,38,00,00
```

**Nota:** tras eliminar el valor “0000” de la lista de PIN’s del registro (“PinEntries”) y realizar un restablecimiento software, el dispositivo móvil sigue emparejándose automáticamente sin solicitar un PIN con los dispositivos manos libres que utilizan por defecto el valor “0000” para el PIN, por lo que se trata de un comportamiento implícito en la implementación de Bluetooth empleada y no configurable mediante un parámetro.

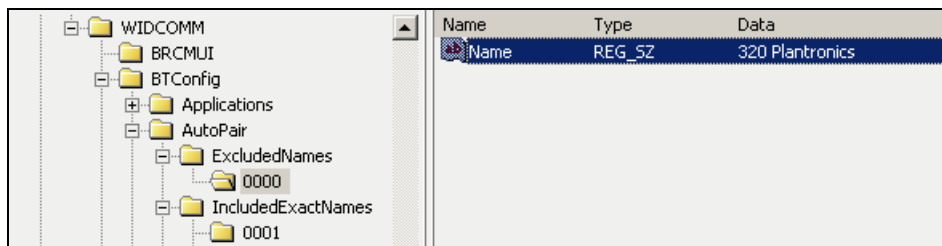
446. El emparejamiento automático no se lleva a cabo con otros dispositivos que emplean valores de PIN diferentes, como por ejemplo “1234”. A través del registro es posible especificar otros PIN’s por defecto según el modelo de dispositivo Bluetooth, así como incluir o excluir dispositivos para el emparejamiento automático en base a su nombre completo o parcial, a través de las siguientes claves del registro:

```
[HKLM\Software\WIDCOMM\BTConfig\AutoPair\ExcludedNames]
[HKLM\Software\WIDCOMM\BTConfig\AutoPair\IncludedPartialNames]
[HKLM\Software\WIDCOMM\BTConfig\AutoPair\IncludedExactNames]
```

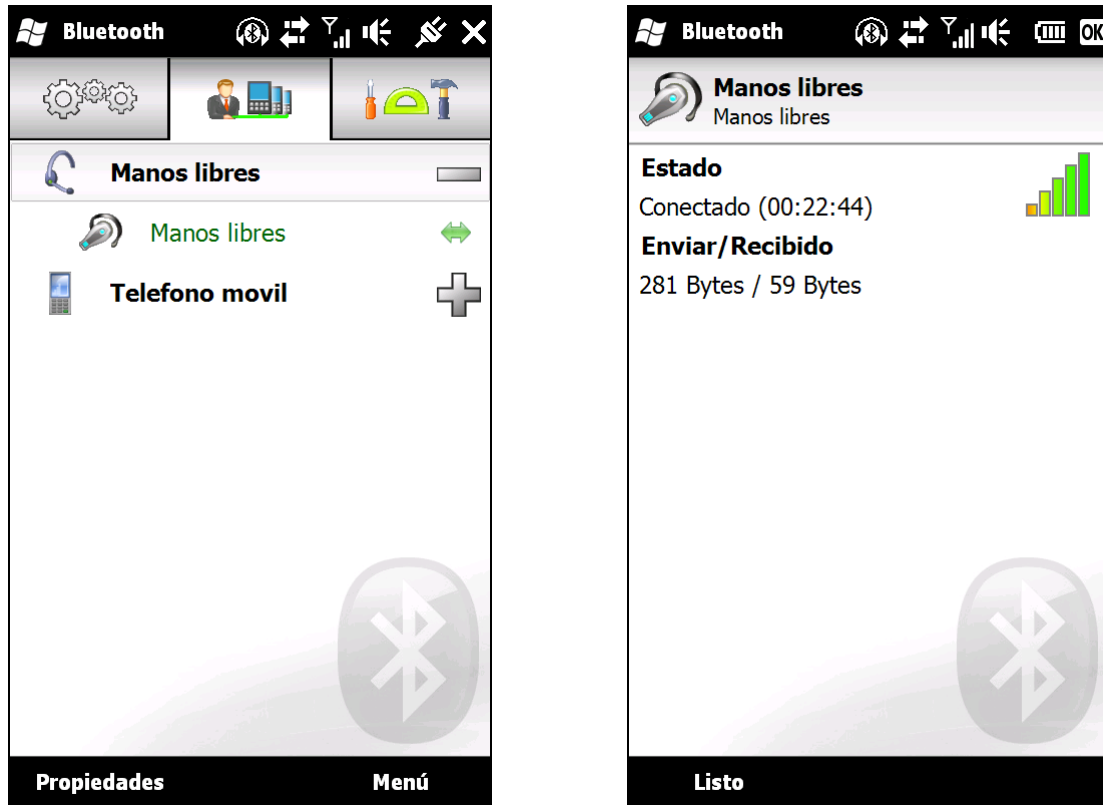
447. La creación de la entrada (“0002”) de la siguiente imagen muestra como añadir un PIN por defecto, con valor “1234”, para el emparejamiento automático con dispositivos Parrot (aquellos que incluyen la cadena “Parrot” en el nombre; “IncludedPartialNames”):



448. Se recomienda eliminar todas las entradas de las claves “Included\*” del registro con las que no se desea que se establezca el emparejamiento automático.
449. Se recomienda añadir una nueva clave en la rama “ExcludedNames” con el objetivo de deshabilitar el emparejamiento automático con los dispositivos manos libres Bluetooth que hacen uso de los PIN empleados por defecto por Windows Mobile 6.5. Por ejemplo, la siguiente imagen muestra como forzar el emparejamiento manual de un dispositivo manos libres “320 Plantronics” a través de la entrada de exclusión “0000”:



450. El interfaz Bluetooth del dispositivo móvil, una vez es habilitado, intenta establecer automáticamente una conexión con los dispositivos manos libres disponibles en la lista de dispositivos emparejados, proceso conocido como conexión automática o *auto connect*. Si el dispositivo Bluetooth se encuentra en el rango de alcance del dispositivo móvil, y fueron emparejados previamente, se establecerá la conexión, estado identificado en Windows Mobile 6.5 por una doble flecha de color verde junto al dispositivo manos libres (imagen inferior izquierda):



**Nota:** si se selecciona el perfil de Bluetooth con la conexión activa actualmente, a través del botón “Menú – Estado” (imagen superior derecha) es posible obtener información del tiempo que lleva activa la conexión, la cantidad de datos recibidos y enviados, y la intensidad de la señal, lo que ofrece una indicación de la distancia aproximada a la que se encuentra en dispositivo Bluetooth del dispositivo móvil. Todos estos datos pueden ser muy útiles durante la gestión de incidentes de seguridad relacionados con tecnologías Bluetooth.

451. El orden empleado para establecer la conexión con los dispositivos manos libres, en el caso de disponer de varios dispositivos emparejados y estar todos ellos disponibles, está regido por la posición en la lista de dispositivos emparejados. Se establecerá la conexión automática sólo con el primer dispositivo de la lista, es decir, aquel que fue añadido más recientemente o aquel con el que se realizó una conexión por última vez.
452. La siguiente clave del registro determina con qué dispositivo se llevará a cabo la conexión. Cada dispositivo con el que se han realizado alguna conexión dispone de una entrada numérica en el registro (ej. “0005”), y aquel cuyo parámetro “DefaultConnection” sea igual a “1” (siendo “0” en el resto) será el elegido para establecer la conexión automática:

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\Connections\0005]
"DefaultConnection"=dword:00000001
"BDName"="320 Plantronics"
"BDAddress"=hex:\
 00,03,89,01,02,03
```

**Nota:** si ningún dispositivo está definido como dispositivo por defecto, es decir, en todos “DefaultConnection” tiene el valor “0”, por ejemplo porque se eliminó manualmente el

emparejamiento con el dispositivo por defecto, Windows Mobile 6.5 no establecerá conexión automática con ningún dispositivo manos libres Bluetooth.

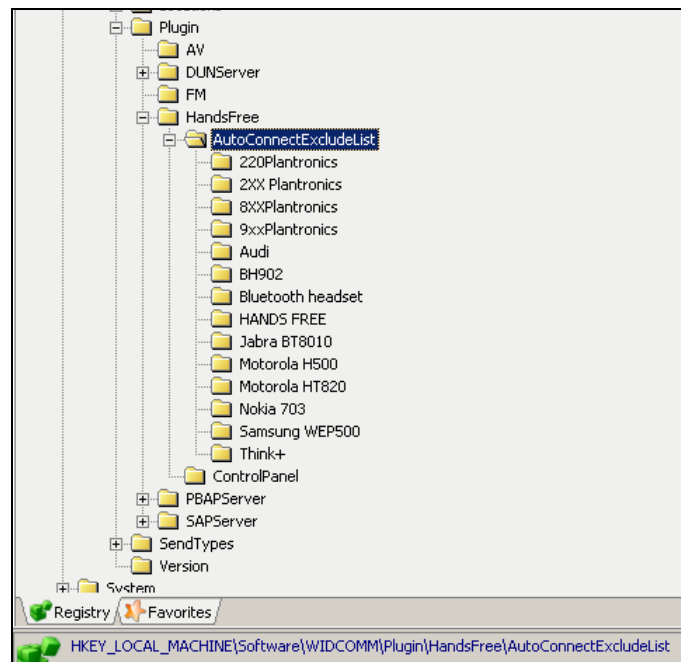
453. El intento de establecimiento de una conexión automática con el primer dispositivo manos libres Bluetooth de la lista de dispositivos emparejados es el comportamiento por defecto en Windows Mobile 6.5. Sin embargo, este comportamiento puede ser modificado a través del registro, ya que permite excluir ciertos dispositivos manos libres en función de su nombre (tipo o modelo). Por ejemplo, para evitar la conexión automática desde Windows Mobile 6.5 hacia un dispositivo manos libres “320 Plantronics” basta con crear la siguiente clave del registro (sin valores asociados):

HKLM\Software\WIDCOMM\Plugin\HandsFree\AutoConnectExcludeList\**320 Plantronics**

El valor de la entrada debe corresponder al nombre exacto del dispositivo manos libres Bluetooth, o a una cadena de caracteres que coincida con los caracteres iniciales del nombre (por ejemplo, “320” cuando el nombre es “320 Plantronics”). Así, por ejemplo, para deshabilitar la conexión automática con todos los dispositivos manos libres cuyo nombre comienza por “E”, basta con crear la siguiente entrada del registro:

HKLM\Software\WIDCOMM\Plugin\HandsFree\AutoConnectExcludeList\**E**

454. Por defecto, Windows Mobile 6.5 no realiza conexiones automáticas con la lista de dispositivos manos libres Bluetooth mostrados en la siguiente imagen:



455. Se recomienda añadir a esta lista todos aquellos dispositivos manos libres con los que se haya emparejado el dispositivo móvil, con el objetivo de disponer de un mayor control sobre el establecimiento de conexiones Bluetooth, requiriendo que el usuario inicie la conexión de forma activa (en lugar de iniciarse automáticamente).
456. Adicionalmente, debe tenerse en cuenta que el establecimiento de una conexión automática podría realizarse incluso cuando el dispositivo móvil está configurado para que no sea así, ya que el dispositivo manos libres también podría iniciar la conexión si dispone de capacidades de conexión automática al ser activado (situación habitual).

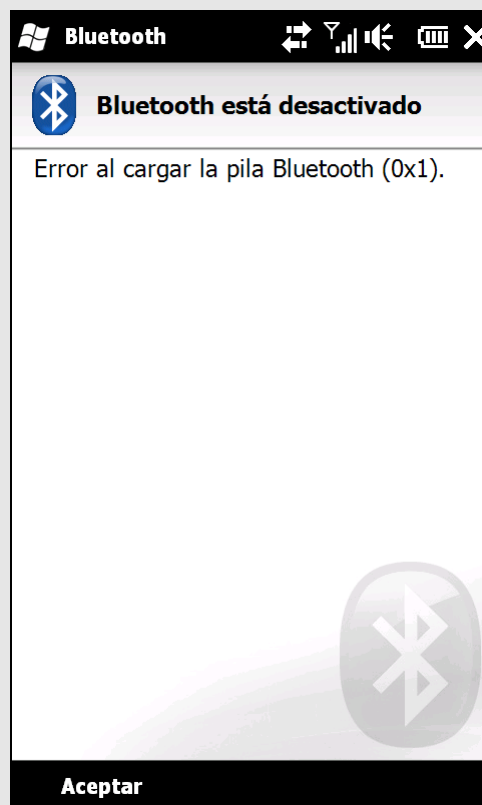
457. Es posible limitar los intentos de conexión desde el dispositivo manos libres al dispositivo móvil a través de la configuración de los parámetros de seguridad del perfil “HandsFree”. Por defecto, la configuración de seguridad es la siguiente:

| Perfil Bluetooth | Autenticación | Autorización | Cifrado |
|------------------|---------------|--------------|---------|
| HandsFree        | 1             | 0            | 1       |

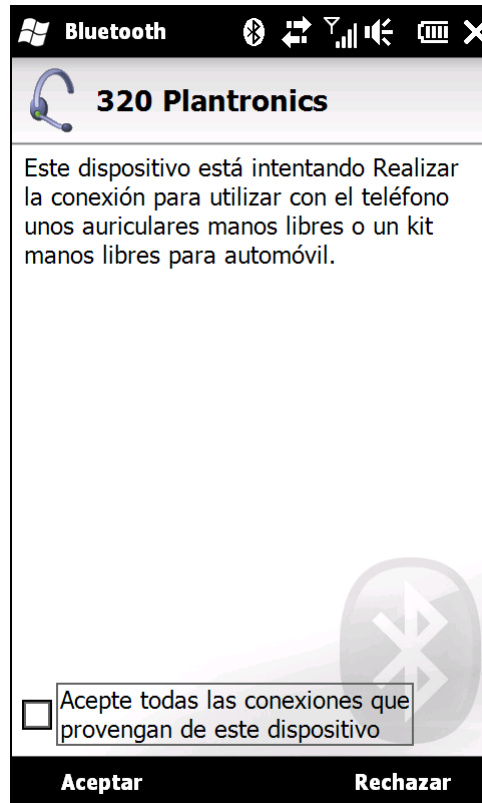
458. Las siguientes claves del registro permiten habilitar los diferentes mecanismos de seguridad asociados al perfil de manos libres (HandsFree):

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\Plugin\HandsFree\ControlPanel]
"Name"="Hands Free"
"Enabled"=dword:00000001
"Encryption"=dword:00000001
"Authorization"=dword:00000001
"Authentication"=dword:00000001
```

**Nota:** pese a que el parámetro “Enabled” de la anterior clave del registro parece permitir habilitar o deshabilitar (fijando el valor a “0”) el perfil “HandsFree”, escenario recomendado en el caso de no hacer uso del mismo, en realidad Windows Mobile 6.5 no permite deshabilitar este perfil, y en caso de hacerlo la pila Bluetooth no podrá ser activada, generándose el siguiente error:

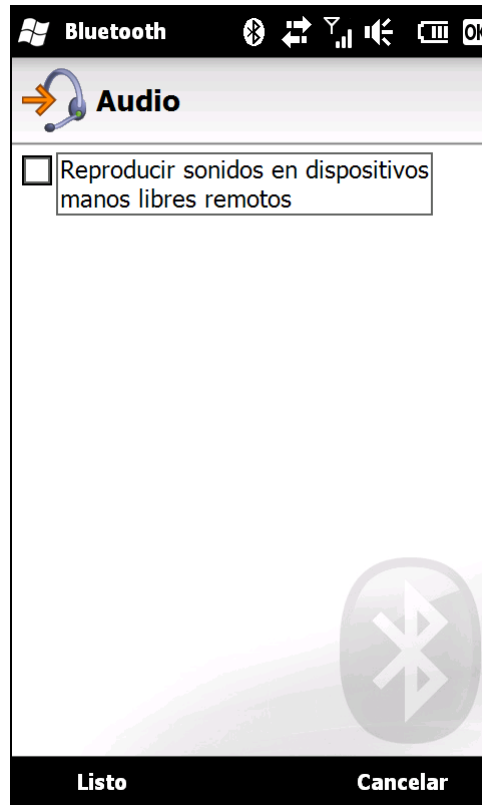


459. Cuando el mecanismo de autorización ha sido activado, al recibirse el intento de conexión por parte del dispositivo manos libres, Windows Mobile 6.5 solicitará confirmación por parte del usuario, notificándole del intento:



460. Se recomienda habilitar todos los mecanismos de seguridad disponibles (autenticación, autorización y cifrado) para el perfil de manos libres, "HandsFree", con el objetivo de tener un mayor control sobre las conexiones originadas desde dispositivos manos libres hacia el dispositivo móvil.
461. El menú de configuración de audio, relacionado con dispositivos manos libres Bluetooth, define si se habilita la reproducción de sonidos en dispositivos manos libres remotos a través de Bluetooth:

**Nota:** el menú de configuración de audio está ubicado en las opciones de configuración avanzadas de Bluetooth, quinta opción de la pestaña de configuración de Bluetooth de la izquierda, accesible a través del menú "Inicio – Configuración", mediante el botón "Menú" y la opción "Más", y el icono "Bluetooth".



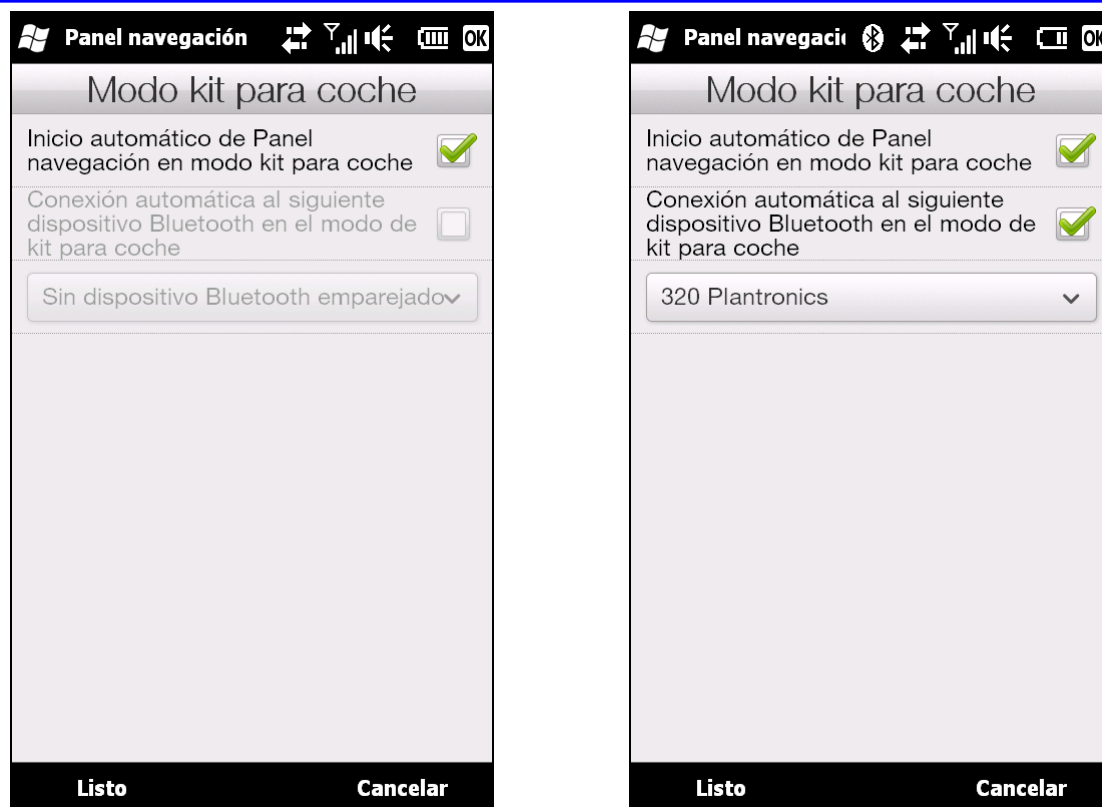
462. Se recomienda no activar (desactivado por defecto) la reproducción de sonidos generados por el dispositivo móvil en dispositivos manos libres remotos, salvo que se quiera hacer uso explícito de esta funcionalidad.

463. La posibilidad de reproducir sonidos en dispositivo manos libres remotos a través de Bluetooth es gestionada por la siguiente clave del registro, cuyo valor es “0” si está deshabilitado (valor por defecto) y “2” en el caso de ser activado:

```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\Plugin\HandsFree]
"AudioPreferences"=dword:00000000
```

**Nota:** la reproducción de sonidos, aparte de la gestión de llamadas de teléfono mediante Bluetooth (que funciona también en manos libres mono), sólo es posible si el dispositivo manos libres Bluetooth es estéreo, es decir, implementa el perfil A2DP, *Advanced Audio Distribution Profile*. El establecimiento de una conexión de audio estéreo Bluetooth está indicado mediante un icono diferente en la barra de título (ver apartado “5.17. Comunicaciones Bluetooth”).

464. El modo kit para coche de HTC, disponible a través del menú “Inicio – Configuración – Otros – Modo kit para coche”, gestiona el comportamiento del dispositivo móvil al estar conectado en un vehículo a un kit para coche, y en concreto la salida de audio por el altavoz y su volumen, la integración con NaviPanel (panel de navegación), la utilización del GPS y la orientación de la pantalla (vertical u horizontal). La imagen inferior izquierda muestra la configuración por defecto:



465. El panel de navegación facilita el uso del dispositivo móvil en un vehículo:



466. Las siguientes claves del registro determinan si el panel de navegación se activa en modo kit para coche (“AutoNaviPanel”), si se realiza una conexión automática con un dispositivo Bluetooth en modo kit para coche (“AutoBlueTooth”), y con qué dispositivo Bluetooth (“PairedBTAddr”). Los valores de los dos primeros parámetros serán “1” si han sido activados en el interfaz de usuario (imagen superior derecha):

```
[HKEY_CURRENT_USER\ControlPanel\CarKitMode]
"PairedBTAddr"="320 Plantronics"
"AutoNaviPanel"=dword:00000000
"AutoBlueTooth"=dword:00000000
```

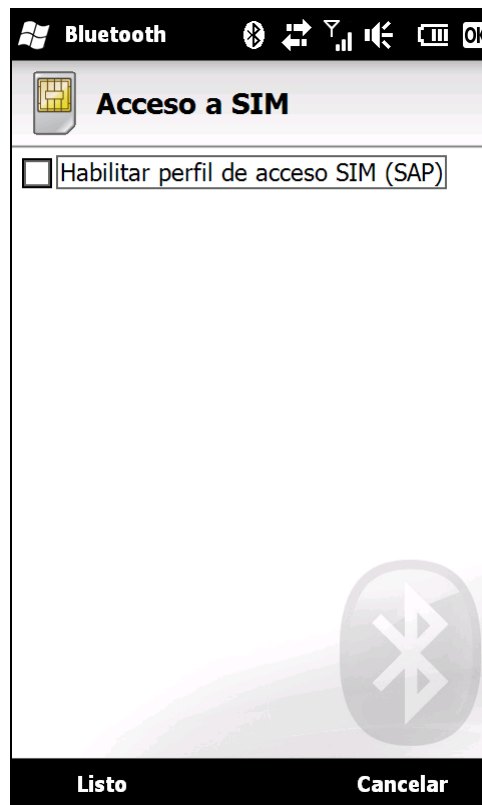
467. Se recomienda deshabilitar la conexión automática en modo kit para coche con un dispositivo Bluetooth, “AutoBlueTooth” (salvo que se quiera hacer uso explícito de esa funcionalidad), con el objetivo de disponer de un mayor control sobre las conexiones establecidas con dispositivos manos libres Bluetooth, tal y como se recomendó previamente cuando el dispositivo móvil no se encuentra en modo kit para coche.

### 5.17.9 SAP: SIM ACCESS PROFILE

468. El menú de configuración del perfil de acceso a la tarjeta SIM (SAP, *SIM Access Profile*) permite habilitar o deshabilitar este perfil.

**Nota:** el menú de configuración del perfil de acceso a la tarjeta SIM está ubicado en las opciones de configuración avanzadas de Bluetooth, quinta opción de la pestaña de configuración de Bluetooth de la izquierda, accesible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Bluetooth”.

469. Se recomienda deshabilitar el perfil de acceso a la tarjeta SIM (SAP), habilitado por defecto, salvo que se quiera hacer uso explícito de este perfil a través de Bluetooth:



470. En el caso de hacer uso del perfil SAP, se recomienda habilitar el perfil temporalmente en el momento de su utilización, para volver a deshabilitarlo una vez utilizado. Para ello no es necesario reiniciar el interfaz Bluetooth, sino que basta con habilitar la opción de configuración y pulsar el botón “Listo”.

471. La disponibilidad del perfil de acceso a la tarjeta SIM (SAP) es gestionada por la siguiente clave del registro, cuyo valor es “0” si está deshabilitado y “1” si está habilitado:

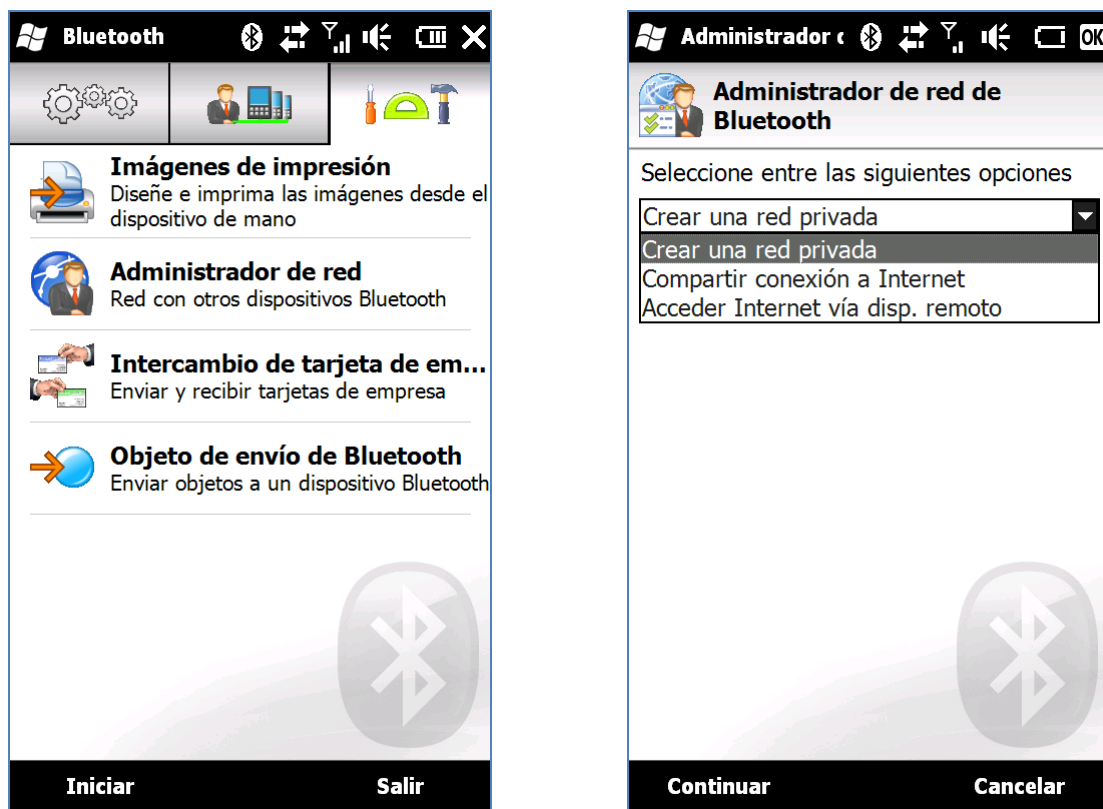
```
[HKEY_LOCAL_MACHINE\Software\WIDCOMM\Plugin\SAPServer\ControlPanel]
"Enabled"=dword:00000000
```

472. Pese a que todos los mecanismos de seguridad del perfil SAP están habilitados por defecto (ver apartado “5.17.11. Otros perfiles Bluetooth”), debido a la criticidad de la información y funcionalidad disponible a través de él, en caso de no hacer uso de este perfil, debería deshabilitarse. El perfil SAP permite el acceso a la tarjeta SIM a través de

Bluetooth por ejemplo desde un vehículo para usar sus capacidades de telefonía (o desde otros dispositivos para la realización de micropagos).

#### 5.17.10 RED DE ÁREA PERSONAL (PAN)

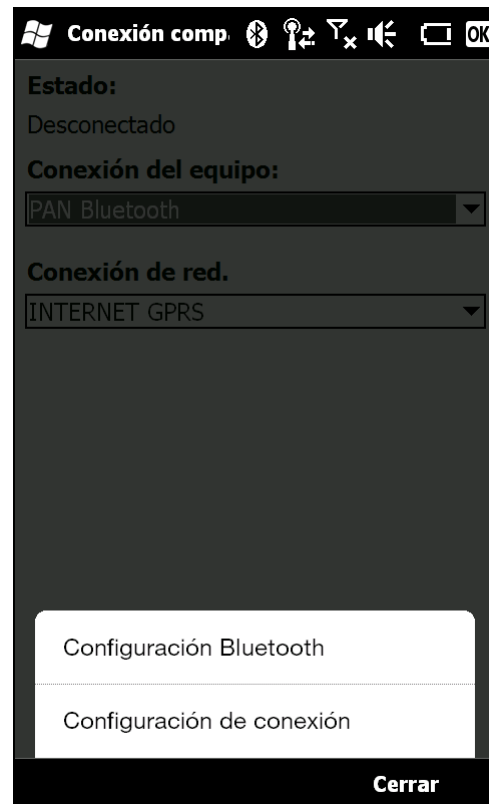
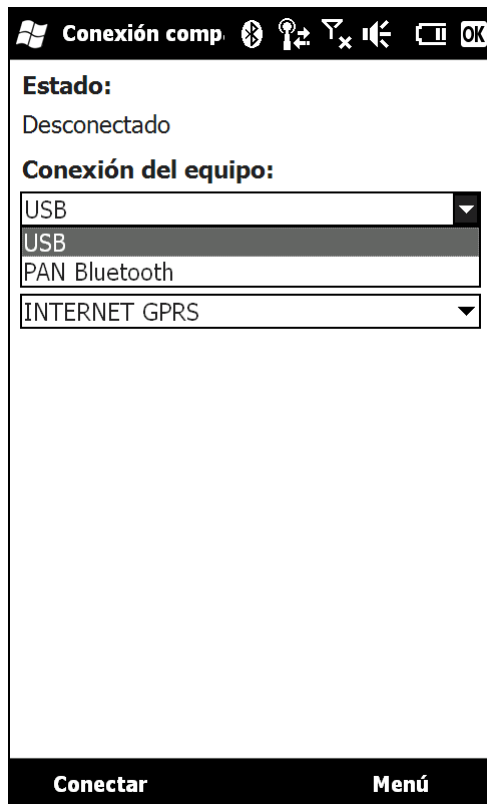
473. El dispositivo móvil basado en Windows Mobile 6.5 dispone del perfil de red de área personal (PAN, *Personal Area Network*) para establecer conexiones TCP/IP con otros dispositivos a través de Bluetooth.
474. Las conexiones de red a través de Bluetooth se pueden originar desde otro dispositivo si el perfil PAN está habilitado en el dispositivo móvil (ver apartado “5.17.11. Otros perfiles Bluetooth” para deshabilitar este perfil), o desde el propio dispositivo móvil hacia otro dispositivo que disponga del perfil PAN, a través del menú de “Administrador de red” de Bluetooth:



**Nota:** el menú de “Administrador de red” de Bluetooth está ubicado en las opciones de herramientas de Bluetooth, segunda opción de la pestaña de configuración de Bluetooth de la derecha, accesible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Bluetooth”.

475. Desde el “Administrador de red” de Bluetooth (imagen superior derecha) es posible crear una red privada entre dispositivos Bluetooth (169.254.x.x/16), compartir la conexión a Internet (de telefonía móvil) del dispositivo móvil desde el otro dispositivo (analizado posteriormente) o viceversa, acceder a Internet desde el dispositivo móvil vía el otro dispositivo (si dispone de dichas capacidades).

476. La realización de un escaneo de puertos a través de la conexión PAN (red privada) muestra los mismos resultados que a través del interfaz Wi-Fi (ver apartado “5.21.4. Escaneo de puertos TCP y UDP”).
477. La configuración del perfil PAN (ej. TCP/IP) está disponible en la siguiente clave del registro: “HKEY\_LOCAL\_MACHINE\Comm\BTCEPAN1”.
478. A través del perfil PAN es posible hacer uso de las capacidades de *tethering* del dispositivo móvil, es decir, hacer uso de las capacidades de comunicación de datos de telefonía móvil del terminal para acceder a Internet desde otros dispositivos, como por ejemplo un ordenador.
479. Las capacidades de *tethering* pueden ser ofrecidas por el dispositivo móvil a través del perfil PAN de Bluetooth o a través de cable USB (opción recomendada desde el punto de vista de seguridad; ver apartado “5.16. Comunicaciones USB”).
480. Para poder hacer uso de estas capacidades de interconexión es necesario activar el módulo de “Conexión compartida” (ICS, *Internet Connection Sharing*), disponible desde el menú “Inicio – Herramientas (Herram.)”:



481. El módulo de “Conexión compartida” permite configurar el perfil Bluetooth (enlazando con el interfaz de configuración de Bluetooth) y la conexión de datos de telefonía móvil (enlazando con el interfaz de configuración de conexiones de datos).
482. Se recomienda deshabilitar el módulo de conexión compartida o *tethering* salvo que se requiera hacer uso de su funcionalidad. En cualquier caso, pese a estar deshabilitado, la configuración de este módulo debería utilizar por defecto la opción USB para la conexión entre el equipo y el dispositivo móvil, y la conexión “GPRS VACIA” (creada en el apartado “5.20. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”) para la

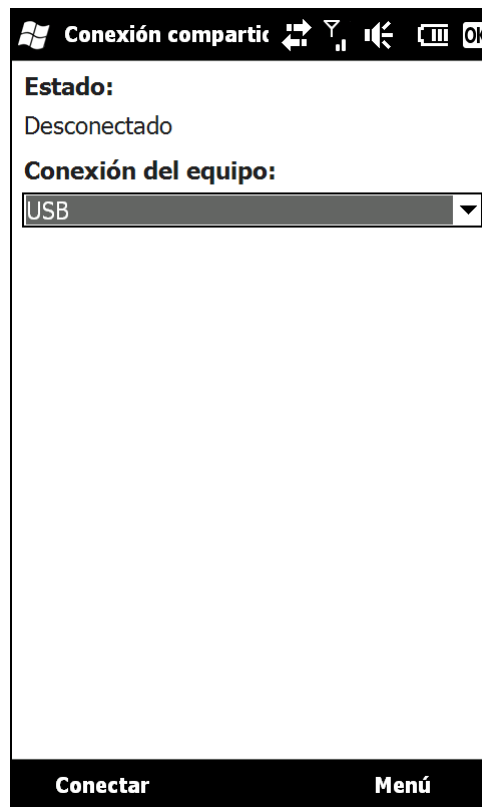
conexión de red, con el objetivo de limitar el establecimiento de conexiones no autorizadas a través de este módulo.

483. La siguiente clave del registro especifica las conexiones de telefonía móvil y del dispositivo móvil a utilizar por defecto (las últimas conexiones empleadas):

```
[HKEY_CURRENT_USER\Software\Microsoft\InternetSharing]
"LastCellConnection"="GPRS VACIA"
"LastHostConnection"="USB"
```

484. Si se desea evitar el uso de la funcionalidad de “Conexión compartida” es posible forzar a través del registro (mediante la creación de un nuevo parámetro) la conexión de datos de telefonía móvil a emplear, de forma que no sea posible seleccionarla a través del interfaz de usuario (imagen inferior), al eliminarse la sección “Conexión de red”. En este caso, se recomienda seleccionar la conexión “GPRS VACIA” mencionada previamente para no disponer de conectividad alguna:

```
[HKEY_LOCAL_MACHINE\Comm\InternetSharing\Settings]
"ForceCellConnection"="GPRS VACIA"
```



485. La siguiente clave del registro dispone de la configuración del módulo de conexión compartida [Ref.- 64]. Se recomienda configurar el módulo para que esté deshabilitado en el inicio, y al ser habilitado, para hacer uso de las capacidades de traducción de direcciones (NAT, *Network Address Translation*) y de las capacidades de filtrado (la configuración por defecto de todas las opciones es la recomendada):

```
[HKEY_LOCAL_MACHINE\Comm\ConnectionSharing]
"DisabledOnBoot"=dword:00000001
"EnableAddressTranslation"=dword:00000001
"EnablePacketFiltering"=dword:00000001
```

**Nota:** la utilización de las capacidades de traducción de nombres (NAT) requiere que el dispositivo móvil haga de router, y por tanto que el parámetro “HKEY\_LOCAL\_MACHINE\Comm\Tcpip\Parms\IpEnableRouter” esté activo (ver apartado “5.21.2. Perfil de conexión: Internet o Trabajo”), funcionalidad gestionada automáticamente por el módulo de “Conexión compartida”.

486. El filtrado de paquetes se activa en el módulo de NAT, pero solo para IPv4 (no para IPv6 – razón adicional para deshabilitar la pila IPv6; ver apartado “5.21.6. IPv6”), bloqueando conexiones no solicitadas en el interfaz público de ICS. Las conexiones originadas en el interfaz privado o registradas en el módulo de NAT serán permitidas.

487. El módulo ICS es también utilizado por el perfil Bluetooth de redes de acceso telefónico (DUN, *Dial-Up Networking*), cada vez más en desuso respecto al perfil PAN [Ref.- 65].

### 5.17.11 OTROS PERFILES BLUETOOTH

488. El menú “Acerca de” permite, a través del botón “Perfiles”, conocer los diferentes perfiles Bluetooth disponibles en el dispositivo móvil (once perfiles por defecto):

**Nota:** el menú “Acerca de” corresponde a la sexta opción de la pestaña de configuración de Bluetooth de la izquierda, accesible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Bluetooth”.



489. Se recomienda de manera general deshabilitar todos los perfiles Bluetooth que no vayan a ser utilizados, con el objetivo de reducir la superficie de exposición del dispositivo móvil frente a ataques a través de Bluetooth, así como incrementar el nivel de seguridad de los

perfiles a utilizar a través de los mecanismos de seguridad disponibles en Bluetooth. A continuación se detalla como deshabilitar cada tipo de perfil Bluetooth.

490. En Windows Mobile 6.5 los mecanismos de seguridad están habilitados por defecto para la mayoría de los perfiles, denominados en algún caso “servicios” por Microsoft, con las excepciones de la siguiente tabla. El valor indica si el mecanismo de seguridad está habilitado (“1”) o deshabilitado (“0”) por defecto:

| Perfil Bluetooth (Servicios)                                      | On/Off | Autenticación | Autorización | Cifrado |
|-------------------------------------------------------------------|--------|---------------|--------------|---------|
| Bluetooth Serial Port (0001)                                      | 1      | 1             | 0            | 1       |
| OBEX Object Push (0002)                                           | 1      | 0             | 1            | 1       |
| OBEX File Transfer (0003)                                         | 0      | 1             | 1            | 1       |
| Network Access (0004):<br><i>PAN Group Network &amp; PAN User</i> | 1      | 1             | 1            | 1       |

491. El perfil de puerto serie (Serial Port) no requiere autorización por defecto, por lo que no se notifica al usuario acerca de los intentos de conexión recibidos, y el perfil OBEX Object Push no requiere (teóricamente) autenticación por defecto debido a su modelo de uso, intercambio rápido de información que no requiere el emparejamiento previo de los dispositivos Bluetooth.

492. Para disponer de un entorno de seguridad mejorado, se recomienda activar los mecanismos de autorización y autenticación en los perfiles de puerto serie y OBEX Object Push (ver apartado “5.17.7. OBEX Object Push”), respectivamente.

493. Los “Servicios” Bluetooth están definidos en la siguiente clave del registro:

HKEY\_LOCAL\_MACHINE\Software\WIDCOMM\BTConfig\Services

494. Los servicios Bluetooth pueden ser deshabilitados mediante el parámetro “Auto” (valor igual a “0”) de su correspondiente clave del registro. El interfaz Bluetooth debe ser deshabilitado y habilitado para que los cambios surtan efecto. Por defecto, tres de los cuatro servicios están habilitados, excepto OBEX FTP.

495. Los mecanismos de seguridad disponibles por defecto en Windows Mobile 6.5 para otros perfiles, denominados en algún caso “plugins” por Microsoft, se detallan en la siguiente tabla. El valor indica si el mecanismo de seguridad está habilitado (“1”) o deshabilitado (“0”) por defecto:

| Perfil Bluetooth (Plugins)                                                   | On/Off | Autenticación | Autorización | Cifrado |
|------------------------------------------------------------------------------|--------|---------------|--------------|---------|
| Dial-up Networking (DUN)                                                     | 1      | 1             | 1            | 1       |
| HandsFree:<br><i>Headset Audio Gateway &amp;<br/>Handsfree Audio Gateway</i> | 1*     | 1             | 0            | 1       |
| Phone Book Access Profile<br>(PBAP)                                          | 1      | 1             | 1            | 1       |

|                          |   |   |   |   |
|--------------------------|---|---|---|---|
| SIM Access Profile (SAP) | 1 | 1 | 1 | 1 |
|--------------------------|---|---|---|---|

\*: Ver excepción en el proceso de desactivación de perfiles, asociada al plugin “HandsFree”, en el apartado “5.17.8. Manos libres Bluetooth”.

496. Con el objetivo de disponer de mayor control sobre las conexiones hacia el dispositivo móvil desde dispositivos manos libres, se recomienda habilitar el mecanismo de autorización en el perfil o plugin “HandsFree”.

497. Los “Plugins” Bluetooth están definidos en la siguiente clave del registro:

```
HKEY_LOCAL_MACHINE\Software\WIDCOMM\Plugin
```

498. Los plugins Bluetooth pueden ser deshabilitados mediante el parámetro “Enabled” (valor igual a “0”) de su correspondiente clave del registro, “ControlPanel”. El interfaz Bluetooth debe ser deshabilitado y habilitado para que los cambios surtan efecto. Por defecto los cuatro plugins están habilitados.

499. El único método identificado para deshabilitar los perfiles Bluetooth de Audio Gateway, Handsfree (manos libres) y Headset (auriculares), ya que no pueden ser deshabilitados individualmente, es a través de la desactivación desde el registro (mediante la siguiente clave) de los servicios generales de Bluetooth de Windows Mobile 6.5. Tras reiniciar el dispositivo móvil, si se intenta activar la pila Bluetooth se generará un mensaje de error (ver apartado “5.17.8. Manos libres Bluetooth”):

```
[HKEY_LOCAL_MACHINE\Services\BtCeProfiles]
"Flags"=dword:00000004
```

**Nota:** teóricamente, los servicios de Windows Mobile 6.5 pueden ser deshabilitados individualmente a través del parámetro “Flags” del registro, valor 0x00000004, de cada servicio [Ref.- 58], sin embargo esta configuración no afecta al servicio “BTAGSVC” (Bluetooth Audio Gateway) individualmente:

```
HKEY_LOCAL_MACHINE\Services\nombre servicio
```

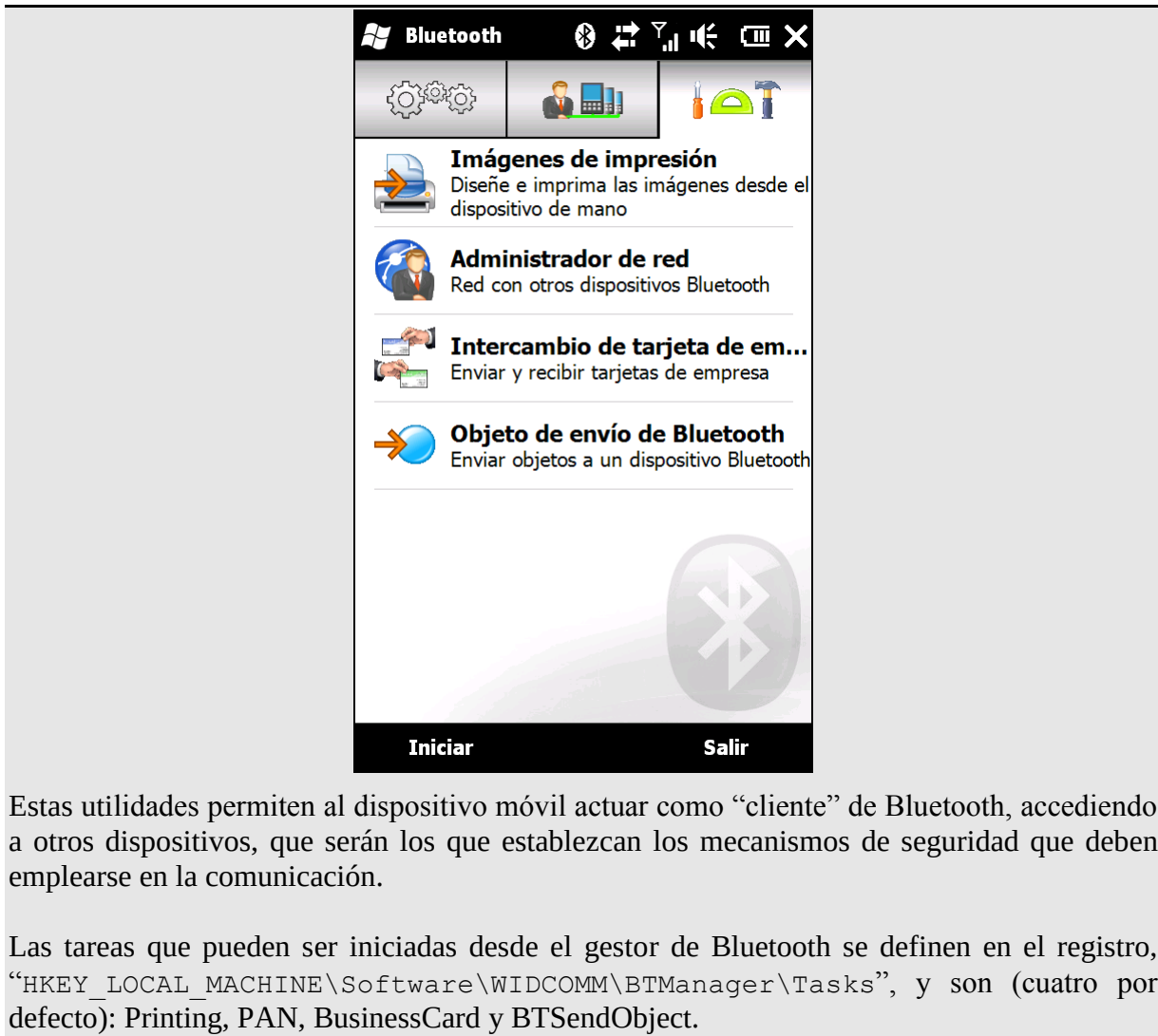
Es necesario reiniciar el dispositivo móvil para que los cambios surtan efecto.

**Nota:** los mecanismos de seguridad disponibles por defecto en Windows Mobile 6.5 para lo que la pila WIDCOMM denomina “aplicaciones” Bluetooth, donde el dispositivo móvil actúa de “cliente” estableciendo conexiones Bluetooth salientes, tienen deshabilitado tanto la autenticación como el cifrado (no disponen de autorización), excepto para “ActiveSync Serial Port”. Las “aplicaciones” Bluetooth están definidas en la siguiente clave del registro:

```
HKEY_LOCAL_MACHINE\Software\WIDCOMM\BTConfig\Applications
```

Los controles de seguridad son establecidos por el dispositivo “servidor” de Bluetooth.

**Nota:** la pestaña de la derecha del menú de configuración de Bluetooth (disponible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Bluetooth”) contiene utilidades para el uso de ciertos perfiles Bluetooth, como la impresión de imágenes, la conexión de red con otros equipos, el intercambio de tarjetas de empresa y el envío de objetos a través de Bluetooth:



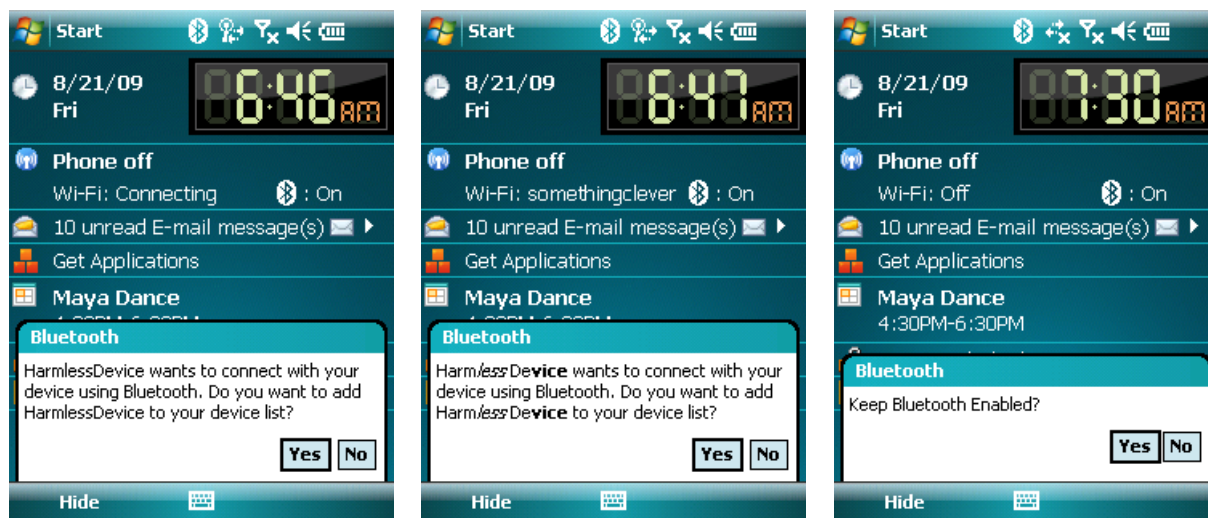
Estas utilidades permiten al dispositivo móvil actuar como “cliente” de Bluetooth, accediendo a otros dispositivos, que serán los que establezcan los mecanismos de seguridad que deben emplearse en la comunicación.

Las tareas que pueden ser iniciadas desde el gestor de Bluetooth se definen en el registro, “HKEY\_LOCAL\_MACHINE\Software\WIDCOMM\BTManager\Tasks”, y son (cuatro por defecto): Printing, PAN, BusinessCard y BToSendObject.

### 5.17.12 ATAQUES BLUELINE

500. Windows Mobile emplea el lenguaje HTML (contenidos web) para mostrar los mensajes y avisos de diferentes componentes del interfaz gráfico, incluidas las notificaciones de acceso generadas por el interfaz Bluetooth (ver apartado “5.19.1. Ejecución de contenido web en mensajes de texto”).
501. Cuando los mecanismos de autorización de Bluetooth están activos, el dispositivo solicita confirmación al usuario antes de permitir el acceso desde otros dispositivos, mostrando en la notificación el nombre Bluetooth del otro dispositivo.
502. Debido a la ausencia de mecanismos de validación de dicho nombre, éste puede incluir etiquetas HTML. Pese a que un atacante no puede eliminar la existencia de los botones de confirmación o el título, las etiquetas HTML pueden ser empleadas para desplazar el texto mostrado por defecto en el mensaje de notificación [Ref.- 108]. Este ataque Bluetooth es conocido como Blueline.
503. Mediante el desplazamiento de dicho texto, un atacante puede llevar a cabo ataques de ingeniería social, mostrar en la notificación cualquier mensaje que potencialmente será aceptado positivamente por el usuario, como por ejemplo “¿Desea que el interfaz Bluetooth continúe activo?”.

504. Si el usuario víctima responde afirmativamente a dicho mensaje, estará aceptando la conexión con el dispositivo Bluetooth externo controlado por el atacante.



NOTA: Imágenes de ejemplo obtenidas de “<http://pauldotcom.com/wiki/index.php/Episode209>”.

**Nota:** la existencia de esta vulnerabilidad BlueLine en Windows Mobile está condicionada a las capacidades añadidas por ciertos fabricantes de dispositivos móviles. Si las capacidades de notificación existentes por defecto en el interfaz gráfico de Bluetooth en Windows Mobile han sido reemplazadas por el fabricante, la vulnerabilidad podría ser eliminada o incluso ser más crítica, permitiendo ataques de Cross-Site Scripting (XSS).

En el caso del dispositivo móvil empleado como referencia en la presente guía, la vulnerabilidad no está presente, ya que HTC proporciona un subsistema de notificaciones propietario que no interpreta el nombre de otros dispositivos Bluetooth como HTML.

### 5.17.13 DOS EN EL NOMBRE BLUETOOTH

505. Windows Mobile 6 es vulnerable frente a una denegación de servicio (DoS) asociada al procesamiento de nombres Bluetooth malformados de otros dispositivos.

506. En septiembre de 2008 [Ref.- 109] se anunció la vulnerabilidad en el driver de Bluetooth, indicando que tras la recepción de un nombre Bluetooth de elevada longitud (por ejemplo, 248 caracteres, el máximo definido por la especificación Bluetooth), el dispositivo móvil fallará y se reiniciará.

507. La vulnerabilidad puede ser explotada tanto durante el proceso de descubrimiento de otros dispositivos, como al recibir conexiones de otros dispositivos Bluetooth.

508. En el momento de elaboración de la presente guía no hay disponible ninguna actualización que resuelva esta vulnerabilidad.

**Nota:** el dispositivo móvil empleado como referencia en la presente guía no es vulnerable a esta denegación de servicio en el nombre Bluetooth.

## 5.18 COMUNICACIONES WI-FI

### 5.18.1 DESACTIVACIÓN DE LAS COMUNICACIONES WI-FI

509. La principal recomendación de seguridad asociada a las comunicaciones Wi-Fi (802.11) en dispositivos móviles es no activar el interfaz inalámbrico Wi-Fi salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Wi-Fi [Ref.- 49].

**Nota:** durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía (activado automáticamente la primera vez que se enciende el terminal), el interfaz Wi-Fi está habilitado, mostrándose al usuario las redes Wi-Fi disponibles en la ubicación del dispositivo móvil para su fácil selección y configuración.

Este comportamiento, centrado en incrementar la facilidad de uso y configuración del terminal, no es el recomendado desde el punto de vista de seguridad, ya que habilita funcionalidad por defecto (por ejemplo, capacidades de conexión Wi-Fi) en la que el usuario podría no estar interesado, introduciéndose así configuraciones por defecto inseguras. Se recomienda desactivar el interfaz Wi-Fi tan pronto finalice el proceso de configuración inicial.

En el caso de no realizar la configuración de ninguna red Wi-Fi durante el proceso de configuración inicial, el interfaz Wi-Fi es deshabilitado automáticamente al finalizar el mismo.

En caso de establecer una conexión Wi-Fi durante el proceso de configuración inicial (asociada al perfil “Trabajo”, pese a que el perfil por defecto en Windows Mobile 6.5 es “Internet”), el dispositivo móvil ofrece la posibilidad de configurar cuentas de correo electrónico y cuentas de redes sociales, quedando el interfaz Wi-Fi activo al finalizar el mismo. En este caso, salvo que se deshabilite el interfaz Wi-Fi explícitamente, permanecerá activo incluso tras reiniciar el terminal.

510. El interfaz inalámbrico Wi-Fi puede ser desactivado en Windows Mobile 6.5 a través del menú “Inicio – Configuración – Controles inalámbricos” (que proporciona acceso al “Comm Manager”), mediante el botón deslizante de activación y desactivación asociado a la sección “WLAN”:



511. El estado del interfaz Wi-Fi puede ser verificado de forma rápida y sencilla por el usuario del dispositivo móvil a través de la barra superior de estado.
512. Windows Mobile 6.5 proporciona información en la barra superior de estado sobre el estado del interfaz Wi-Fi, la disponibilidad de redes Wi-Fi, y si se está o no conectado a una red Wi-Fi actualmente, a través del siguiente conjunto de iconos:

|  |                                      |
|--|--------------------------------------|
|  | Wi-Fi activada                       |
|  | Red(es) inalámbrica(s) disponible(s) |
|  | Conectado a una red inalámbrica      |

**Nota:** el interfaz Wi-Fi en Windows Mobile 6.5 no puede ser deshabilitado en tiempo real únicamente a través de la manipulación del registro. Las siguientes tres claves del registro forman parte del proceso de desactivación de las capacidades Wi-Fi, pero tras aplicarlas, el estado del interfaz sigue siendo activo, tal como muestran tanto el “Comm Manager” como la pestaña de configuración de Wi-Fi (analizada posteriormente):

```
[HKEY_LOCAL_MACHINE\Software\Drivers\WLAN]
"WlanStatus"=dword:00000000

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Power\State]
"{98C5250D-C29A-4985-AE5F-AFE5367E5006}\BCMSDDHD1"=dword:00000000

Cambios de estado en el interfaz Wi-Fi: activación, conexión...
Sólo cambia el icono de estado del interfaz Wi-Fi en la barra de título:
(Su valor es 19 en activo y 1 en inactivo)
```

```
[HKEY_LOCAL_MACHINE\System\State\Hardware]
"Wifi"=dword:00000001
```

Sin embargo, tras modificar estos valores en el registro y proceder a reiniciar el dispositivo móvil (incluso tras un restablecimiento software o *soft reset*), el interfaz Wi-Fi permanecerá deshabilitado.

513. Windows Mobile 6.5 mantiene el estado del interfaz Wi-Fi tras reiniciar el dispositivo móvil (incluso tras un restablecimiento de software o *soft reset*), es decir, si el interfaz Wi-Fi estaba activo al apagar el terminal, al encender el dispositivo móvil seguirá activo, incluso con el terminal bloqueado.

514. Igualmente, al salir del modo de vuelo el estado del interfaz Wi-Fi será restaurado, activándose en el caso de haber estado activo previamente (al activar el modo de vuelo).

515. El interfaz Wi-Fi permanece activo durante 30 segundos cuando el dispositivo móvil está conectado a una red y pasa al estado de espera o *stand-by* (desatendido), es decir, está encendido pero con la pantalla apagada y bloqueado. Pasado ese tiempo el dispositivo móvil se desconecta de la red Wi-Fi.

516. Es posible configurar el dispositivo móvil para que no se lleve a cabo esta desconexión y que mantenga la conexión con la red Wi-Fi en todo momento. En dispositivos móviles HTC, como el empleado para la elaboración de la presente guía, es necesario fijar el valor “1” (“0” por defecto”) en la siguiente clave del registro:

```
[HKEY_LOCAL_MACHINE\Comm\BCMSDDHD1\Parms]
"HTCKeepWifiOnWhenUnattended"=dword:00000001
```

517. En caso de no estar conectado a una red Wi-Fi, en el estado de espera el dispositivo móvil no genera ningún tráfico 802.11.

**Nota:** para otros dispositivos Windows Mobile 6.5 no HTC, es necesario modificar varias claves del registro asociadas a la alimentación del dispositivo móvil y sus estados (concretamente Resuming, Suspend y Unattended), fijando el valor de “Default” a “1” de la clave “{98C5250D-C29A-4985-AE5F-AFE5367E5006}”:

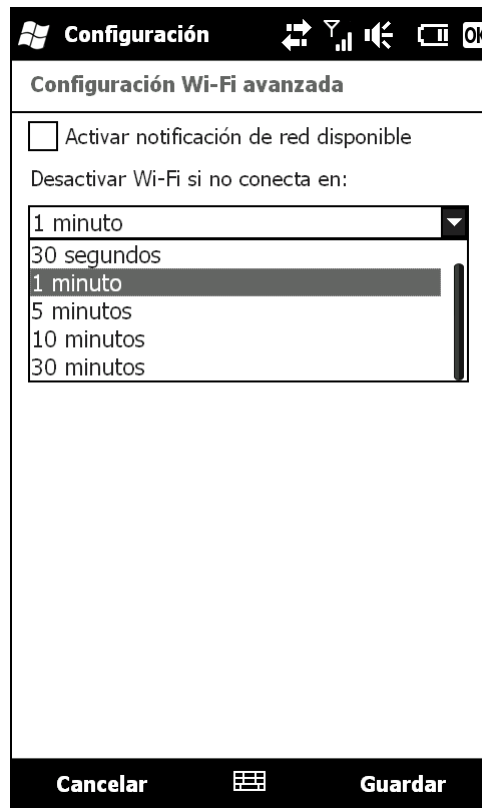
```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Power\State
```

Este cambio podría afectar a otras tecnologías de comunicaciones, como Bluetooth, 2G/3G y ActiveSync (<http://forum.xda-developers.com/showthread.php?t=273990&highlight=wifi+standby>).

518. Existe una opción muy interesante disponible en Windows Mobile 6.5 que permite desactivar el interfaz Wi-Fi si no se ha establecido una conexión en un periodo de tiempo determinado, como por ejemplo un minuto, de forma que si la conexión Wi-Fi es activada (de forma intencionada o accidental), será automáticamente desactivada al no establecerse una conexión con una red conocida previamente en un periodo determinado.

519. Aunque esta funcionalidad fue diseñada para preservar la batería del dispositivo móvil, y evitar así que el terminal busque constantemente redes conocidas a las que conectarse, la desactivación automática del interfaz Wi-Fi tiene implicaciones de seguridad relevantes, por lo que se recomienda su utilización con un valor de un minuto.

520. La opción está disponible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Conexiones – Wi-Fi”. Seleccionar el botón “Redes inalámbricas”, el botón “Menú” y la opción “Avanzadas”:



521. La siguiente clave del registro especifica el tiempo en segundos tras el cual el interfaz Wi-Fi será desactivado si no se ha establecido ninguna conexión. Si no se desea activar esta funcionalidad, su valor debe ser “0”. El siguiente ejemplo especifica un intervalo de tiempo de 60 segundos (en hexadecimal, 0x3C):

```
[HKEY_LOCAL_MACHINE\ControlPanel\WiFi]
"Timeout"=dword:0000003C
```

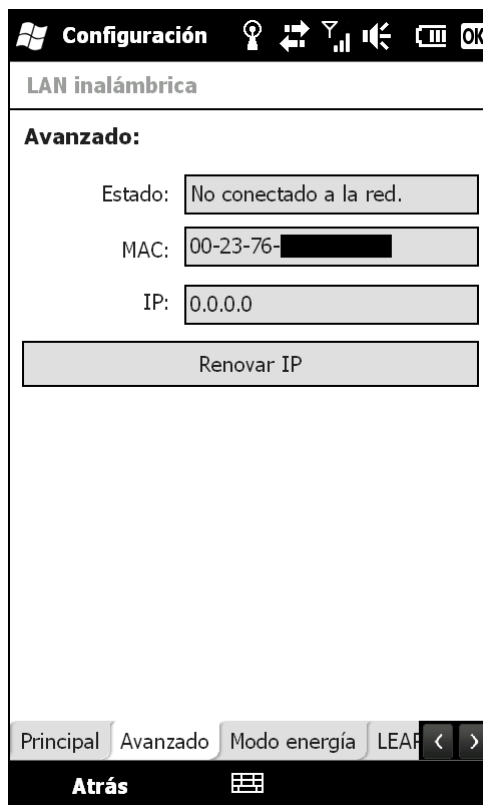
522. La misma pantalla de configuración permite activar las notificaciones de redes Wi-Fi disponibles, gestionadas por la siguiente clave del registro, con un valor “0” si las notificaciones están deshabilitadas y “9” si están activas:

```
[HKCU\ControlPanel\Notifications\{DDBD3B44-80B0-4b24-9DC4-839FEA6E559E}]
"Options"=dword:00000009
```

523. Se recomienda habilitar la opción “Activar notificación de red disponible” con el objetivo de que el usuario del dispositivo móvil disponga de más información sobre las señales y redes disponibles en su actual ubicación. En caso de que el número de redes Wi-Fi disponibles genere un número excesivo de notificaciones, se aconseja deshabilitar este parámetro con el objetivo de premiar funcionalidad frente a seguridad.

**Nota:** en función del fabricante y modelo de dispositivo móvil, la funcionalidad de notificación de la existencia de redes Wi-Fi puede no estar disponible. En el caso del dispositivo móvil empleado para la elaboración de la presente guía, al ser activada esta funcionalidad es deshabilitada automáticamente por el terminal, sin generar notificaciones de redes Wi-Fi, debido a su integración con el interfaz de usuario HTC Sense.

524. Debe tenerse en cuenta que, a diferencia del interfaz Bluetooth, para poder llevar a cabo la configuración de la pila de comunicaciones Wi-Fi a través del interfaz de usuario del dispositivo móvil no es necesario activar el interfaz (excepto para la visualización de la información de estado del interfaz Wi-Fi), por lo que se recomienda no activar el interfaz para realizar las modificaciones de la configuración.
525. La dirección del interfaz Wi-Fi está disponible a través del menú “Inicio – Configuración – Controles inalámbricos – WLAN”, botón “Avanzado”, mediante la pestaña del mismo nombre, “Avanzado”, y en concreto, en el campo “MAC”:



526. El adaptador Wi-Fi “Broadcom 802.11 DHD Network Adapter” parece no almacenar la dirección Wi-Fi del interfaz en el registro.

**Nota:** la parte de la dirección Wi-Fi asociada al fabricante (primeros tres *bytes* de la dirección) puede permitir identificar el tipo de dispositivo móvil. En el ejemplo analizado, el valor “00:23:76” está asignado por el IEEE (<http://standards.ieee.org/regauth/oui/index.shtml>) a “HTC”:

|                  |                           |
|------------------|---------------------------|
| 00-23-76 (hex)   | HTC Corporation           |
| 002376 (base 16) | HTC Corporation           |
|                  | No.23 Hsin Hua Rd.        |
|                  | Taoyuan Taiwan 330        |
|                  | TAIWAN, REPUBLIC OF CHINA |

527. Es aconsejable comparar la dirección Wi-Fi del dispositivo móvil con su dirección Bluetooth (ver apartado “5.17. Comunicaciones Bluetooth”), con el objetivo de

identificar si se trata de direcciones correlativas. En caso afirmativo, un potencial atacante podría obtener la dirección de Bluetooth a partir de la dirección Wi-Fi, con los riesgos que ello conlleva [Ref.- 1], al emplearse la ocultación de la dirección Bluetooth en diferentes escenarios como mecanismo de seguridad.

528. Es necesario ser especialmente cuidadoso respecto al lugar dónde se enciende el dispositivo móvil, ya que aunque el interfaz Wi-Fi esté deshabilitado en Windows Mobile 6.5, al encender el dispositivo móvil se genera tráfico Wi-Fi desvelando tanto su dirección MAC como la lista de redes ocultas configuradas, antes incluso de desbloquear el terminal:

```
696 08:46:34.799543 00:23:76:ff:ff:ff: IEEE -38 Probe Request, SN=16, FN=0, Flags=.....C, SSID=Broadcast
698 08:46:34.822051 00:23:76:ff:ff:ff: IEEE -22 Probe Request, SN=17, FN=0, Flags=.....C, SSID=Broadcast
700 08:46:34.842419 00:23:76:ff:ff:ff: IEEE -22 Probe Request, SN=18, FN=0, Flags=.....C, SSID=Broadcast
706 08:46:34.864902 00:23:76:ff:ff:ff: IEEE -24 Probe Request, SN=19, FN=0, Flags=.....C, SSID=Broadcast
707 08:46:34.865889 00:1d:7e:00:23:76: IEEE -68 Probe Response, SN=2708, FN=0, Flags=.....C, BI=100, SSID="WLAN"
709 08:46:34.867296 00:1d:7e:00:23:76: IEEE -70 Probe Response, SN=2708, FN=0, Flags=.....R...C, BI=100, SSID="WLAN"
711 08:46:34.885293 00:23:76:ff:ff:ff: IEEE -22 Probe Request, SN=20, FN=0, Flags=.....C, SSID=Broadcast
712 08:46:34.909304 00:1d:7e:00:23:76: IEEE -67 Probe Response, SN=2709, FN=0, Flags=.....C, BI=100, SSID="WLAN"
```

529. El tráfico generado corresponde a paquetes *probe request*, enviados con el objetivo de identificar todas las redes Wi-Fi disponibles en la zona (*Broadcast*), así como peticiones de búsqueda específicas para las redes Wi-Fi ocultas configuradas en el dispositivo móvil (ver apartado “5.18.5. Recomendaciones de seguridad para la conexión a redes Wi-Fi”).

530. Esta vulnerabilidad es especialmente relevante al encender el dispositivo móvil en entornos inseguros dónde no se desea generar ningún tráfico Wi-Fi.

**Nota:** esta vulnerabilidad (TAD-2010-002) de revelación de información ha sido confirmada por Microsoft, aunque no publicará una actualización para solucionarla [Ref.- 106].

**Nota:** los detalles del driver Wi-Fi empleado están disponibles en el registro, incluyendo el nombre del interfaz Wi-Fi y versiones del driver y firmware [Ref.- 53]:

```
HKEY_LOCAL_MACHINE\Software\Drivers\WLAN
```

El nombre del interfaz Wi-Fi (“AdapterName”) asocia el driver con el interfaz, por ejemplo “BCMSDHDH1”, cuya configuración está disponible en la siguiente clave del registro:

```
HKEY_LOCAL_MACHINE\Comm\BCMSDDHD1
```

## 5.18.2 SELECCIÓN DE LA RED DE DATOS EN WINDOWS MOBILE

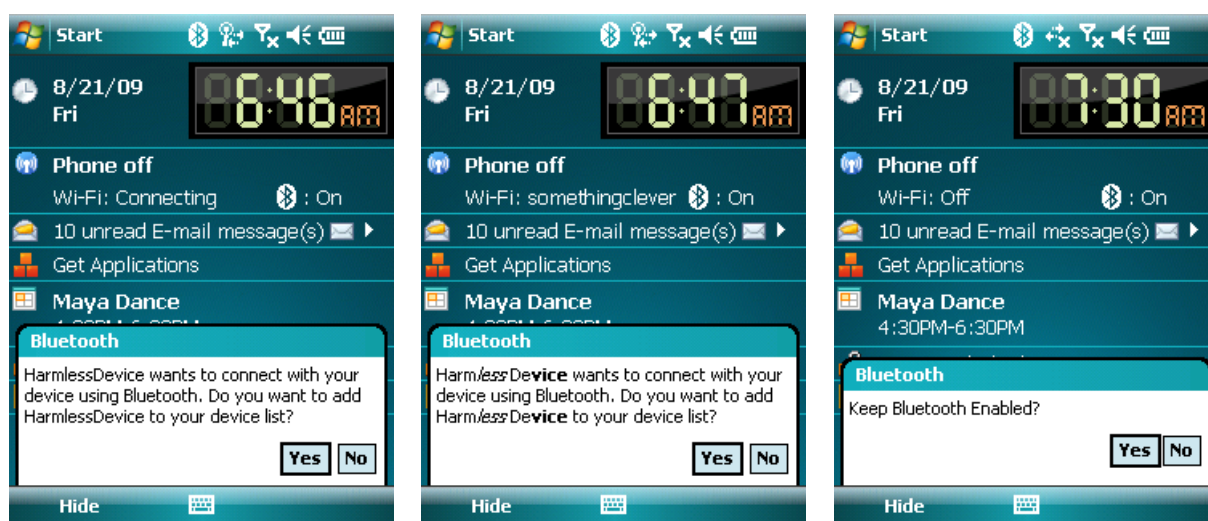
**Nota:** la selección de la red de datos en Windows Mobile 6.5 afecta principalmente a la red de datos de telefonía móvil 2G/3G (analizada en el apartado “5.20. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”) y al interfaz Wi-Fi.

## 5.18.3 ATAQUES BLUELINE

531. Windows Mobile emplea el lenguaje HTML (contenidos web) para mostrar los mensajes y avisos de diferentes componentes del interfaz gráfico, incluidas las notificaciones de acceso generadas por el interfaz Bluetooth (ver apartado “5.19.1. Ejecución de contenido web en mensajes de texto”).

532. Cuando los mecanismos de autorización de Bluetooth están activos, el dispositivo solicita confirmación al usuario antes de permitir el acceso desde otros dispositivos, mostrando en la notificación el nombre Bluetooth del otro dispositivo.

533. Debido a la ausencia de mecanismos de validación de dicho nombre, éste puede incluir etiquetas HTML. Pese a que un atacante no puede eliminar la existencia de los botones de confirmación o el título, las etiquetas HTML pueden ser empleadas para desplazar el texto mostrado por defecto en el mensaje de notificación [Ref.- 108]. Este ataque Bluetooth es conocido como Blueline.
534. Mediante el desplazamiento de dicho texto, un atacante puede llevar a cabo ataques de ingeniería social, mostrar en la notificación cualquier mensaje que potencialmente será aceptado positivamente por el usuario, como por ejemplo “¿Desea que el interfaz Bluetooth continúe activo?”.
535. Si el usuario víctima responde afirmativamente a dicho mensaje, estará aceptando la conexión con el dispositivo Bluetooth externo controlado por el atacante.



NOTA: imágenes de ejemplo obtenidas de “<http://pauldotcom.com/wiki/index.php/Episode209>”.

**Nota:** la existencia de esta vulnerabilidad Blueline en Windows Mobile está condicionada a las capacidades añadidas por ciertos fabricantes de dispositivos móviles. Si las capacidades de notificación existentes por defecto en el interfaz gráfico de Bluetooth en Windows Mobile han sido reemplazadas por el fabricante, la vulnerabilidad podría ser eliminada o incluso ser más crítica, permitiendo ataques de Cross-Site Scripting (XSS).

En el caso del dispositivo móvil empleado como referencia en la presente guía, la vulnerabilidad no está presente, ya que HTC proporciona un subsistema de notificaciones propietario que no interpreta el nombre de otros dispositivos Bluetooth como HTML.

#### 5.18.4 DOS EN EL NOMBRE BLUETOOTH

536. Windows Mobile 6 es vulnerable frente a una denegación de servicio (DoS) asociada al procesamiento de nombres Bluetooth malformados de otros dispositivos.
537. En septiembre de 2008 [Ref.- 109] se anunció la vulnerabilidad en el driver de Bluetooth, indicando que tras la recepción de un nombre Bluetooth de elevada longitud (por ejemplo, 248 caracteres, el máximo definido por la especificación Bluetooth), el dispositivo móvil fallará y se reiniciará.

538. La vulnerabilidad puede ser explotada tanto durante el proceso de descubrimiento de otros dispositivos, como al recibir conexiones de otros dispositivos Bluetooth.
539. En el momento de elaboración de la presente guía no hay disponible ninguna actualización que resuelva esta vulnerabilidad.

**Nota:** el dispositivo móvil empleado como referencia en la presente guía no es vulnerable a esta denegación de servicio en el nombre Bluetooth.

540. Debido a las múltiples opciones de conectividad de datos disponibles en los dispositivos móviles, como Bluetooth, Wi-Fi, 2G/3G, ActiveSync *pass-through*, etc, en caso de haber múltiples opciones habilitadas y disponibles, Windows Mobile 6.5 gestiona cual es la mejor conexión a usar en cada momento a través del *Connection Manager* [Ref.- 56]. De esta forma evita que el usuario tenga que decidir constantemente que conexión utilizar y proporciona la conectividad necesaria a las aplicaciones que ejecutan en el dispositivo móvil.
541. Los criterios empleados para seleccionar la mejor opción incluyen el tipo de red, Internet o Trabajo (red privada; ver apartado “5.21.2. Perfil de conexión: Internet o Trabajo”), el ancho de banda, el nivel de seguridad [Ref.- 54], etc. Las opciones de conexión y sus propiedades están definidas normalmente por el operador de telefonía móvil (ver apartado “5.20. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”), pero pueden ser personalizadas por el departamento de TI.
542. Los detalles de configuración del Connection Manager están almacenados en el registro:

HKEY\_LOCAL\_MACHINE\Comm\ConnMgr

**Nota:** el parámetro “ReadOnly” de cada conexión disponible en el registro para el Connection Manager (\Providers\\*\Connections\\*) permite bloquear la modificación de la conexión por parte del usuario (valor igual a “1”), opción empleada en ocasiones por los operadores de telefonía móvil.

543. El Connection Manager permite disponer de varias conexiones activas simultáneamente, conocido como *dual homing* [Ref.- 54], como por ejemplo 2G/3G y Wi-Fi, 2G/3G y *pass-through*, o Wi-Fi y *pass-through*.
544. Se recomienda evitar disponer de escenarios *dual homing*, como disponer de la conexión Wi-Fi y la conexión de datos de telefonía móvil (2G o 3G) simultáneamente (ver apartado “5.20. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”), con el objetivo de que el dispositivo móvil no actúe de pasarela entre distintas redes.
545. Las capacidades de enrutamiento de tráfico entre diferentes redes a nivel de la pila TCP/IP está definido por el parámetro “IpEnableRouter” (ver apartado “5.21.3. Seguridad en TCP/IP”), aunque el Connection Manager gestiona este escenario mediante el establecimiento de niveles de seguridad para cada conexión [Ref.- 54].
546. Las diferentes conexiones disponibles a través del Connection Manager disponen de los parámetros “Secure” y “SecureLevel” en el registro con el propósito de priorizar el uso de unas redes frente a otras. Por defecto, el orden de prioridad por defecto de las conexiones de datos es el siguiente:

- ActiveSync *pass-through* (DTPT).
- Wi-Fi.

- Telefonía móvil de datos: GPRS/UMTS (2G/3G).

547. Por defecto, por ejemplo, en el caso de tener habilitado tanto el interfaz Wi-Fi como de telefonía móvil, el dispositivo móvil se conectará con prioridad a las redes Wi-Fi disponibles. Si la señal de las mismas es reducida, entonces conmutará a la conexión 2G/3G, en función de la cobertura disponible.
548. Desde el punto de vista de seguridad podría considerarse más seguro cursar todo el tráfico de datos a través de las redes de telefonía móvil (cuando estén disponibles según la cobertura existente) en lugar de a través de redes Wi-Fi, siempre que se fuerce a que la conexión de datos de telefonía móvil emplee tecnologías 3G frente a 2G (ver apartado “5.20. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”).

**Nota:** en el caso del dispositivo móvil empleado para la elaboración de la presente guía, la manipulación de los parámetros del registro “Secure” y “SecureLevel” (y “AlwaysOn” [Ref.-105]), junto al parámetro “HTCDisconnGPRSWhenGotIP” [1] propio de HTC, no permiten modificar el comportamiento por defecto: en el caso de disponer de ambas conexiones activas (telefonía móvil de datos y Wi-Fi), el dispositivo móvil otorga mayor prioridad a la conexión Wi-Fi. Por tanto, se recomienda deshabilitar el interfaz Wi-Fi si se desea utilizar únicamente el interfaz de telefonía de datos.

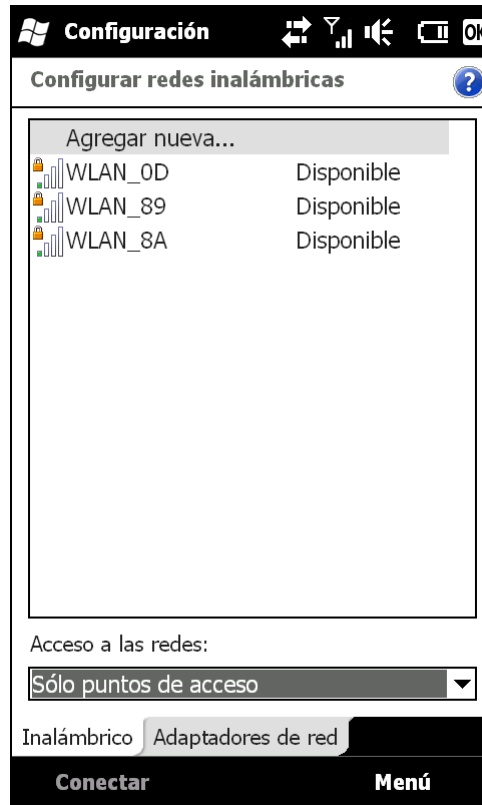
[1] HKEY\_LOCAL\_MACHINE\Comm\BCMSDDHD1\Parms  
"HTCDisconnGPRSWhenGotIP"=dword:00000001

**Nota:** debe tenerse en cuenta que el interfaz de telefonía de datos es activado automáticamente si se requiere una conexión de datos y no hay ninguna disponible, no así el interfaz Wi-Fi, que debe ser activado manualmente.

549. En el caso contrario, en el que se quiera cursar todo el tráfico de datos a través de redes Wi-Fi se recomienda consultar el apartado “5.20. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”, que contiene información detallada de cómo deshabilitar el interfaz de datos de telefonía móvil.

### 5.18.5 RECOMENDACIONES DE SEGURIDAD PARA LA CONEXIÓN A REDES WI-FI

550. Este apartado proporciona recomendaciones de configuración a través de los diferentes parámetros disponibles en Windows Mobile 6.5 para la conexión segura a redes Wi-Fi.
551. Se recomienda configurar Windows Mobile 6.5 para permitir conexiones Wi-Fi únicamente a redes Wi-Fi con infraestructura (o basadas en puntos de acceso), y restringir así la conexión a redes Wi-Fi entre equipos (*ad-hoc*). Esta opción de configuración está disponible desde el menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Conexiones – Wi-Fi”. Tras seleccionar el botón “Redes inalámbricas”, la pestaña “Inalámbrico” contiene la opción “Acceso a las redes:” en la parte inferior de la pantalla:



552. La información que determina el tipo de redes Wi-Fi a las que se permite conectar está definida en la siguiente clave del registro. El valor del parámetro “ControlFlags” (cuyo valor por defecto es 0x01818002), y en concreto el último carácter hexadecimal, determina la configuración de las redes Wi-Fi a las que se permite conectar: “2” indica que se permite acceso a “Todas (las redes) disponibles” (opción por defecto), el valor “1” indica “Sólo puntos de acceso” (opción recomendada) y el valor “0” indica “Sólo de equipo a equipo”.

```
[HKLM\Software\Microsoft\WZCSVC\Parameters\Interfaces\BCMSDDHD1]
"ControlFlags"=dword:01818001
```

**Nota:** el tipo de datos REG\_DWORD (*Double Word*) del registro de Windows Mobile tiene un tamaño de 32 bits ó 4 bytes, y se representa en hexadecimal con 8 caracteres hexadecimales: 0x01234567.

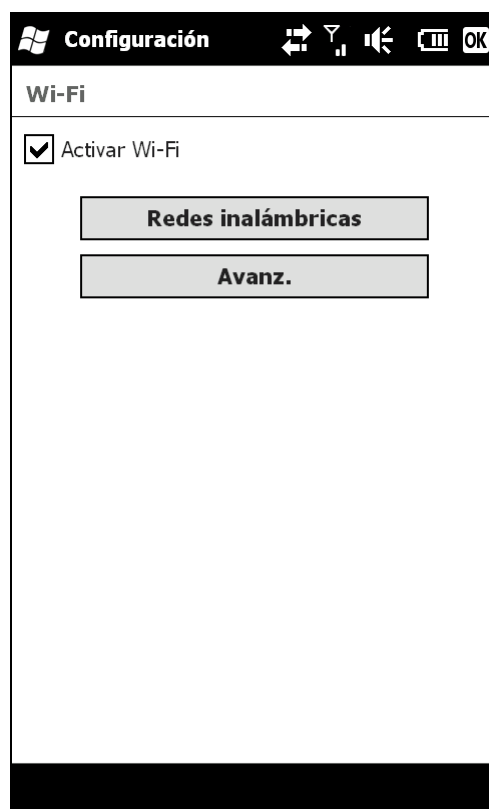
El valor de “ControlFlags” de la configuración de WZCSVC contiene múltiples opciones de configuración. En concreto, el tipo de red a la que se permite conectar está definida en el carácter hexadecimal menos significativo (situado más a la derecha).

**Nota:** el tipo de red Wi-Fi a la que se permite conectar puede ser establecida también de forma más sencilla mediante un fichero XML de aprovisionamiento de configuración del dispositivo móvil (ver apartado “5.8. Modificación local de políticas de seguridad”). El siguiente fichero permite configurar el tipo de red Wi-Fi a “Sólo puntos de acceso” mediante la directiva “parm” [Ref.- 77] (“0”: sólo ad-hoc, “1”: sólo APs, y “2”: cualquiera):

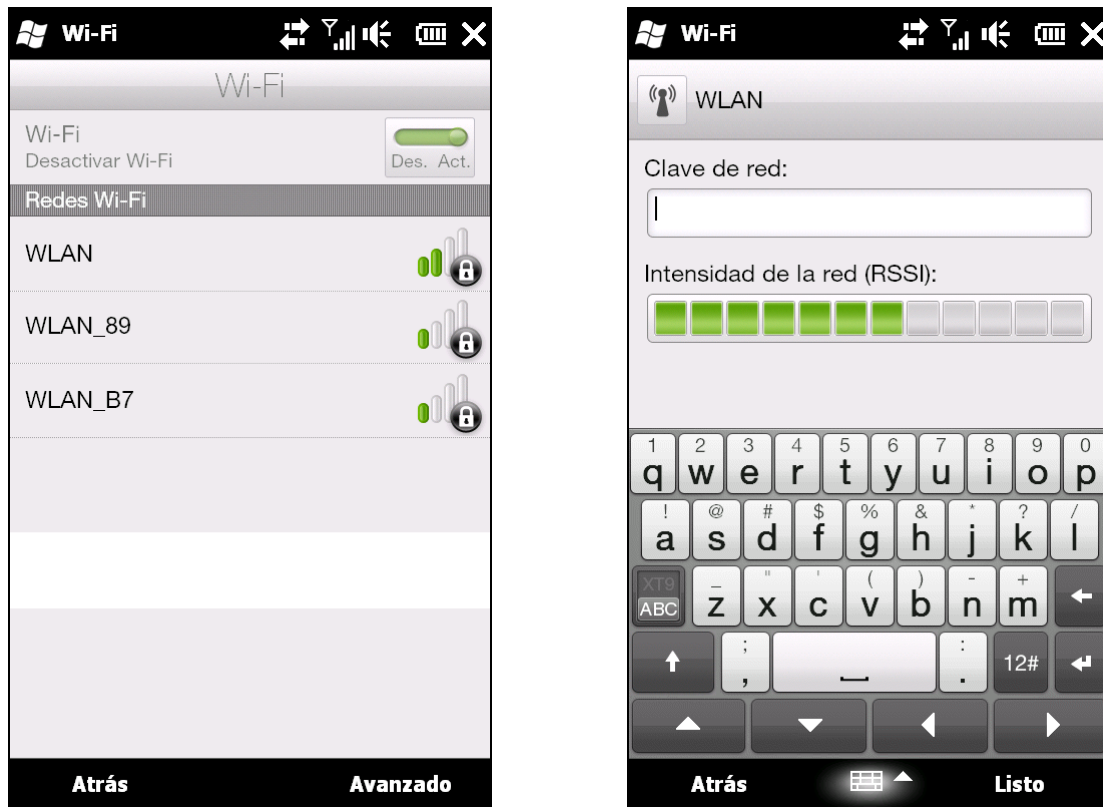
```
<wap-provisioningdoc>
 <characteristic type="Wi-Fi">
 <parm name="Filter" value="1"/>
 </characteristic>
</wap-provisioningdoc>
```

```
</characteristic>
</wap-provisioningdoc>
```

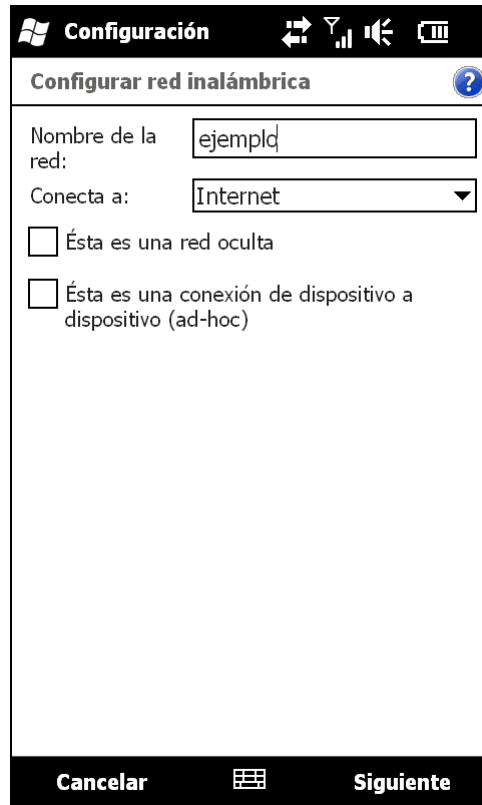
553. La configuración detallada de las redes Wi-Fi se puede realizar desde el menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Conexiones – Wi-Fi”. Seleccionar el botón “Redes inalámbricas” (imagen inferior izquierda), y la pestaña “Inalámbrico”.
554. Mediante la selección de una de las redes disponibles (equivalente a la opción “Editar”), o a través del botón “Menú” y las opciones “Editar” o “Agregar nueva...” (imagen inferior derecha), es posible configurar todas las opciones de conexión de una nueva red Wi-Fi, o editar las de una red ya existente:



555. Se recomienda hacer uso de este mecanismo de configuración frente a seleccionar la red Wi-Fi desde el listado de redes disponibles en el “Comm Manager” (menú “Inicio – Configuración – Controles inalámbricos – WLAN”), ya que en este segundo caso, no es posible identificar los mecanismos de seguridad de la red, y únicamente es posible configurar la contraseña de acceso para la red seleccionada (“WLAN” en el ejemplo inferior):



556. Todas las redes que implementan algún tipo de mecanismo de seguridad, WEP, WPA ó WPA2, aparecen con un candado en el icono de la red, pero no es posible diferenciar el mecanismo de seguridad empleado específicamente desde el “Comm Manager” (menú “Inicio – Configuración – Controles inalámbricos – WLAN”). Las redes Wi-Fi son ordenadas según la intensidad de la señal (de mayor a menor intensidad).
557. Por tanto, antes de establecer una primera conexión con una nueva red Wi-Fi, se recomienda agregar la nueva red Wi-Fi de forma manual (en lugar de a través del “Comm Manager”), con el objetivo de poder especificar todas las opciones de configuración recomendadas desde el punto de vista de seguridad (descritas a continuación).
558. El proceso de configuración de la contraseña, tanto desde el menú de configuración Wi-Fi como desde el “Comm Manager”, no oculta el texto introducido en pantalla (por ejemplo con el carácter “\*”), por lo que el usuario debe prestar atención a cómo y dónde introduce la contraseña de conexión a la red Wi-Fi para evitar que un potencial atacante la obtenga mediante la visualización de la pantalla del dispositivo móvil.
559. Dentro de las opciones de configuración, la primera pantalla de configuración hace posible especificar el nombre de la red (SSID), si conecta a Internet o Trabajo (ver apartado “5.21.2. Perfil de conexión: Internet o Trabajo”), si se trata de una red oculta (parámetro analizado en detalle a continuación), y si es una red Wi-Fi entre equipos o dispositivos (ad-hoc):



560. Se recomienda no marcar la casilla “Ésta es una red oculta”, necesaria a la hora de intentar conectarse a redes Wi-Fi ocultas, es decir, que no especifican el nombre de la red (SSID, Service Set Identifier) en las tramas de anuncio de *broadcast* o *beacons*, redes también conocidas como *nonbroadcast*.
561. Aunque en primera instancia puede parecer que el uso de redes Wi-Fi ocultas es una opción más segura, en realidad no es así, ya que es sencillo para un potencial atacante descubrir su existencia e incluso el nombre de esas supuestamente redes ocultas.
562. Sin embargo, el uso de una red oculta implica reducir el nivel de seguridad en los clientes Wi-Fi que se conectan a ella, como por ejemplo los dispositivos móviles basados en Windows Mobile 6.5. Si una red está oculta, los clientes Wi-Fi se verán obligados a comprobar de forma explícita si está presente, generando tramas (de tipo *probe request*) que desvelan el nombre de la red, y lo que es más crítico, que les exponen frente a ataques de suplantación de dicha red por parte de un potencial atacante (especialmente cuando la red no emplea mecanismos de seguridad).
563. Windows Mobile 6.5 implementa de forma adecuada la especificación Wi-Fi (exceptuando la vulnerabilidad mencionada posteriormente), no generando tráfico que desvele la lista de redes Wi-Fi configuradas en el dispositivo móvil (conocida como la PNL, *Preferred Network List*), escenario similar al existente en equipos de escritorio basados en Windows XP con la actualización de seguridad KB917021 aplicada [Ref.-50].
564. Sin embargo, para todas aquellas redes configuradas en las que se seleccione la opción “Ésta es una red oculta”, Windows Mobile 6.5 sí generará tráfico que desvelará las redes Wi-Fi disponibles en su lista de redes e intentará conectarse a ellas, escenario que puede ser empleado por un potencial atacante para disponer de conectividad con el dispositivo móvil y proceder a explotar vulnerabilidades en el mismo.

565. En la imagen inferior, el dispositivo móvil intenta descubrir la presencia de dos redes ocultas disponibles en su configuración, “wifi” y “Taddong”, durante el proceso de encendido del terminal, cada vez que se produce la activación del interfaz Wi-Fi y periódicamente una vez el interfaz Wi-Fi ha sido activado:

```

812 08:46:39.349530 00:23:76: ff:ff:ff:ff:ff:ff IEEE -21 Probe Request, SN=94, FN=0, Flags=.....C, SSID="wifi"
814 08:46:39.372034 00:23:76: ff:ff:ff:ff:ff:ff IEEE -24 Probe Request, SN=95, FN=0, Flags=.....C, SSID="wifi"
815 08:46:39.392439 00:23:76: ff:ff:ff:ff:ff:ff IEEE -23 Probe Request, SN=96, FN=0, Flags=.....C, SSID="wifi"
816 08:46:39.414941 00:23:76: ff:ff:ff:ff:ff:ff IEEE -26 Probe Request, SN=97, FN=0, Flags=.....C, SSID="wifi"
817 08:46:39.435367 00:23:76: ff:ff:ff:ff:ff:ff IEEE -24 Probe Request, SN=98, FN=0, Flags=.....C, SSID="wifi"
830 08:46:40.237110 00:23:76: ff:ff:ff:ff:ff:ff IEEE -24 Probe Request, SN=119, FN=0, Flags=.....C, SSID="Taddong"
831 08:46:40.257335 00:23:76: ff:ff:ff:ff:ff:ff IEEE -23 Probe Request, SN=120, FN=0, Flags=.....C, SSID="Taddong"
833 08:46:40.280230 00:23:76: ff:ff:ff:ff:ff:ff IEEE -25 Probe Request, SN=121, FN=0, Flags=.....C, SSID="Taddong"
834 08:46:40.300602 00:23:76: ff:ff:ff:ff:ff:ff IEEE -24 Probe Request, SN=122, FN=0, Flags=.....C, SSID="Taddong"
835 08:46:40.323090 00:23:76: ff:ff:ff:ff:ff:ff IEEE -25 Probe Request, SN=123, FN=0, Flags=.....C, SSID="Taddong"

```

**Nota:** El comportamiento esperado de Windows Mobile 6.5 es que el dispositivo móvil desvele únicamente las redes Wi-Fi ocultas configuradas. Sin embargo, durante las pruebas realizadas se verificó que una vez el interfaz Wi-Fi ha sido activado, cada 30 segundos, desvela todas las redes configuradas, independientemente de si han sido clasificadas como ocultas o no. En el ejemplo inferior, “wifi” y “Taddong” son redes ocultas, mientras que “ejemplo” y “hotspot” son redes visibles para las que no se debería generar tráfico:

```

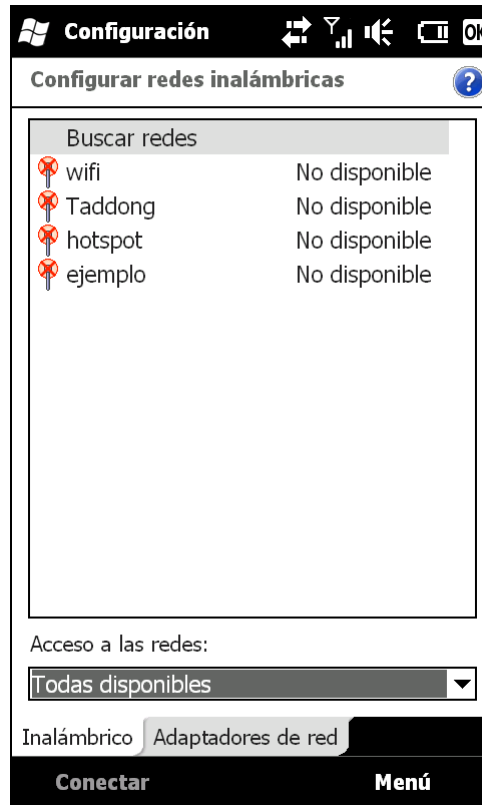
14139 09:01:55.555507 00:23:76: ff:ff:ff:ff:ff:ff IEEE -38 Probe Request, SN=252, FN=0, Flags=.....C, SSID="wifi"
14140 09:01:55.556143 00:23:76: ff:ff:ff:ff:ff:ff IEEE -38 Probe Request, SN=253, FN=0, Flags=.....C, SSID="Taddong"
14141 09:01:55.556885 00:23:76: ff:ff:ff:ff:ff:ff IEEE -17 Probe Request, SN=254, FN=0, Flags=.....C, SSID="ejemplo"
14142 09:01:55.577661 00:23:76: ff:ff:ff:ff:ff:ff IEEE -15 Probe Request, SN=255, FN=0, Flags=.....C, SSID="hotspot"
14143 09:01:55.579007 00:23:76: ff:ff:ff:ff:ff:ff IEEE -14 Probe Request, SN=257, FN=0, Flags=.....C, SSID="Taddong"
14144 09:01:55.598288 00:23:76: ff:ff:ff:ff:ff:ff IEEE -13 Probe Request, SN=259, FN=0, Flags=.....C, SSID="hotspot"
14145 09:01:55.599636 00:23:76: ff:ff:ff:ff:ff:ff IEEE -18 Probe Request, SN=261, FN=0, Flags=.....C, SSID="Taddong"
14805 09:02:25.737771 00:23:76: ff:ff:ff:ff:ff:ff IEEE -24 Probe Request, SN=343, FN=0, Flags=.....C, SSID="hotspot"
14806 09:02:25.738377 00:23:76: ff:ff:ff:ff:ff:ff IEEE -38 Probe Request, SN=344, FN=0, Flags=.....C, SSID="wifi"
14807 09:02:25.739125 00:23:76: ff:ff:ff:ff:ff:ff IEEE -20 Probe Request, SN=345, FN=0, Flags=.....C, SSID="Taddong"
14808 09:02:25.739880 00:23:76: ff:ff:ff:ff:ff:ff IEEE -38 Probe Request, SN=346, FN=0, Flags=.....C, SSID="ejemplo"
14809 09:02:25.759789 00:23:76: ff:ff:ff:ff:ff:ff IEEE -22 Probe Request, SN=349, FN=0, Flags=.....C, SSID="Taddong"

```

Este no es el comportamiento esperado al clasificar una red Wi-Fi como oculta en Windows Mobile 6.5, por tanto, debido a la existencia de esta vulnerabilidad de seguridad, el parámetro “Ésta es una red oculta” no tiene efecto en la versión analizada (última versión disponible).

Esta vulnerabilidad (TAD-2010-003) de revelación de información ha sido confirmada por Microsoft, aunque no publicará una actualización para solucionarla [Ref.- 107].

566. La lista de redes preferidas (PNL), es decir, a las que se ha conectado previamente el dispositivo móvil o que han sido configuradas en el mismo (ver apartado “5.18.6. Conexión automática a redes Wi-Fi”), puede ser visualizada tras deshabilitar el interfaz Wi-Fi, desde el menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Conexiones – Wi-Fi”. Seleccionar el botón “Redes inalámbricas” y la pestaña “Inalámbrico”(por defecto):



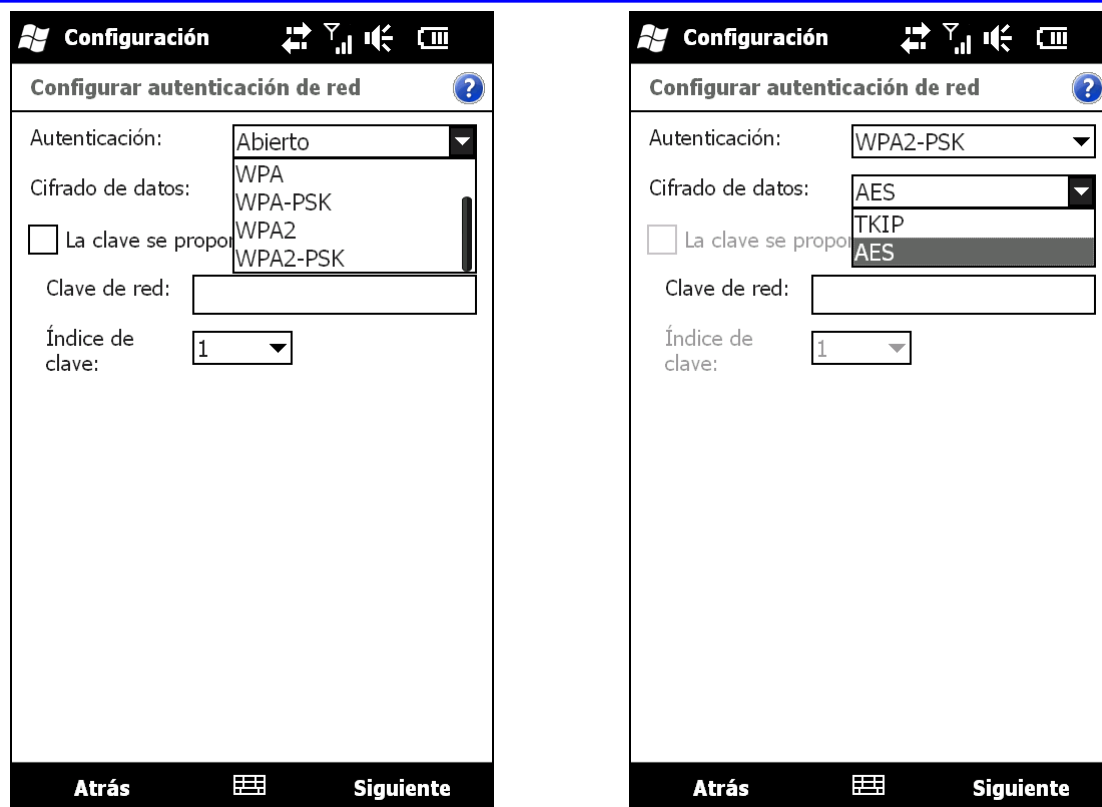
**Nota:** los detalles de configuración de las redes Wi-Fi son almacenados en la siguiente clave del registro en formato binario. Para cada red Wi-Fi, existe un parámetro denominado “Static#0000”, dónde el número “0000” aumenta secuencialmente para cada red Wi-Fi de la lista de redes preferidas. El valor del parámetro “ActiveSettings” es una copia de uno de los parámetros “Static#nnnn” e indica la red Wi-Fi a la que se está conectado actualmente:

```
HKLM\Software\Microsoft\WZCSVC\Parameters\Interfaces\BCMSDDHD1
```

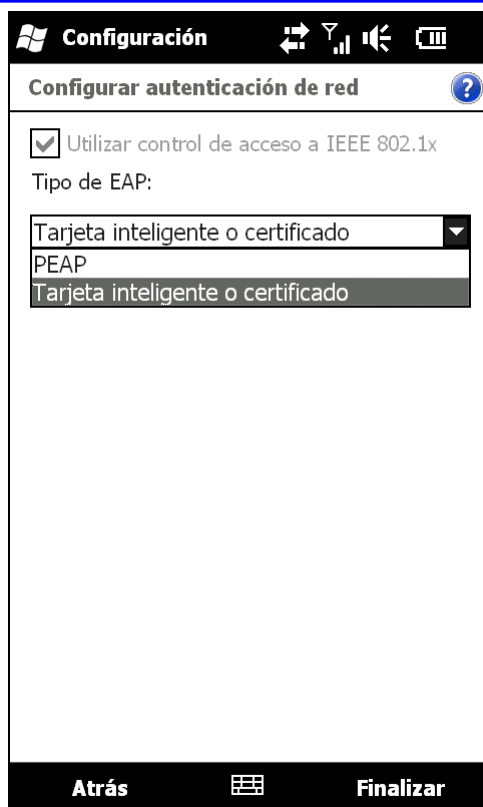
Adicionalmente las siguientes dos claves del registro también incluyen referencias a las redes Wi-Fi configuradas en el dispositivo móvil, como proveedores de comunicaciones y su configuración EAP, respectivamente:

```
HKLM\Comm\ConnMgr\Providers\{9eefcedf-a6bc-4457-a8ae-fb664a196450}
HKCU\Comm\EAPOL\Config
```

567. Continuando con las opciones de configuración al agregar una nueva red Wi-Fi, la segunda pantalla de configuración permite especificar el mecanismo de autenticación y de cifrado de datos, así como indicar la contraseña empleada por la red Wi-Fi:



568. Se recomienda conectarse únicamente a redes que emplean WPA2 (Personal, WPA2-PSK, o Enterprise, WPA2) como mecanismo de autenticación, y AES como mecanismo de cifrado. En su defecto, debería emplearse WPA/TKIP.
569. En caso de emplear WPA2 (o WPA) en su versión Enterprise, con mecanismos basados en 802.1X/EAP, la siguiente pantalla de configuración permite seleccionar el tipo de mecanismo EAP empleado para la autenticación dentro de aquellos soportados por Windows Mobile 6.5. Windows Mobile 6.5 incluye soporte para los dos tipos de EAP disponibles en los sistemas operativos de escritorio de Microsoft: “PEAP” (Protected EAP) o “Tarjeta inteligente o certificado” (correspondiente al estándar EAP-TLS):



570. Para poder hacer uso de autenticación mediante PEAP, es necesario disponer de un certificado digital en el servidor de autenticación de la red Wi-Fi (por ejemplo, RADIUS), y el dispositivo móvil se autenticará mediante usuario y contraseña (MS-CHAPv2), y dominio.

**Nota:** al seleccionar “PEAP” es posible obtener un mensaje de aviso indicando la necesidad de usar un certificado digital personal, pese a que no es necesario disponer de un certificado cliente. Windows Mobile 6.5 genera el siguiente mensaje de error refiriéndose a la necesidad de disponer del certificado digital raíz empleado para generar el certificado usado por el servidor de autenticación de la red Wi-Fi:

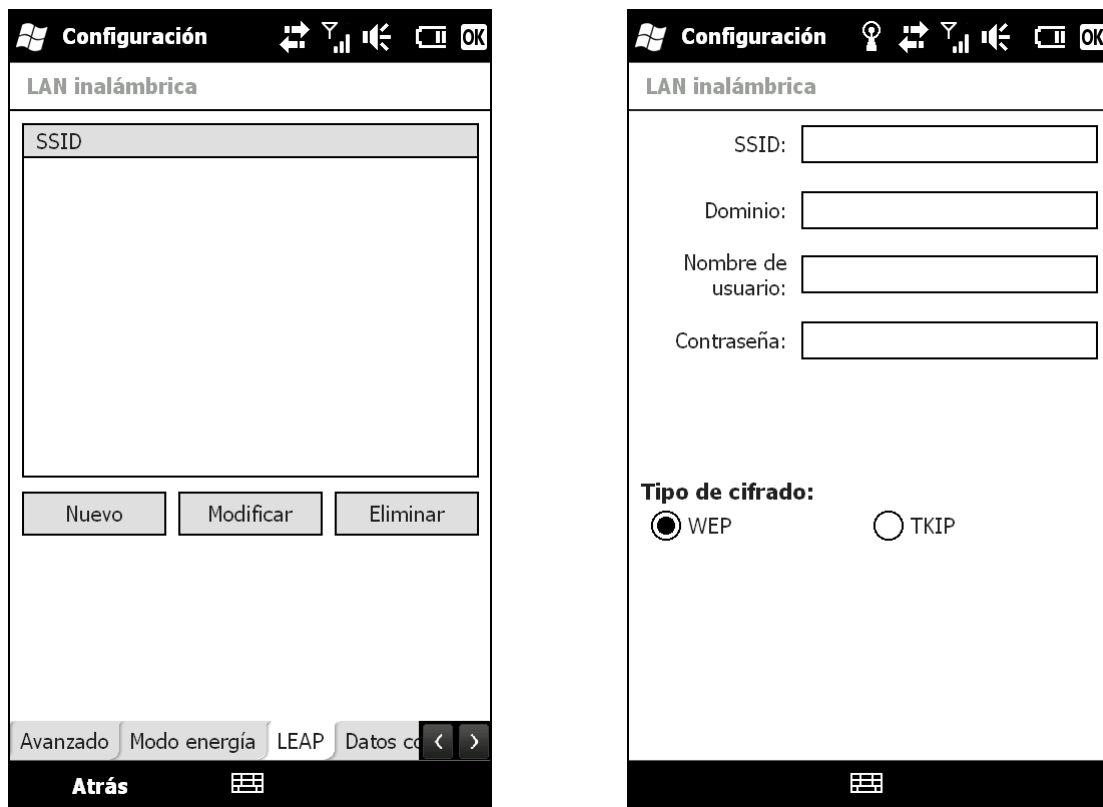


571. Para poder hacer uso de autenticación mediante “Tarjeta inteligente o certificado” (EAP-TLS), es necesario disponer de un certificado digital tanto en el servidor de autenticación de la red Wi-Fi, como en el dispositivo móvil.
572. Por tanto, en el caso de EAP-TLS sí es necesario importar un certificado digital personal (normalmente en formato PKCS12) en el dispositivo móvil. Para instalar el certificado personal basta con transferir el fichero del certificado digital personal (.PFX o .P12) al dispositivo móvil y pulsar sobre él desde el explorador de ficheros, proporcionando la contraseña de protección del fichero que contiene el certificado personal [Ref.- 75].
573. Una vez el certificado personal ha sido importado en el dispositivo móvil, estará disponible a través del menú “Inicio – Configuración – Seguridad – Certificados”, en la pestaña “Personal” (pudiendo también incluir certificados raíz e intermedios).

**Nota:** tanto en el caso de autenticación “PEAP” como “Tarjeta inteligente o certificado”, es necesario cargar previamente en Windows Mobile 6.5 el certificado digital de la autoridad certificadora (CA), raíz o intermedia, empleada para generar los certificados digitales asociados al servidor de autenticación de la red Wi-Fi, salvo que se usen certificados emitidos por una de las CA’s ya existentes en Windows Mobile 6.5 [Ref.- 75].

Para instalar el certificado basta con transferir el fichero del certificado digital (.CER, .DER o .P7B) al dispositivo móvil y pulsar sobre él desde el explorador de ficheros. Una vez el certificado ha sido importado en el dispositivo móvil, estará disponible a través del menú “Inicio – Configuración – Seguridad – Certificados”, en la pestaña “Intermedio” o “Raíz” (dependiendo del tipo de certificado).

574. La configuración de autenticación de cada red Wi-Fi configurada se almacena en la clave del registro “HKEY\_CURRENT\_USER\Comm\EAPOL\Config\<nombre\_red>”, a través de los parámetros “EapTypeId” y “Enable8021x”. Por ejemplo, en el caso de emplear autenticación PSK, por ejemplo en redes basadas en WPA o WPA2, los valores de ambos parámetros son “13” y “1” respectivamente.
575. Los tipos de EAP soportados y sus parámetros de configuración están definidos en la clave “HKEY\_LOCAL\_MACHINE\Comm\EAP\Extension” del registro.
576. Windows Mobile 6.5 también dispone de soporte para redes Wi-Fi basadas en autenticación LEAP (*Lightweight Extensible Authentication Protocol*, tecnología diseñada por Cisco) a través de la pestaña “LEAP” del menú de configuración de la red Wi-Fi (menú “Inicio – Configuración – Controles inalámbricos – WLAN”, botón “Avanzado”):



577. La disponibilidad de LEAP se refleja en el parámetro “EnableLeap” (REG\_SZ) de la clave “HKEY\_LOCAL\_MACHINE\Comm\BCMSDDHD1\Parms” del registro.
578. Los perfiles de LEAP se almacenan en la misma clave del registro, bajo el parámetro binario “HTCLEAPProfile”, y el número de perfiles está indicado por el parámetro “HTCLEAPValidProfileNum” (REG\_DWORD).
579. Debido a las múltiples vulnerabilidades asociadas al protocolo de autenticación LEAP, no se recomienda su utilización, al exponer las credenciales de acceso (usuario y contraseña) frente a potenciales atacantes y, en concreto, frente a ataques de diccionario. Adicionalmente, LEAP está asociado al uso de redes Wi-Fi basadas en WEP o TKIP (WPA), tecnologías Wi-Fi con vulnerabilidades de seguridad públicamente conocidas.
580. En resumen, desde el punto de vista de seguridad de Windows Mobile 6.5 como cliente Wi-Fi, se recomienda hacer uso de redes inalámbricas no ocultas, basadas en WPA2 con

cifrado AES, y autenticación de tipo Personal, con una contraseña de acceso (PSK, *Personal Shared Key*) suficientemente robusta (más de 20 caracteres), o de tipo Enterprise, basada en mecanismos de autenticación 802.1X/EAP, y de tipo EAP-TLS preferiblemente.

**Nota:** con el objetivo de proteger el dispositivo móvil y aumentar su nivel de seguridad, se desaconseja el uso de redes inalámbricas públicas y abiertas, con un nivel de seguridad reducido o inexistente (sin mecanismos de autenticación y cifrado), como por ejemplo *hotspots* Wi-Fi disponibles en hoteles, aeropuertos o centros de conferencias [Ref.- 1].

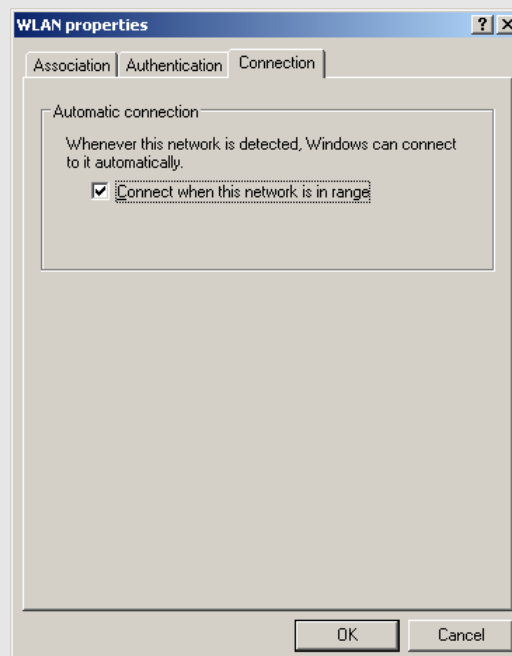
Los riesgos de seguridad asociados a este tipo de entornos incluyen la captura e interceptación del tráfico y datos por parte de un potencial atacante, la posibilidad de inyección de tráfico para la realización de ataques directos y accesos no autorizados contra el dispositivo móvil, ataques de suplantación de la red, y a ataques de denegación de servicio, entre otros.

### 5.18.6 CONEXIÓN AUTOMÁTICA A REDES WI-FI

581. Windows Mobile 6.5 intenta conectarse automáticamente a las redes Wi-Fi existentes en su lista de redes preferidas. Si alguna de estas redes Wi-Fi está disponible, establecerá la conexión.

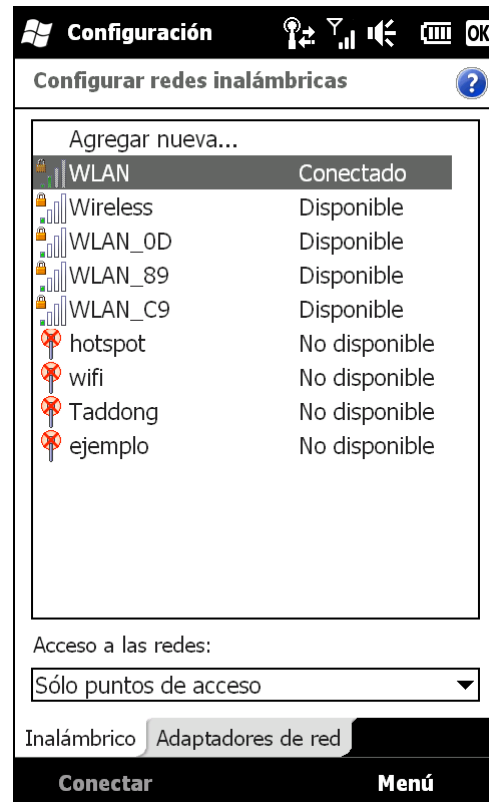
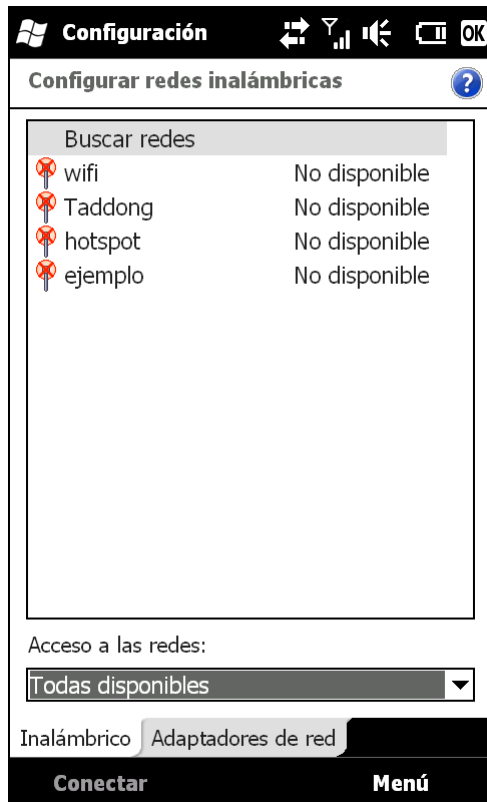
**Nota:** no se ha identificado ninguna opción de configuración, ni en el interfaz de usuario ni a través del registro (como parámetro individual), en Windows Mobile 6.5 para deshabilitar el proceso de conexión automática a redes Wi-Fi si el interfaz Wi-Fi está activo.

Los sistemas operativos de escritorio de Microsoft, por ejemplo Windows XP (imagen inferior), sí disponen de esta opción, configurable de forma individual para cada una de las redes disponibles en la lista de redes preferidas:

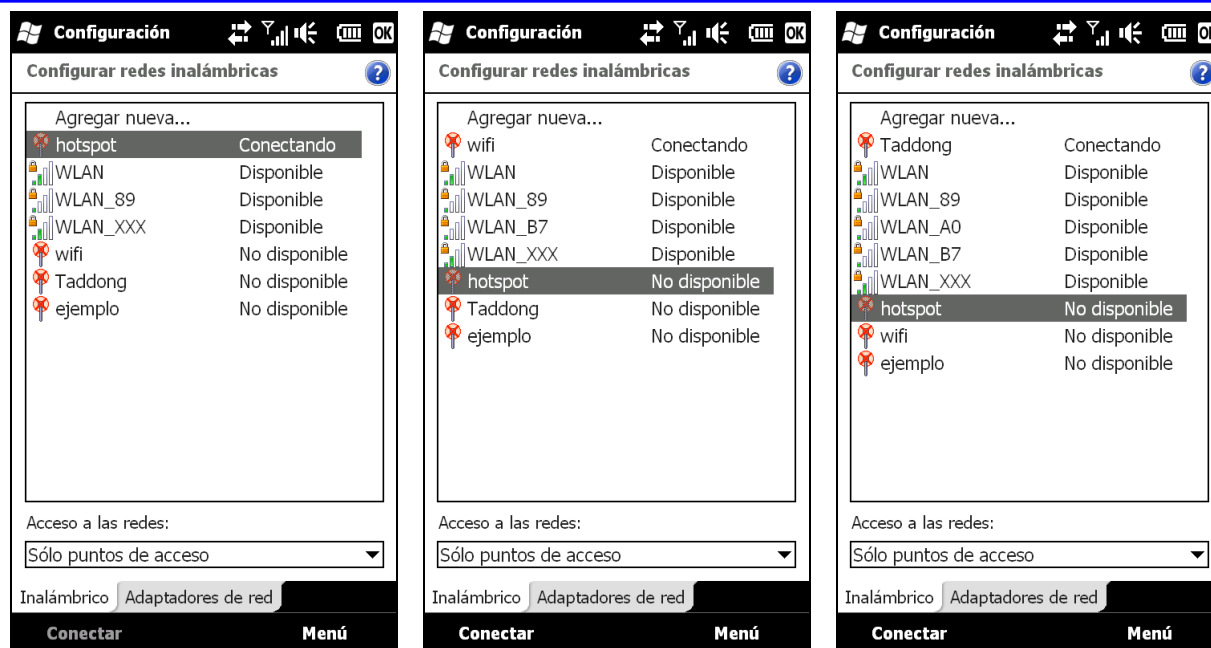


En Windows Mobile 6.5 no es posible deshabilitar la conexión automática ni a través de la modificación del perfil de cada una de las redes preferidas mediante la manipulación directa del registro.

582. La lista de redes preferidas (PNL) está disponible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Conexiones – Wi-Fi”. Seleccionar el botón “Redes inalámbricas”, y la pestaña “Inalámbrico”.
583. Las redes preferidas, es decir, a las que se ha conectado previamente el dispositivo móvil o que han sido configuradas en el mismo, y que no están actualmente disponibles aparecen con un icono rojo indicando este estado y el texto “No disponible”, incluso cuando el interfaz Wi-Fi del dispositivo móvil está deshabilitado (imagen inferior izquierda):



584. Es incluso posible visualizar el comportamiento de Windows Mobile 6.5 en tiempo real y ver como intenta conectarse a las redes Wi-Fi desde el interfaz de usuario del dispositivo móvil, recorriendo secuencialmente la lista de redes preferidas y realizando intentos de conexión con cada una de ellas (ver primera red Wi-Fi de la lista en cada una de las imágenes inferiores, con el texto “Conectando”):



585. Debe tenerse en cuenta que no existe la opción de desconectarse de la red a la que el dispositivo móvil está conectado actualmente. La única opción disponible es deshabilitar el interfaz Wi-Fi.

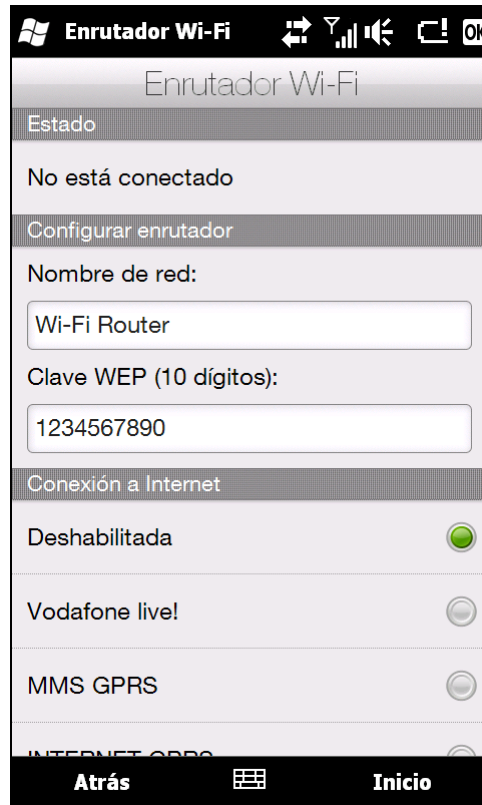
### 5.18.7 ENRUTADOR WI-FI

586. Windows Mobile 6.5, y en concreto el dispositivo móvil analizado (al ser una aplicación desarrollada por HTC), dispone de capacidades para actuar de punto de acceso Wi-Fi y *router* (o enrutador) hacia Internet, proporcionando acceso a múltiples dispositivos vía Wi-Fi a su conexión de datos de telefonía móvil (2G/3G).

587. La funcionalidad de enrutador Wi-Fi está disponible desde el menú “Inicio – Enrutador Wi-Fi” o desde el “Comm Manager” (menú “Inicio – Configuración – Controles inalámbricos”) a través del botón deslizante de activación y desactivación asociado a la sección “Enrutador Wi-Fi”. Su activación requiere disponer de cuatro elementos de comunicaciones activos: las capacidades de telefonía y de telefonía de datos, así como las capacidades Wi-Fi y de enrutador Wi-Fi:



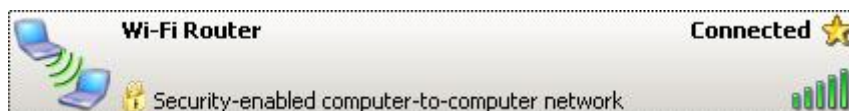
588. Se recomienda no habilitar las capacidades de enrutador Wi-Fi en el dispositivo móvil salvo que se quiera hacer un uso limitado y controlado de esta funcionalidad, ya que la red Wi-Fi asociada sólo puede ser protegida mediante WEP, tecnología de seguridad inalámbrica con múltiples vulnerabilidades de seguridad ampliamente conocidas, no disponiendo de ningún otro mecanismo o control de seguridad para restringir qué dispositivos cliente puede establecer una conexión con el enrutador Wi-Fi.
589. En caso de ser activado el enrutador Wi-Fi, se recomienda modificar el nombre de la red Wi-Fi (o SSID) anunciada por el dispositivo móvil por defecto ("Wi-Fi Router"), así como la contraseña WEP disponible por defecto ("0123456789"; sólo permite 10 dígitos):



590. La activación de la funcionalidad se refleja en la siguiente clave del registro, dónde se almacena el estado del enrutador Wi-Fi (el valor “0” indica que está desconectado, el valor “2” que está conectando, el valor “0xFF” que está siendo deshabilitado, etc), la conexión de telefonía de datos a usar, el nombre de la red Wi-Fi, o la clave sin cifrar, entre otros:

```
[HKEY_LOCAL_MACHINE\Software\HTC\CMInternetSharing]
"CMStatus"=dword:00000000
"WEPKey"="0123456789"
"TargetDataConnection"="GPRS VACIA"
"TargetSSID"="Wi-Fi Router"
```

591. Se recomienda emplear como conexión de telefonía de datos por defecto la conexión “GPRS VACIA” (creada en el apartado “5.20. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”), con el objetivo de evitar que la activación no intencionada de esta funcionalidad proporcione capacidades de conexión a Internet.
592. La red Wi-Fi creada es de tipo *ad-hoc*, o entre equipos, protegida por WEP, se anuncia en el canal 1 (de 802.11), y proporciona incluso capacidades de servidor DHCP para la asignación de direcciones IP a los dispositivos cliente que se conectan a ella:



## 5.19 COMUNICACIONES GSM (2G): MENSAJES DE TEXTO (SMS)

593. Las capacidades de mensajería de texto (SMS, Short Message Service) de los dispositivos móviles permite el envío de mensajes cortos empleando la infraestructura GSM (Global

System for Mobile communications, o 2G) o UMTS (Universal Mobile Telecommunications System, o 3G).

594. El primer nivel de protección asociado al sistema de mensajería de texto pasa por la concienciación del usuario desde el punto de vista de seguridad, teniendo en cuenta que la implementación de este módulo en los dispositivos móviles actuales proporciona numerosas funcionalidades, y no únicamente la visualización de mensajes de texto.
595. Entre las funcionalidades avanzadas se encuentra la posibilidad de mostrar contenidos de texto y contenidos web (HTML, Javascript, etc), así como gestionar datos binarios, como tonos de llamada, e intercambiar ficheros multimedia (audio, vídeo e imágenes) con MMS.

**Nota:** las variantes avanzadas de mensajería móvil, como EMS (Enhanced Messaging Service) y MMS (Multimedia Message Service), hacen uso de conexiones de datos de telefonía móvil (GPRS, EDGE, y UMTS) y no de voz (GSM) como SMS.

596. Debido a las diferentes vulnerabilidades asociadas al módulo de mensajería de texto en múltiples dispositivos móviles actuales, incluyendo Windows Mobile [Ref.- 1], se recomienda que el usuario actúe con prudencia ante la lectura de nuevos mensajes de texto, especialmente los recibidos de fuentes desconocidas.
597. Se recomienda no abrir ningún mensaje de texto no esperado o solicitado, práctica similar a la empleada para la gestión de correos electrónicos. A la hora de acceder y procesar los contenidos del buzón de entrada de mensajes de texto del dispositivo móvil, el usuario debería seguir las mejores prácticas de seguridad, como por ejemplo:
- No deberían abrirse mensajes de texto recibidos desde números desconocidos, ni ejecutar o permitir la instalación de contenidos adjuntos (configuraciones, binarios o multimedia) asociados a mensajes SMS/MMS no esperados.
  - En su lugar, se debería proceder a borrar el mensaje directamente.
  - En caso de acceder a los mensajes, debería desconfiarse de su contenido, y tener especial cuidado, por ejemplo, con la utilización de enlaces a sitios web externos.
598. Adicionalmente, es necesario tener en cuenta que los mensajes de texto pueden contener información sensible y confidencial. Por ejemplo, al gestionar el buzón de voz de un usuario, los operadores de telefonía móvil envían todos los detalles de acceso al buzón de voz, incluido el PIN, mediante un mensaje de texto, como los dos ejemplos de mensajes de texto de dos operadores de telefonía móvil españoles diferentes de las imágenes inferiores. El acceso a dicho mensaje por parte de un potencial atacante permitiría disponer de control completo del buzón de voz del usuario:

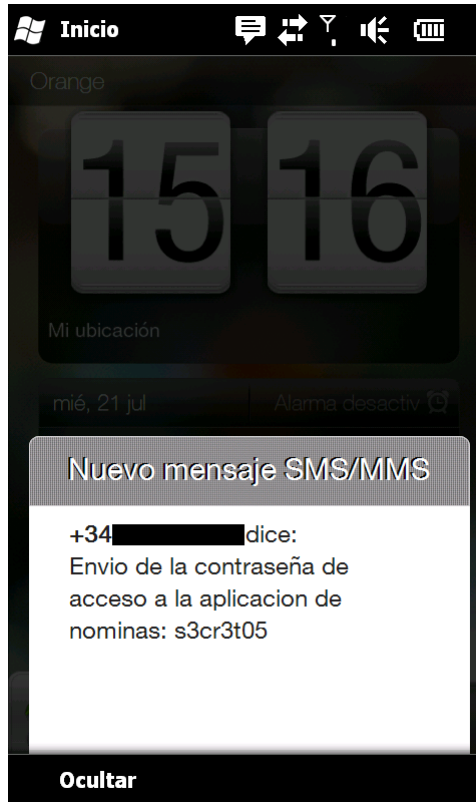


599. Los nuevos mecanismos de autenticación de la banca online también emplean los mensajes de texto para el envío de contraseñas de un solo uso para la realización de operaciones bancarias críticas. El acceso a dicho mensaje por parte de un potencial atacante permitiría completar la operación, como por ejemplo, una transferencia bancaria.
600. El sistema de mensajería de texto de telefonía móvil ha sido rediseñado en Windows Mobile 6.5 (frente a versiones previas de este sistema operativo).

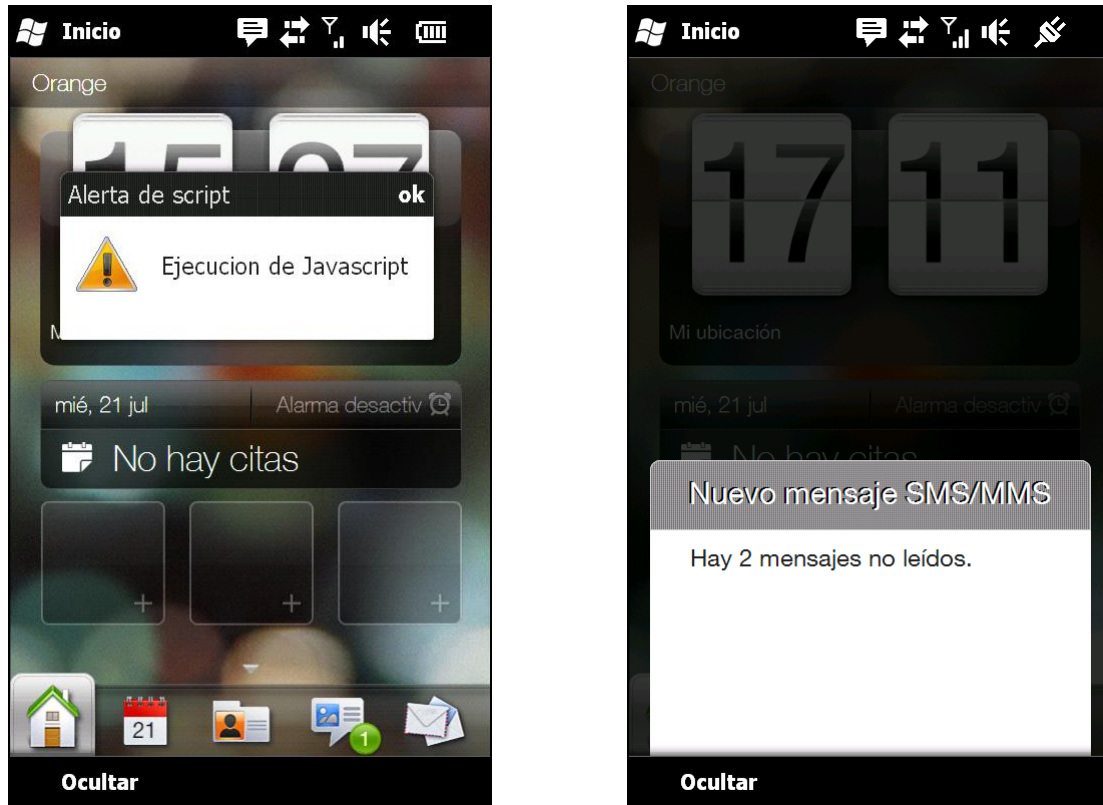
### 5.19.1 EJECUCIÓN DE CONTENIDO WEB EN MENSAJES DE TEXTO

601. Algunos dispositivos móviles son vulnerables a la recepción de mensajes de texto (SMS) que contienen código HTML, ya que dicho contenido no es filtrado adecuadamente por el terminal, y en concreto, por la aplicación de visualización de mensajes de texto [Ref.- 1].
602. Mediante el envío de SMS maliciosos y la inyección de código HTML, y con la simple lectura del mensaje por parte del usuario, un potencial atacante puede abrir conexiones con sitios web maliciosos, descargar ficheros, forzar la descarga continua de contenidos, solicitar la instalación de una nueva autoridad certificadora raíz (root CA) en el dispositivo móvil, etc.
603. Esta vulnerabilidad fue descubierta en dispositivos móviles Palm con WebOS [Ref.- 24], donde incluso, un ataque podría apagar la radio (de telefonía móvil) o borrar todos los contenidos del terminal (modo Palm Demo) a través de códigos GSM específicos.
604. Las capacidades de previsualización de mensajes de texto de Windows Mobile 6.5 en dispositivos móviles HTC son también vulnerables a este tipo de inyección de contenidos web, permitiendo a un potencial atacante, entre otros, efectuar redirecciones a sitios web, o ejecutar código Javascript [Ref.- 25].

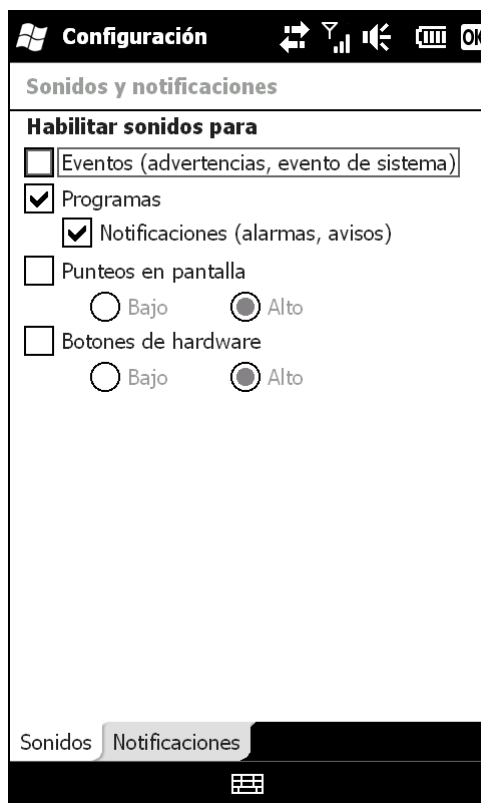
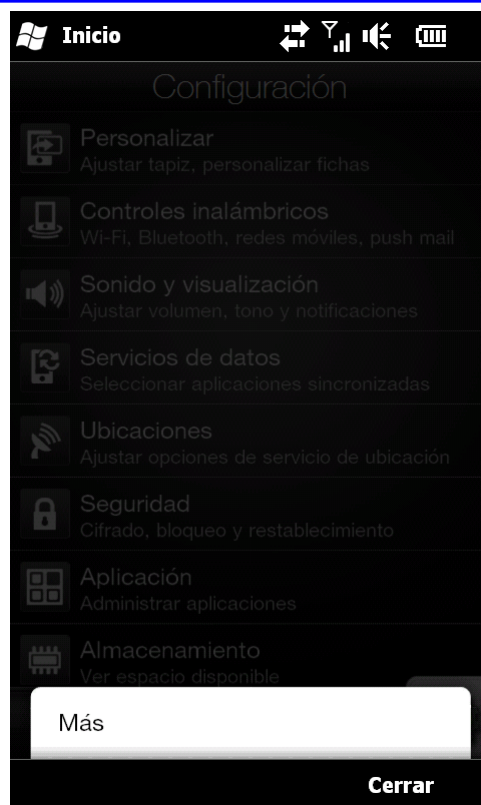
605. La funcionalidad de previsualización de Windows Mobile 6.5 muestra en la pantalla principal los mensajes de texto recibidos. Pese a que podría desvelar información potencialmente confidencial a un potencial atacante, sólo está disponible si la pantalla del dispositivo móvil no está bloqueada, minimizando notablemente su impacto. La información del mensaje mostrada incluye detalles del remitente y el contenido del mensaje:



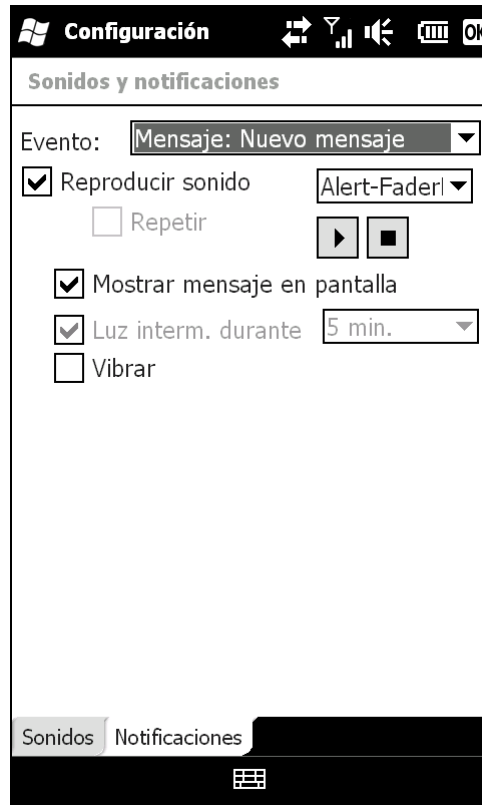
606. Pese a que la publicación de la vulnerabilidad referencia a la misma como un problema de Cross-Site Scripting (XSS) [Ref.- 25], realmente no se trata de una vulnerabilidad XSS (propias de las aplicaciones web y no de los clientes web), sino de una vulnerabilidad de procesamiento e interpretación de contenido web por parte del terminal.
607. La imagen inferior izquierda muestra la ejecución de código Javascript por el módulo de previsualización de la pantalla principal del dispositivo móvil, tras recibir un mensaje de texto con contenido “malicioso”: `<script>alert('Ejecucion de Javascript')</script>`.



608. Los dispositivos móviles HTC con Windows Mobile 6.5 son vulnerables si el mensaje de texto malicioso es el primer mensaje recibido, es decir, si no hay ningún otro mensaje de texto sin leer pendiente, ya que en ese caso, las capacidades de previsualización no muestran el contenido del mensaje malicioso, sino una notificación del número de mensajes pendientes: “Hay N mensajes no leídos.” (imagen superior derecha).
609. Los mensajes de texto sólo serán previsualizados si esta funcionalidad ha sido habilitada. Es posible activar o desactivar esta previsualización a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, accediendo a la sección “Sonidos y notificaciones”:



610. Mediante la pestaña “Notificaciones” de esta sección es posible configurar diferentes parámetros para múltiples eventos. En concreto, el evento “Mensaje: Nuevo Mensaje” permite configurar el comportamiento del dispositivo móvil al recibir un nuevo mensaje de texto, y la opción “Mostrar mensaje en pantalla” determina si las capacidades de previsualización están o no disponibles (es decir, si se es o no vulnerable):



611. En el dispositivo móvil HTC HD2 con Windows Mobile 6.5 empleado para la elaboración de la presente guía, la previsualización de mensajes nuevos de texto está deshabilitada por defecto, por lo que el terminal no es vulnerable. Sin embargo, otros modelos HTC pueden tener la funcionalidad habilitada por defecto.
612. La siguiente clave de registro determina si se muestra el mensaje en pantalla. El valor “5” indica que la notificación está deshabilitada (opción recomendada), y el valor “13” (0x0D) que ha sido habilitada:
- ```
[HKEY_CURRENT_USER\ControlPanel\Notifications\{A877D65B-239C-47a7-9304-0D347F580408}]
"Options"=dword:00000005
```
613. Adicionalmente, se podría eliminar la vulnerabilidad mediante la aplicación de la actualización de seguridad facilitada por HTC que soluciona el problema. La vulnerabilidad fue anunciada públicamente el 22 de abril de 2010 [Ref.- 25]. La última actualización para el sistema SMS de HTC para la versión en español (y en inglés) de Windows Mobile 6.5 es del 5 de julio de 2010 [Ref.- 48] [Ref.- 47], y soluciona la vulnerabilidad pese a que en la descripción no se menciona (ver apartado “5.2.1. Paso a paso: Instalación de la actualización del sistema SMS de HTC”).
614. Una vez la actualización ha sido aplicada y el dispositivo móvil no es vulnerable, al recibirse un mensaje de texto con contenido HTML o Javascript, éste no será interpretado y ejecutado, sino mostrado al usuario como texto:



5.20 COMUNICACIONES GSM (2G) Y UMTS (3G): VOZ Y DATOS

5.20.1 DESACTIVACIÓN DE LAS COMUNICACIONES DE VOZ Y DATOS 2G/3G

615. La principal recomendación de seguridad asociada a las comunicaciones de voz (y SMS) a través de las redes de telefonía móvil en dispositivos móviles es no activar las capacidades de telefonía del terminal salvo que se haga uso de éstas (situación muy habitual, al ser ésta una de las funcionalidades principales de los dispositivos móviles).

Nota: durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía (activado automáticamente la primera vez que se enciende el terminal), el interfaz de telefonía móvil está habilitado, incluso si no se inserta la tarjeta SIM.

Se recomienda desactivar el interfaz de telefonía móvil tan pronto finalice el proceso de configuración inicial, para proceder a la aplicación de las medidas de seguridad seleccionadas.

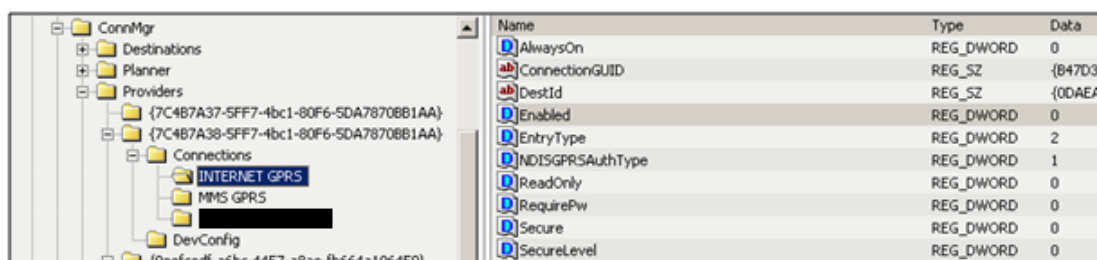
616. Windows Mobile 6.5 permite, a través del “Comm Manager” (menú “Inicio – Configuración – Controles inalámbricos”), deshabilitar de forma individualizada las capacidades de telefonía móvil (voz y SMS), a través del botón deslizante de activación y desactivación asociado a la sección “Teléfono” (imagen inferior izquierda):



617. Al deshabilitar las capacidades de telefonía móvil de voz, si no se dispone de ninguna otra tecnología de comunicaciones habilitada, se activará el “Modo de vuelo” automáticamente, y se deshabilitarán (color gris) las opciones de comunicaciones que requieren disponer de conectividad mediante telefonía móvil: “Conexión de datos” y “Enrutador Wi-Fi” (imagen superior derecha).
618. La principal recomendación de seguridad asociada a las comunicaciones de datos a través de las infraestructuras de telefonía móvil en dispositivos móviles es no activar las capacidades de transmisión y recepción de datos salvo en el caso en el que se esté haciendo uso de éstas, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver, la pila de comunicaciones móviles y cualquiera de los servicios y aplicaciones disponibles a través de esa red y la conexión a Internet.
619. Las conexiones de datos a través de la red de telefonía móvil, GPRS o UMTS (incluyendo MMS), pueden ser deshabilitadas temporalmente a través del “Comm Manager” (menú “Inicio – Configuración – Controles inalámbricos”) y del botón deslizante de activación y desactivación asociado a la sección “Conexión de datos”:



620. Windows Mobile 6.5 no mantiene el estado del interfaz de telefonía de datos tras reiniciar el dispositivo móvil (incluso tras un restablecimiento de software o *soft reset*), es decir, si el interfaz de telefonía de datos estaba activo al apagar el terminal, al encender el dispositivo móvil e introducir el PIN de la tarjeta SIM, no seguirá activo.
621. Igualmente, al salir del modo de vuelo el estado del interfaz de datos de telefonía móvil no será restaurado, y no se activará incluso en el caso de haber estado activo previamente (al activar el modo de vuelo).
622. Sin embargo, tras desactivar la “Conexión de datos”, si alguna aplicación requiere disponer de conectividad (por ejemplo, navegación desde Internet Explorer Mobile, o actualización de datos de alguna aplicación cliente, como “Clima” o “Bolsa”) la conexión de telefonía de datos volverá a ser activada automáticamente. Para evitar cualquier tipo de comunicación se recomienda crear un perfil de conexión de datos vacío (descrito posteriormente en este apartado).
623. La clave del registro asociada a la desactivación de las conexiones de telefonía de datos es la siguiente, “HKEY_LOCAL_MACHINE\Comm\ConnMgr\Providers\{7C4B7A38-5FF7-4bc1-80F6-5DA7870BB1AA}\Connections”, donde cada conexión de datos dispone de un parámetro “Enabled”, que de tener el valor “0”, indica que la conexión está deshabilitada:



624. Para deshabilitar las conexiones de datos de telefonía móvil, se recomienda fijar el valor de “Enable” a “0” para todas las conexiones disponibles, por ejemplo el acceso a Internet mediante GPRS (las referencias del registro a GPRS también incluyen UMTS, es decir, 2G y 3G), la conexión para el intercambio de mensajes multimedia (MMS), WAP y otras conexiones habilitadas por el proveedor de telefonía móvil a través de la tarjeta SIM.

Nota: se ha observado que en algunos terminales con Windows Mobile 6.5 el fijar el valor de “enable” a “0” deshabilita sólo la conexión de forma temporal. Cuando el usuario fuerza la conexión, este valor de registro vuelve a fijarse a “1”. Para evitar conexiones no deseadas se recomienda la creación de una conexión GPRS vacía, detallada a continuación.

625. Una vez deshabilitadas, junto a la configuración de una conexión GPRS vacía (detallada a continuación), los intentos de conexión de datos a través de la infraestructura de telefonía móvil generarán un mensaje de error indicando que no es posible conectar mediante GPRS (mostrado en el apartado “4. Entorno de aplicación de esta guía”).

Nota: además de la seguridad, una de las preocupaciones de los usuarios de dispositivos móviles sin tarifa plana de conexión de datos son los cargos asociados al uso de las comunicaciones de datos a través de las redes de telefonía móvil (2G/3G), especialmente cuando el contrato tiene gastos asociados por la cantidad de datos transmitidos y/o por tiempo o número de conexiones establecidas, o se viaja internacionalmente (itinerancia o *roaming*). Múltiples aplicaciones en Windows Mobile 6.5 pueden iniciar este tipo de conexiones de datos en diferentes momentos del día.

Nota: la desactivación de las conexiones de datos también afecta a los mensajes multimedia (MMS). Adicionalmente Windows Mobile 6.5 permite la activación de diferentes políticas de seguridad para restringir los mensajes de servicio y notificación empleados por los operadores de telefonía móvil para aprovisionar o reconfigurar los dispositivos móviles de los usuarios. Si se desea restringir el procesamiento de este tipo de mensajes se recomienda hacer uso de las siguientes políticas de seguridad (ver “Apéndice A: Tabla de Políticas de seguridad de Windows Mobile”):

- 4108: Mensajes Service Loading (SL)
- 4109: Mensajes Service Indication (SI)
- 4110: Mensajes WAP no firmados
- 4111: Mensajes de aprovisionamiento OTA
- 4113: Enrutamiento de notificaciones WSP

626. Además de las recomendaciones centradas en deshabilitar las conexiones de datos a través del “Comm Manager” (menú “Inicio – Configuración – Controles inalámbricos”) o del registro, descritas previamente, mediante la configuración de una conexión de datos vacía es posible limitar este tipo de conectividad mientras se dispone de capacidades de telefonía de voz y SMS, y Wi-Fi. Esta opción es válida, por ejemplo, para equipos sin el “Comm Manager” de HTC o para evitar tener que editar el registro manualmente.

627. A través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Conexiones – Conexiones”, desde la pestaña “Avanzado” y a través del botón “Selec. redes”, se accede a la pantalla de “Administración de redes”, dónde es posible configurar una conexión GPRS vacía:

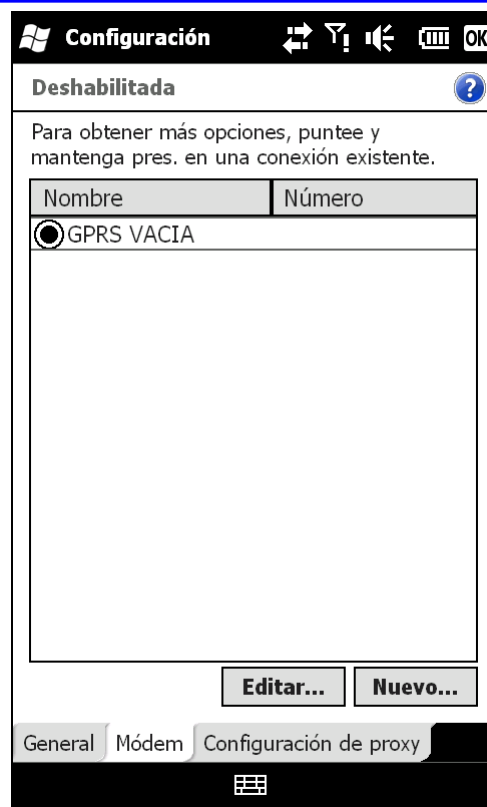
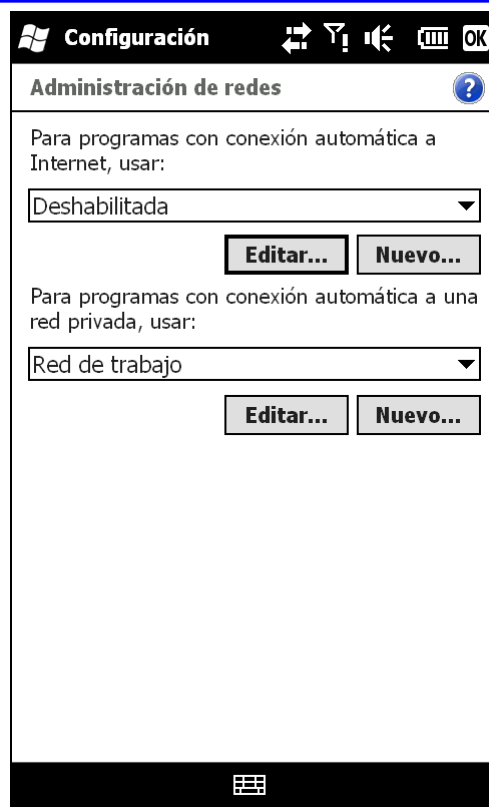


628. Mediante el botón “Nuevo” de la sección de programas con conexión automática a Internet, es posible crear una nueva red, denominada “Deshabilitada” (pestaña “General”), y asociada a una nueva conexión creada a través de la pestaña “Módem” (botón “Nuevo”), denominada “GPRS VACIA”, y cuyo módem es la “Línea de teléfono móvil (GPRS)”, con los siguientes parámetros (imagen inferior derecha):

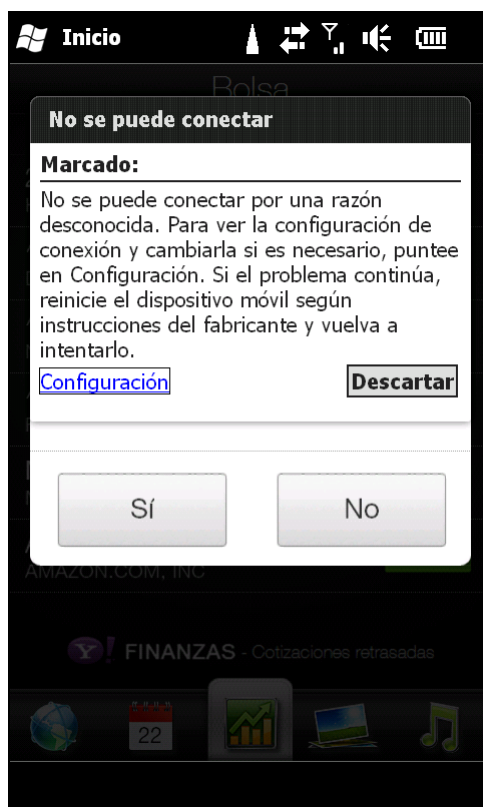
- Nombre de punto de acceso: <vacío>
- Usuario, contraseña y dominio: <todos los campos vacíos>
- Mediante el botón “Avanzado...”, establecer la dirección IP estáticamente con un valor de “0.0.0.0” (pestaña “TCP/IP – “Usar dirección IP específica”), y las direcciones IP de los servidores DNS y WINS (pestaña “Servidores - Dirección se servidor específica”) de forma estática, con un valor de “0.0.0.0” (valor por defecto al fijarlo estáticamente).

629. Adicionalmente, a través de la pestaña “Configuración de proxy” de la nueva red se debe marcar la opción “Esta red conecta a Internet”.

630. Se debe establecer esta nueva red, “Deshabilitada”, como la red seleccionada por defecto en la sección de programas con conexión automática a Internet de la pantalla “Administración de redes” (imagen inferior izquierda):



631. Cualquier intento de conexión de datos a través de la red de telefonía generará el siguiente mensaje de error:

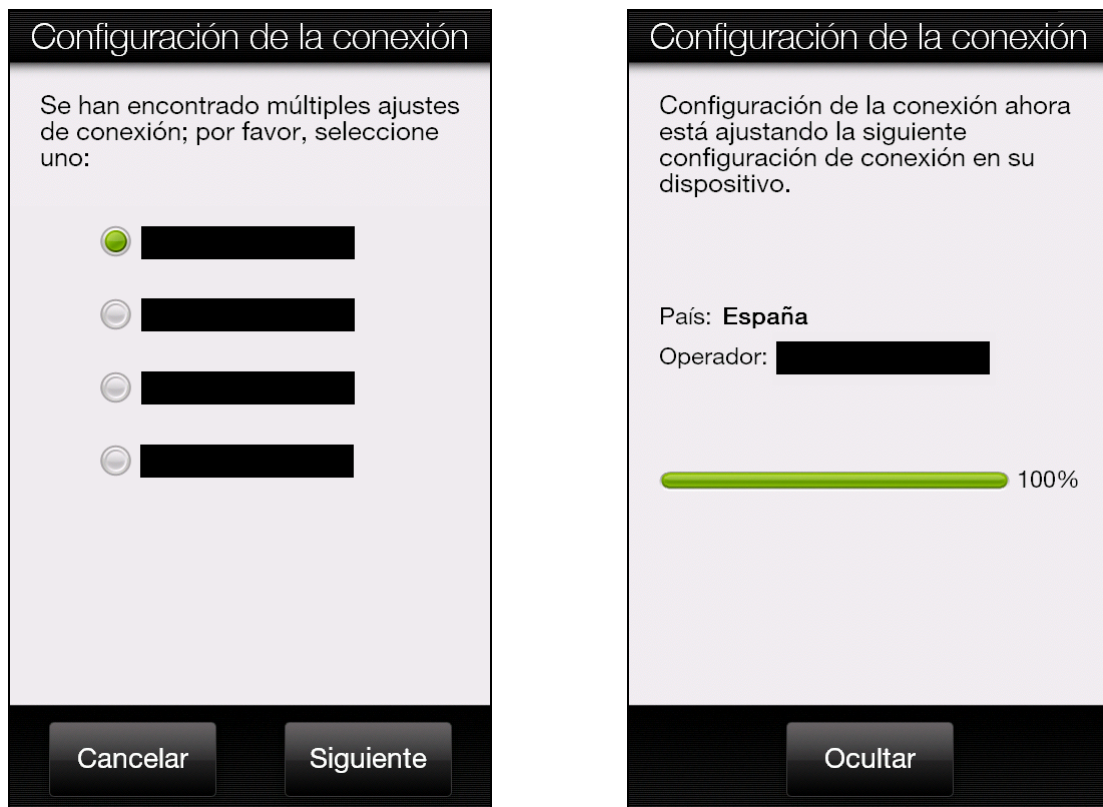


632. El apartado “5.21.2. Perfil de conexión: Internet o Trabajo” proporciona más información sobre las conexiones a Internet y redes privadas.

5.20.2 CONFIGURACIÓN DE LA RED DE DATOS DE TELEFONÍA MÓVIL

633. En dispositivos móviles HTC, al introducir la tarjeta SIM en el dispositivo móvil se lleva a cabo automáticamente el proceso de configuración de las opciones de conectividad de datos asociadas a las redes de telefonía móvil, incluyendo normalmente tres tipos de conexiones de datos: GPRS, mensajes multimedia (MMS) y WAP.

634. En función de la tarjeta SIM empleada y de la base de datos de operadores de telefonía móvil existente en el dispositivo móvil, se mostrarán los ajustes de conexión disponibles (imagen inferior izquierda). El usuario puede seleccionar el operador de telefonía móvil deseado (cuatro opciones en el ejemplo inferior), tras lo que Windows Mobile 6.5 ajustará la configuración de las redes de datos para dicho operador (imagen inferior derecha), sustituyendo la configuración de conexión existente previamente, en concreto, para el perfil “Internet”.



635. La base de datos de operadores está almacenada en el directorio “\windows\” (ficheros “PB81*.db”), tal como especifica la siguiente clave del registro:

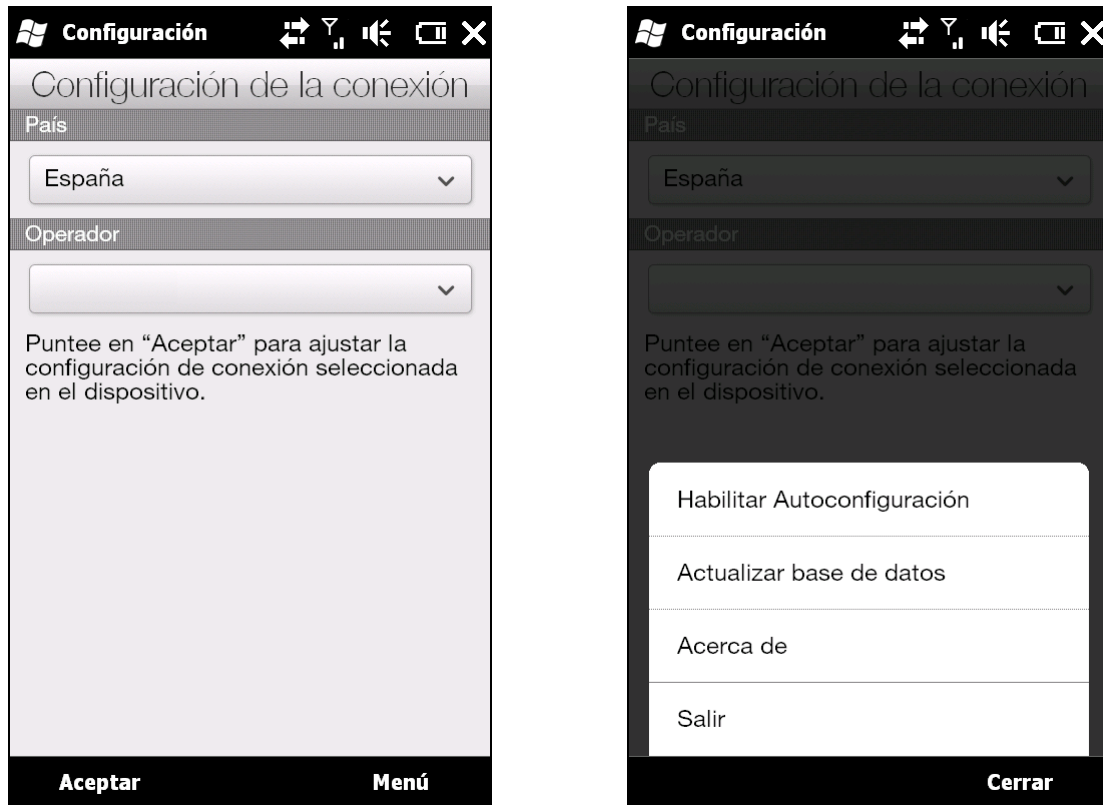
```
[HKEY_CURRENT_USER\Software\HTC\ConnectionSetup]
"provision"="\windows\"
```

636. En este escenario de autoconfiguración por defecto (posteriormente se describe como deshabilitarlo), desde el punto de vista de seguridad, cada vez que se cambia la tarjeta SIM se recomienda acceder a la configuración de datos de telefonía móvil y adecuar la configuración, por ejemplo, para aplicar de nuevo la conexión que deshabilita las comunicaciones de datos (creada en el apartado “5.20. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”).

637. Igualmente, la selección de otro operador (del mismo u otro país) en la pantalla de configuración (analizada posteriormente) modificará la configuración de la conexión de

datos de telefonía móvil, por lo que se recomienda de nuevo adecuar la configuración de datos manualmente tras llevar a cabo esta operación.

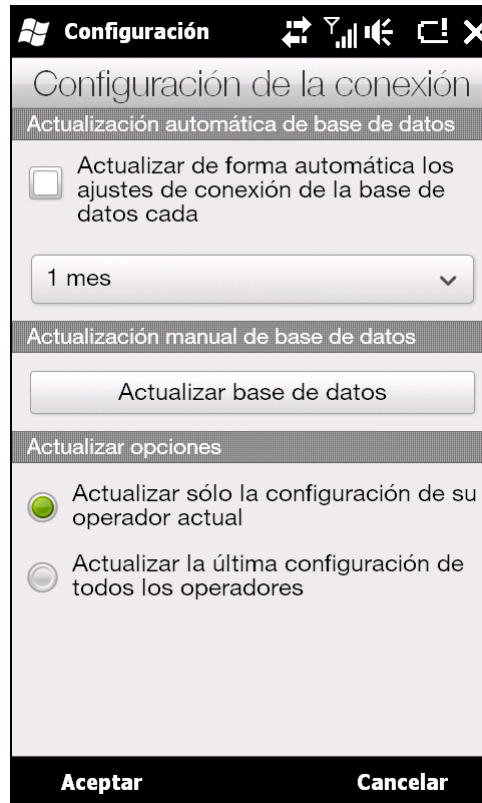
638. El comportamiento de conexión automática se gestiona a través del “Comm Manager” (menú “Inicio – Configuración – Controles inalámbricos”), seleccionando la sección “Conexión de datos”. La configuración actual, incluyendo el país y el operador, se muestra en la pantalla principal:



639. Se recomienda deshabilitar la autoconfiguración de las conexiones de datos (habilitada por defecto para facilitar la utilización del terminal) mediante el botón “Menú”, desmarcando la opción “Habilitar Autoconfiguración”. Esta opción es gestionada por el siguiente parámetro del registro:

```
[HKEY_CURRENT_USER\Software\HTC\ConnectionSetup]
"EnableStartUp"=dword:00000000
```

640. Al deshabilitar la autoconfiguración es necesario crear manualmente la conexión de datos de telefonía móvil 2G/3G a través del Connection Manager (ver apartado “5.21.2. Perfil de conexión: Internet o Trabajo”).
641. La opción “Actualizar base de datos” permite configurar las actualizaciones automáticas de la base de datos con la configuración de la conexión de datos de los operadores de telefonía, definir el periodo entre actualizaciones (1, 3 ó 6 meses), y qué operadores serán actualizados (sólo el actual o todos):



642. Las diferentes opciones de configuración mencionadas son almacenadas en las siguientes claves del registro respectivamente, dónde “Enable” (habilitado si el valor es “1”; deshabilitado si el valor es “0”) especifica si se realizará la descarga automáticamente, “NextCheckTime” (junto a “MaxExpiredSec” y “RandomDays”) define cuando se realizará la siguiente actualización (fecha y hora), y “DiffMode” determina si se actualiza sólo el operador actual (valor “0”) o todos (valor “1”):

```
[HKEY_LOCAL_MACHINE\Software\HTC\ConnSetupDload]
"Enable"=dword:00000000
"NextCheckTime"=hex:\
    00,15,83,8B,43,7B,CB,01
"DiffMode"=dword:00000000
```

643. Se recomienda utilizar la configuración por defecto, dónde las actualizaciones automáticas y periódicas de la base de datos no están habilitadas y, en caso de producirse una actualización, por ejemplo manualmente a través del botón “Actualizar base de datos”, sólo se actualizará el operador actual.
644. La opción “Acerca de” proporciona información sobre la versión de la base de datos de operadores de telefonía disponible actualmente en el dispositivo móvil.
645. El proceso de actualización y descarga de la base de datos de operadores emplea conexiones HTTP (no cifradas, TCP/80) desde el dispositivo móvil hacia “dbcsN.htc.com” (donde “N” tiene un valor entre 1 y 3, y se solicitan todos los ficheros de la base de datos, por ejemplo, “/dbcs/PB81/PB81.ini”), por lo que se recomienda emplear una red segura para realizar el proceso de actualización. En cualquier caso, en algún momento la transferencia de la actualización viajará por parte de la infraestructura de Internet sin cifrar, viéndose expuesta a su posible manipulación por un potencial atacante.

Nota: se han identificado escenarios donde el proceso de actualización de la base de datos de operadores ha inhabilitado de forma permanente el acceso a la pantalla de configuración de la conexión de datos, afectando a la disponibilidad de la información de los operadores. Antes de llevar a cabo la actualización se recomienda realizar una copia de seguridad del dispositivo móvil, ya que sólo es posible solucionar esta situación con un restablecimiento de fábrica.

Nota: los perfiles de conexión pueden variar entre distintos dispositivos móviles basados en Windows Mobile 6.5 y especialmente, en el caso de un mismo dispositivo móvil, entre diferentes operadores de telefonía móvil, por lo que se recomienda realizar un análisis detallado de las opciones de conexión disponibles para un dispositivo móvil y operador de telefonía concreto en función de la configuración de su tarjeta SIM.

5.20.3 SELECCIÓN DE LA RED DE DATOS 3G

646. Las redes de telefonía 2G (o GSM) presentan diferentes vulnerabilidades en la actualidad, como por ejemplo la posibilidad de suplantación de la red por parte de un potencial atacante debido a debilidades en los mecanismos de autenticación, o la posibilidad de capturar y descifrar el tráfico de voz GSM debido a debilidades en los algoritmos de cifrado, A5/1 [Ref.- 1].
647. Con el objetivo de mitigar las vulnerabilidades existentes actualmente en las redes de telefonía móvil 2G (o GSM), se recomienda forzar al dispositivo móvil a conectarse únicamente, tanto para comunicaciones de voz como de datos, a la red de telefonía 3G (o UMTS).
648. Windows Mobile 6.5 permite restringir las comunicaciones de telefonía móvil a través del menú “Inicio – Configuración – Controles inalámbricos – Teléfono”, y en concreto de la opción “Banda” (Elegir banda base).
649. Se recomienda fijar tanto para el tipo de red, como para la frecuencia de banda, los valores “WCDMA” y “UMTS(2100+900)”, respectivamente:



650. El principal inconveniente de esta configuración es que si el usuario se encuentra en una zona dónde no se dispone de cobertura 3G (o superior, 3.5G), no se podrá hacer uso del dispositivo móvil, ya que premia la seguridad por encima de la disponibilidad del servicio de telefonía (voz y datos).

651. Las siguientes claves del registro especifican los valores de banda base, dónde el parámetro "OpMode" toma el valor "1" para red GSM, "2" para red WCDMA (opción recomendada), y "3" para la selección automática de red, y el parámetro "Band" toma el valor "0" para una selección automática de la frecuencia de banda, "1" para GSM+UMTS, "2" para GSM, y el valor "3" para UMTS (opción recomendada):

```
[HKEY_LOCAL_MACHINE\Software\OEM\UMTS]
"OpMode"=dword:00000002
```

```
[HKEY_LOCAL_MACHINE\Software\OEM\UMTS\BandSelection]
"Band"=dword:00000003
```

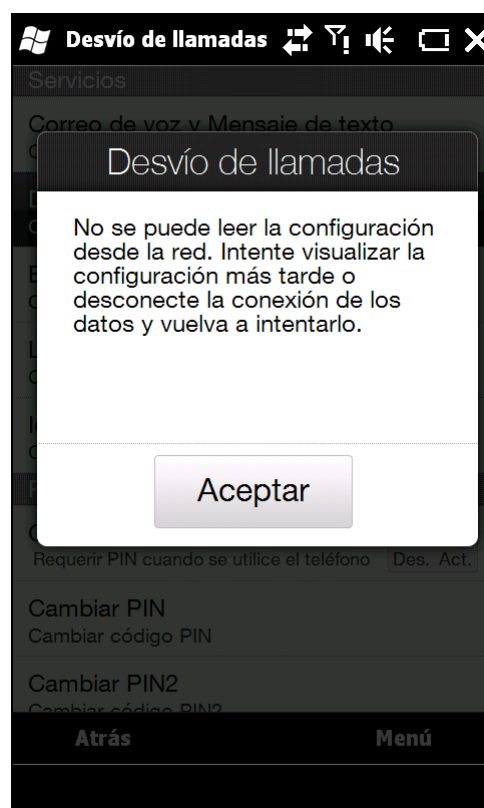
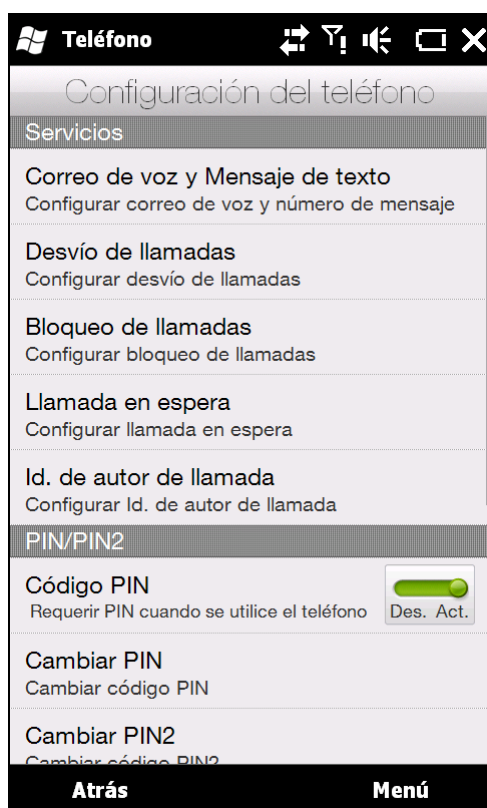
652. Windows Mobile 6.5 proporciona información en la barra de estado superior sobre las tecnologías de telefonía móvil de datos para las que se dispone de cobertura a través del siguiente conjunto de iconos, que representan la disponibilidad y el estado de la conexión para una red 3.5G (HSPA), 3G (WCDMA/UMTS), 2.75G (EDGE) y 2.5G (GPRS), respectivamente:

| | |
|---|-----------------------|
|  | HSPA disponible |
|  | HSPA conectado |
|  | WCDMA/UMTS disponible |
|  | WCDMA/UMTS conectado |
|  | EDGE disponible |
|  | EDGE conectado |
|  | GPRS disponible |
|  | GPRS conectado |

653. La ausencia de cobertura y conectividad está identificada por los siguientes iconos, que indican que se está buscando el servicio de telefonía y que no se dispone de él, respectivamente:



654. Adicionalmente al no disponer de servicio de telefonía se pueden obtener mensajes de error, por ejemplo al intentar configurar otros servicios del teléfono, como el desvío de llamadas:



655. La configuración por defecto del dispositivo móvil premia la conectividad, permitiendo el uso de redes de telefonía móvil 2G o 3G de forma automática en función de su cobertura y disponibilidad:

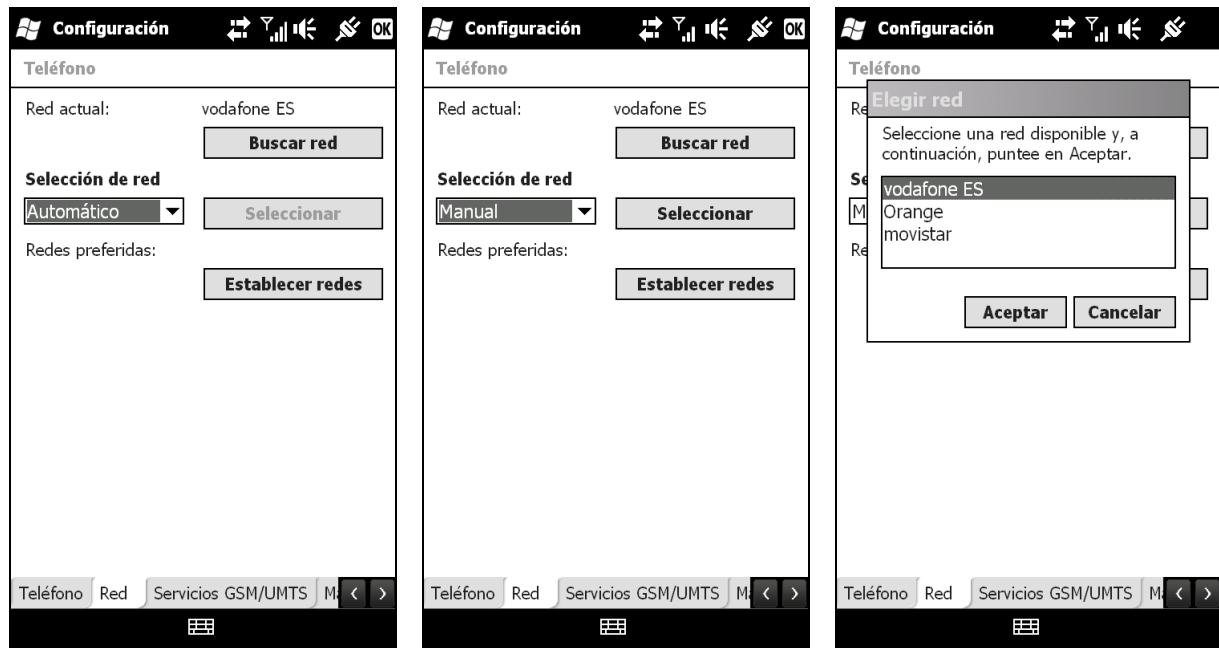


656. El estado activo del módulo de teléfono y la disponibilidad de conectividad de telefonía en base al nivel de intensidad de señal, vienen identificados por los siguientes iconos, respectivamente:



5.20.4 RECOMENDACIONES DE SEGURIDAD PARA LA CONEXIÓN A REDES 2G/3G

657. Desde el menú de configuración del teléfono (“Inicio – Configuración – Controles inalámbricos – Teléfono”) y a través del botón “Menú”, es posible acceder a las opciones “Selección de red” y “Red avanzada” (esta sección de configuración también está disponible a través del menú “Inicio – Configuración”, botón “Menú – Más”, mediante la opción “Conexiones – Red avanzada”).
658. La selección de red permite definir si la red de telefonía será seleccionada de forma automática (opción por defecto) por el dispositivo móvil en función de la intensidad de la señal, o sí el usuario puede definir de forma manual la red a la que desea conectarse de la lista de redes disponibles:



659. Las opciones de “Red avanzada” permiten, mediante la pestaña “HSDPA/HSUPA” (imagen inferior izquierda), habilitar o deshabilitar los protocolos HSPA (es decir, 3.5G), y en concreto HSDPA/HSUPA (*High-Speed Downlink/Uplink Packet Access*; opción por defecto) o sólo HSDPA. Esta opción de configuración permite por tanto al usuario seleccionar entre redes 3.5G (icono con la “H” (HSPA)) o redes 3G (icono “3G”).

660. Se recomienda habilitar ambos protocolos de 3.5G, HSDPA/HSUPA, si se desea disponer de conexiones de datos de alta velocidad (siempre que el operador de telefonía móvil ofrezca soporte para ellos), ya que no hay vulnerabilidades de seguridad conocidas asociadas a esta tecnología frente a las tecnologías 3G. Los cambios en la configuración de HSPA requieren reiniciar el dispositivo móvil.

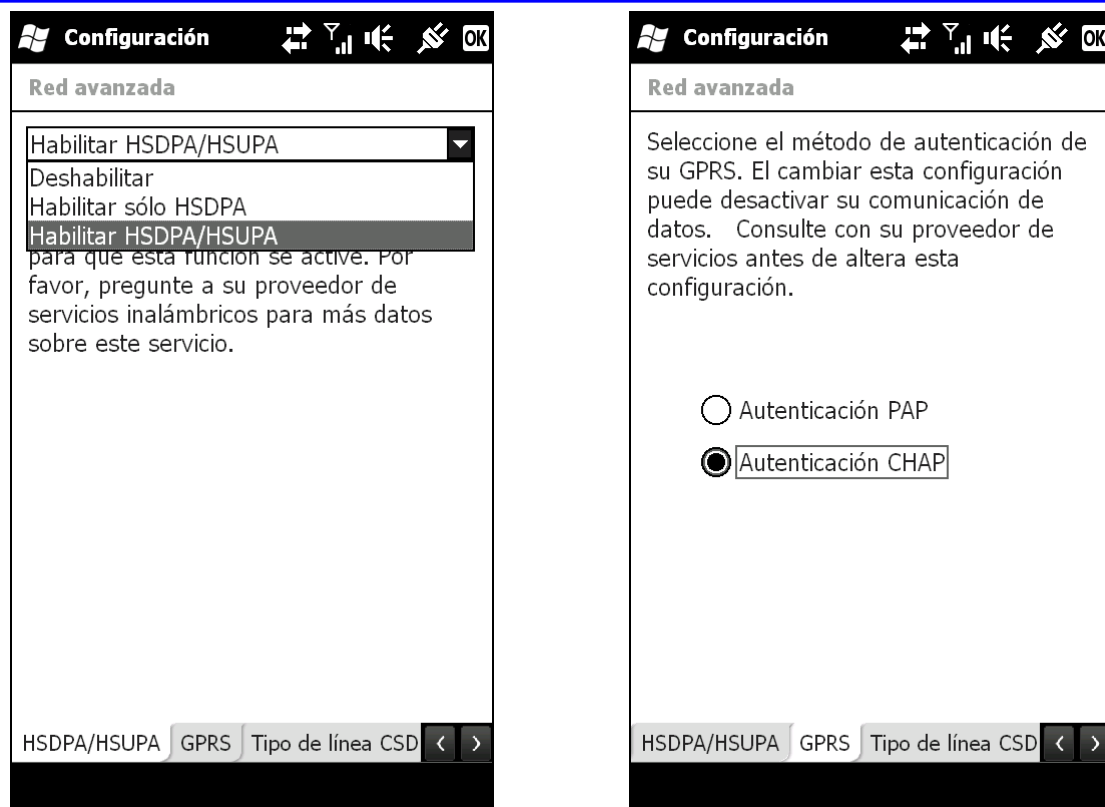
661. La siguiente clave del registro especifica los valores de “HSDPA/HSUPA”, dónde el parámetro “DisH” toma el valor “0” si se deshabilita, “1” para sólo HSDPA, y “2” (por defecto) para “HSDPA/HSUPA” (opción recomendada):

```
[HKEY_LOCAL_MACHINE\Software\OEM\RIL]
"DisH"=dword:00000002
```

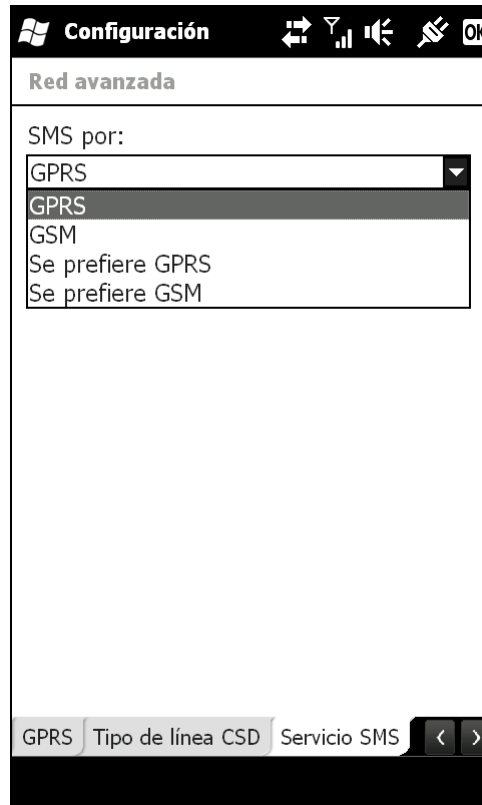
662. En el caso de conexiones de datos 2.5G, GPRS, es posible seleccionar el método de autenticación mediante la pestaña “GPRS” (imagen inferior derecha). Se recomienda usar CHAP frente a PAP (opción por defecto), si es un método soportado por el operador de telefonía móvil, ya que incluye mejoras de seguridad.

663. La siguiente clave del registro especifica los valores de autenticación de GPRS, dónde el parámetro toma el valor “1” para PAP (por defecto), y “2” para CHAP (opción recomendada):

```
[HKEY_CURRENT_USER\ControlPanel\PhoneExtendFunction]
"GPRSAuthenticationMethod"=dword:00000002
```



664. La pestaña “Servicio SMS” de “Red avanzada” permite seleccionar el método de transporte empleado para el envío de mensajes de texto (SMS), pudiendo optar por cuatro opciones: GSM (2G), GPRS (2.5G) o ambos, dando prioridad a GSM o a GPRS. Se recomienda, si el operador de telefonía móvil soporta ambos, la opción de GPRS, ya que al menos GPRS no presenta las vulnerabilidades en los algoritmos de cifrado de GSM [Ref.- 1]:



665. La siguiente clave del registro especifica los valores de red para el envío de SMS, dónde el parámetro toma el valor “0” para GPRS (opción recomendada), “1” para GSM, “2” (por defecto) si se prefiere GPRS y “3” si se prefiere GSM:

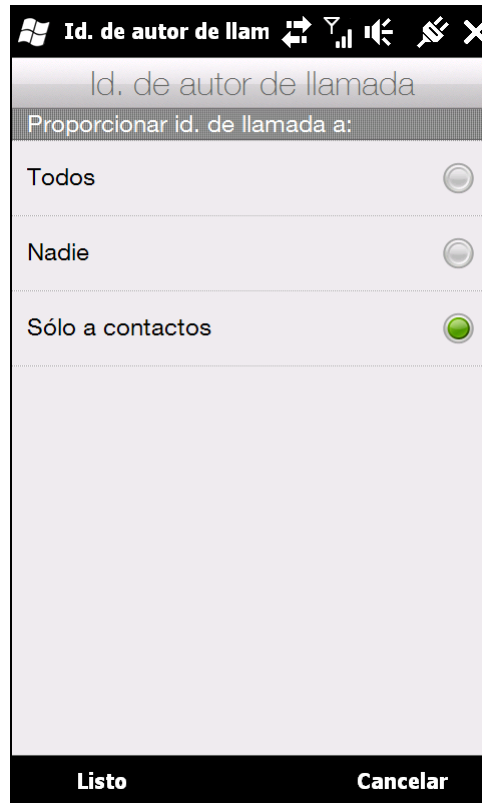
```
[HKEY_LOCAL_MACHINE\Software\Microsoft\RIL]
"SMSService"=dword:00000000
```

Nota: las pruebas realizadas con alguno de los operadores de telefonía móvil en España confirman que es posible emplear tanto autenticación PAP como CHAP (recomendada) para GPRS, y que no es posible el envío de mensajes SMS a través de GPRS (recomendada), debiendo usarse en su lugar la opción GSM (opción recomendada: “Se prefiere GPRS”).

Las pruebas realizadas parecen indicar que la opción GSM se refiere al uso de “conmutación de circuitos (voz)” para el envío de mensajes de texto, mientras que la opción GPRS se refiere al uso de “conmutación de paquetes (datos)”. Se verificó que es posible el envío de SMS, con la opción GSM, incluso cuando se ha forzado el uso de una banda base específica, y más concretamente, la opción recomendada de 3G/UMTS, tipo de red “WCDMA” y frecuencia de banda “UMTS(2100+900)”. Por tanto la opción GSM para el envío de mensajes SMS implica “GSM/UMTS” (2G o 3G) y no únicamente 2G.

666. Con el objetivo de proteger la privacidad del usuario, el módulo de telefonía de Windows Mobile 6.5 permite al usuario definir en qué tipo de llamadas se enviará la información de identificación como autor de la llamada: todas las llamadas (opción por defecto), ninguna (opción recomendada en un entorno de alta seguridad) o sólo al llamar a teléfonos de la lista de contactos (opción recomendada en un entorno de seguridad intermedio).

667. El menú “Inicio – Configuración – Controles inalámbricos – Teléfono – Id. de autor de llamada” permite establecer la configuración más adecuada:



668. La siguiente clave del registro especifica el valor de envío del identificador del autor de la llamada, donde el parámetro “SendCallID” toma el valor “0” para enviarlo a todos (por defecto) o a nadie, y “1” para enviarlo sólo a contactos (opción recomendada). Para diferenciar entre todos y nadie se usa el segundo parámetro, “CallerID”, con valor “1” indicando todos o valor “2” indicando nadie, o sólo contactos (opción recomendada):

```
[HKEY_CURRENT_USER\ControlPanel\Phone]
"SendCallID"=dword:00000001

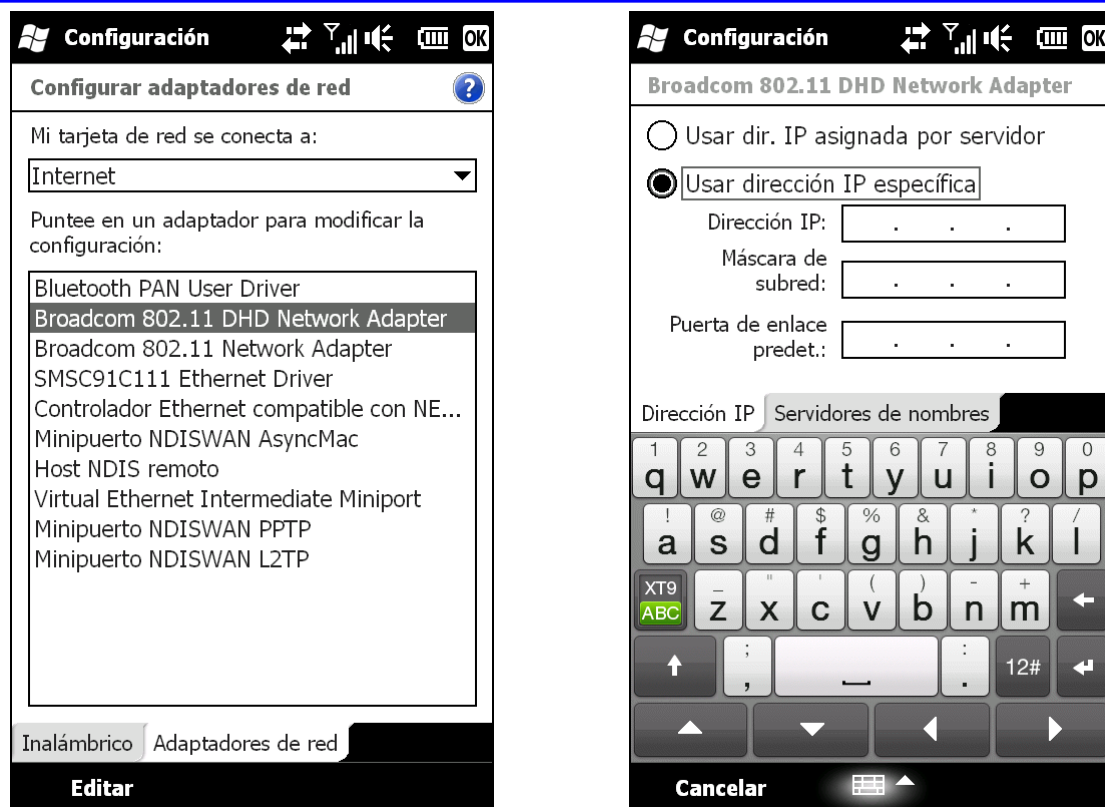
[HKEY_CURRENT_USER\ControlPanel\PhoneExtendFunction]
"CallerID"=dword:00000002
```

5.21 COMUNICACIONES TCP/IP

669. Esta sección proporciona recomendaciones de seguridad para la pila de comunicaciones TCP/IP del dispositivo móvil, incluyendo recomendaciones generales para TCP/IP (IPv4), SSL/TLS, IPv6 y VPN's.

5.21.1 ADAPTADORES DE RED

670. Los adaptadores de red disponibles en el dispositivo móvil para las diferentes tecnologías de comunicaciones están disponibles en el menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Conexiones – Wi-Fi”. Tras seleccionar el botón “Redes inalámbricas”, la pestaña “Adaptadores de red” muestra todos los adaptadores, incluyendo el interfaz Wi-Fi ó 802.11 (imagen inferior izquierda):



671. Seleccionando cualquiera de los adaptadores de red disponibles es posible configurar los parámetros de la pila TCP/IP para ese adaptador (imagen superior derecha), incluyendo si la dirección es obtenida dinámicamente por DHCP o es configurada estáticamente (junto a la máscara de red y el *router* o puerta de enlace por defecto) desde la pestaña “Dirección IP”, así como los servidores DNS y WINS desde la pestaña “Servidores de nombres” (ver apartado “5.21. Comunicaciones TCP/IP”).
672. La información de configuración de los adaptadores de red se almacena en el registro, y concretamente bajo la clave “HKEY_LOCAL_MACHINE\Comm”, y en concreto en el dispositivo móvil empleado, en las entradas “BCMSD1” y “BCMSD1DHD1” para los adaptadores “Broadcom 802.11 Network Adapter” y “Broadcom 802.11 DHD Network Adapter” (utilizado en la conexión a redes Wi-Fi), respectivamente.
673. Los parámetros de configuración del interfaz Wi-Fi se almacenan en la clave del registro “HKEY_LOCAL_MACHINE\Comm\BCMSDDHD1\Parms”, donde “BCMSDDHD1” es el nombre del interfaz Wi-Fi empleado.
674. El “Comm Manager” (menú “Inicio – Configuración – Controles inalámbricos”) de HTC también emplea el registro para identificar el adaptador de red Wi-Fi a emplear:

```
[HKEY_LOCAL_MACHINE\Software\HTC\CommManager\WLAN]
"DeviceName"="{ 98C5250D-C29A-4985-AE5F-AFE5367E5006 } \BCMSDDHD1"
```

5.21.2 PERFIL DE CONEXIÓN: INTERNET O TRABAJO

675. Uno de los aspectos fundamentales para realizar una configuración de seguridad adecuada sobre las redes de datos a las que puede conectarse el dispositivo móvil es comprender el modelo de conectividad de Windows Mobile a través del Connection Manager para las conexiones de datos de telefonía móvil (módulo analizado en el apartado “5.18.2. Selección de la red de datos en Windows Mobile”), asociado a los

perfiles de conexión “Internet” o “Trabajo”. El modelo también afecta al interfaz Wi-Fi con ciertas particularidades (ver apartado “5.21.2.1. Wi-Fi: perfil de conexión Internet o Trabajo”).

676. Windows Mobile diferencia entre las conexiones de datos que permiten disponer de conectividad a Internet, y las que permiten disponer de conectividad únicamente a una red privada o red de trabajo [Ref.- 73].
677. La configuración de los perfiles de conexión está disponible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Conexiones – Conexiones”. La pestaña “Avanzado” (imagen inferior izquierda) permite la selección de redes para cada perfil a través del botón “Selec. Redes” (imagen inferior derecha):



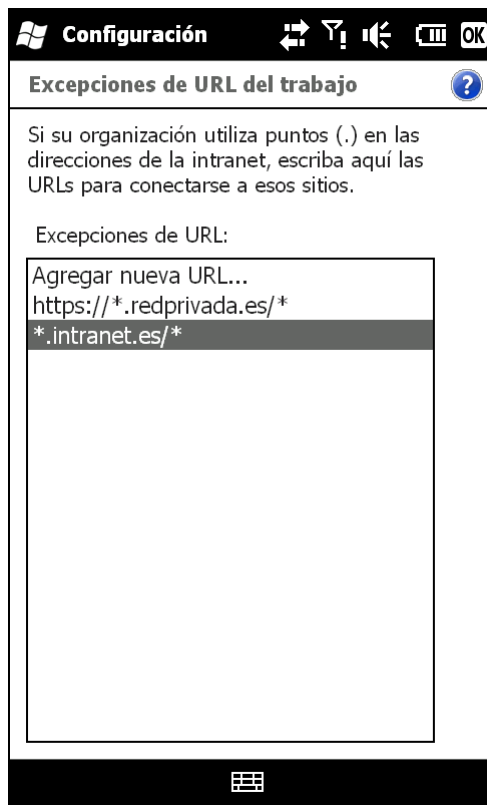
678. Por defecto la conexión para el perfil de “Internet” es “Mi ISP” y la conexión para el perfil de “Trabajo” es “Red de trabajo”, ambas conexiones con ninguna configuración asociada (módem, proxy, VPN, etc).

Nota: los identificadores (GUID, Globally Unique Identifier) de la red destino ("DestId") para los perfiles de "Internet" y de "Trabajo" son:

- Internet: "{436EF144-B4FB-4863-A041-8F905A62C572}"
- Trabajo: "{A1182988-0D73-439e-87AD-2A5B369F808B}"

679. La pantalla de “Administración de redes” permite definir la red por defecto a emplear para los programas que desean conectar a Internet y para los programas que desean conectar a una red privada, “Trabajo”.
680. Las conexiones de “Internet” conectan el dispositivo móvil directamente a Internet, con una dirección IP pública, como por ejemplo las redes de datos de telefonía móvil (2G/3G).

681. Las conexiones de “Trabajo” conectan el dispositivo móvil a una red privada o Intranet, ya que Windows Mobile fue diseñado como dispositivo móvil de uso empresarial, entornos en los que se dispone de servidores y recursos de red internos.
682. El modelo utilizado por Windows Mobile para determinar si un intento de conexión requiere de una conexión de “Internet” o de “Trabajo” se basa en la dirección destino empleada, por ejemplo, en la URL de Internet Explorer Mobile [Ref.- 74]:
- Si la dirección tiene puntos en el nombre, por ejemplo “http://www.taddong.com”, se utilizará la conexión definida en el perfil de “Internet” (salvo que se disponga de una conexión de “Internet” activa).
 - Si la dirección no tiene puntos en el nombre, es decir, se está referenciando un servidor interno sin especificar el dominio, por ejemplo “http://servidorweb”, se utilizará la conexión definida en el perfil de “Trabajo” (salvo que se disponga de una conexión de “Trabajo” activa).
 - Si se emplean direcciones IP en lugar de nombres, el dispositivo móvil se intentará conectar directamente al equipo destino independientemente de la conexión.
683. Si se desea acceder a recursos de una red privada o Intranet a través de una dirección que tiene puntos, por ejemplo “http://servidorweb.intranet.es”, Windows Mobile proporciona una tabla de excepciones para definir que dominios (o direcciones con puntos) son empleados en la red privada, por ejemplo “*.intranet.es”:



684. El formato de las excepciones emplea URL's, por lo que debe incluir el protocolo (http, https, etc), el equipo o hostname (incluyendo el dominio) y el recurso accedido (URI). Es posible emplear el carácter “*” como comodín, indicando la presencia de cualquier elemento en ese campo. Por ejemplo:

- “*/*.*.midominio.es/*”: crea una excepción para redirigir a la Intranet cualquier tráfico hacia cualquier equipo y recurso en el dominio “midominio.es” (equivalente a “*.midominio.es”).
- “https://www.midominio.es/*”: crea una excepción para redirigir a la Intranet el tráfico HTTPS hacia cualquier recurso del equipo “www. midominio.es”.
- “*/*.*/*”: crea una excepción para redirigir a la Intranet cualquier tráfico.

Nota: es posible que en algunos terminales no funcione correctamente “*/*.*/*” como excepción para redirigir a la intranet cualquier parte del tráfico. Se ha comprobado que en terminales como Samsung Omnia II esta excepción debe crearse como “*./*/*”.

685. Las excepciones son aplicadas de la más a la menos restrictiva.

Nota: es posible añadir excepciones de direcciones Intranet al dispositivo móvil a través del aprovisionamiento mediante ficheros XML (ver apartado “5.8. Modificación local de políticas de seguridad”), que no serán visibles a través del interfaz de usuario, y por tanto, no pueden ser modificadas por el usuario.

686. Si se desea conectar a una red privada desde una conexión de “Internet” es necesario hacer uso de las capacidades de redes privadas virtuales o VPN (*Virtual Private Network*) del dispositivo móvil (ver apartado “5.21.7. VPN”).

Nota: pese a que el perfil de “Trabajo” permite definir conexiones vía módem, ésta es una tecnología cada vez más en desuso actualmente, empleándose en su lugar VPN’s.

687. Si se desea conectar a Internet desde una conexión de “Trabajo” es necesario hacer uso de un proxy, encargado de gestionar las comunicaciones hacia Internet desde la red privada.

688. El servidor proxy puede ser definido en el dispositivo móvil desde la pestaña “Configuración de proxy” del asistente de configuración de la red:



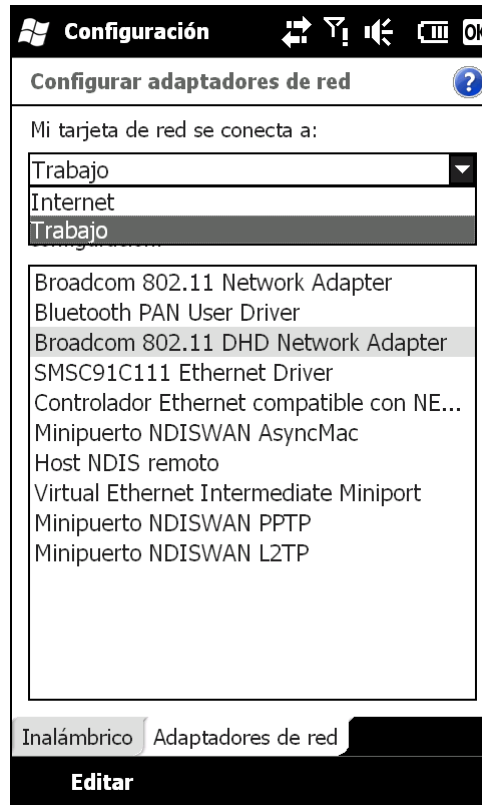
689. Mediante el botón “Avanzado...” (imagen superior derecha) es posible establecer la configuración para los diferentes tipos de proxies soportados por Windows Mobile (HTTP, WAP - TCP/9201, Conexión WAP segura - TCP/9203, Socks versión 4 ó 5 – TCP/1080), así como especificar las credenciales (en caso de ser necesarias) para hacer uso de los servicios del servidor proxy: usuario, contraseña y dominio.

Nota: debe tenerse en cuenta que existe la posibilidad de que ciertas aplicaciones cliente (no programadas adecuadamente según los estándares de Windows Mobile) realicen accesos directos a los interfaces de comunicaciones del dispositivo móvil, por ejemplo, a la red de datos de telefonía móvil (2G/3G), o no hagan uso de la configuración de proxy [Ref.- 74].

5.21.2.1 Wi-Fi: perfil de conexión Internet o Trabajo

690. Las redes Wi-Fi pueden ser redes privadas (red empresarial, red doméstica, etc) y redes públicas (*hotspots* Wi-Fi), y ambas suelen ser empleadas para la conexión a Internet, por lo que en la configuración por defecto se asigna el perfil de “Internet” a las redes Wi-Fi.

691. La pantalla de configuración de los adaptadores de red (ver apartado “5.21.1. Adaptadores de red”) permite definir el perfil de conexión (“Internet” o “Trabajo”) para todas las tarjetas de red, incluido el interfaz Wi-Fi (ó Bluetooth - PAN):



692. La conectividad a través del adaptador de red es clasificada por defecto bajo el perfil de “Trabajo” desde la pantalla de “Adaptadores de red”, sin embargo es clasificada como “Internet” por defecto al agregar una nueva red Wi-Fi. Tiene prevalencia el perfil asociado a la red Wi-Fi específica a la que está conectado el dispositivo móvil frente al perfil genérico del adaptador de red.

Nota: el valor seleccionado para el perfil en la red Wi-Fi está definido por el parámetro “DestId” del interfaz Wi-Fi en el registro, y apunta al GUID del perfil de “Internet” por defecto:

```
HKLM\Comm\ConnMgr\Providers\{f792e23c-dc19-4668-9be4-f8688b4c18d6}\BCMSDDHD1
```

El perfil genérico asociado al adaptador de red modifica el GUID destino (parámetro “DestId”) en la siguiente clave del registro:

```
HKEY_LOCAL_MACHINE\ControlPanel\WiFi\Ethernet
```

Los cambios en el primer parámetro requieren reiniciar el interfaz Wi-Fi. La existencia de ambas claves del registro está condicionada a que el interfaz Wi-Fi del dispositivo móvil esté habilitado.

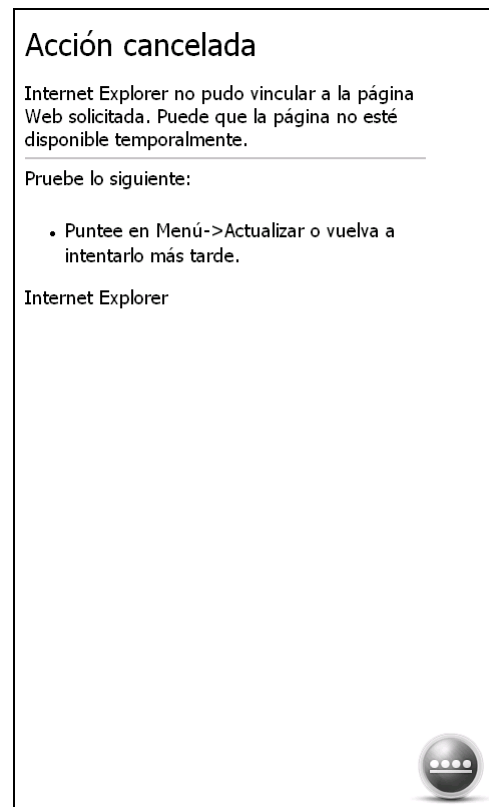
Nota: en este escenario, los accesos a recursos de la red privada, como por ejemplo “http://servidor/”, generan una petición directa HTTP (TCP/80) no cifrada a “m.live.com” (“/Search/Results.aspx?mid=8002&lc=es&q=http://servidor/”) revelando en la consulta (parámetro “q”) el recurso interno accedido. El servidor web responde con una redirección (302) al buscador Bing (“m.bing.com”) y la misma consulta.

Este comportamiento por defecto de Internet Explorer Mobile tiene un impacto relevante desde el punto de vista de seguridad, ya que revela todos los detalles de los recursos internos accedidos (aquellos que no tienen ningún punto en su nombre) a través de la red y a los servidores web indicados (propiedad de Microsoft).

Se recomienda deshabilitar este comportamiento de realización de búsquedas a través de Bing existente por defecto eliminando el proveedor de búsquedas automático de Internet Explorer Mobile (ver apartado “5.29.1. Proveedor de búsquedas automático”).

693. Si se desea acceder a recursos de una red privada a través de la conexión Wi-Fi, con el perfil de “Internet” asignado, será necesario definir en la conexión asociada al perfil de “Trabajo” una VPN. Tras definir la VPN, los accesos a recursos internos (aquellos que no tienen ningún punto en su nombre) son cursados a través de la VPN.

694. Sin embargo, si el servidor VPN no está disponible (por ejemplo, la resolución de nombres, DNS, falla), el dispositivo móvil generará un mensaje de error de conexión a la VPN, pero empleará el método de búsqueda a través de Bing descrito previamente, desvelando los detalles de los servidores internos en Internet (imagen inferior izquierda):



695. Si no se dispone de un proveedor de búsquedas automático definido, opción recomendada, si el servidor VPN no está disponible se indicará con el mismo mensaje de error, y el navegador web también generará un mensaje de error (imagen superior derecha) indicando que no ha podido acceder al servidor interno especificado.

5.21.3 SEGURIDAD EN TCP/IP

696. Con el objetivo de incrementar el nivel de seguridad de la pila TCP/IP empleada para las conexiones de datos en Windows Mobile 6.5, es posible modificar ciertos parámetros de configuración que condicionan su comportamiento.

697. Los parámetros de configuración generales de TCP/IP (IPv4) se almacenan en la siguiente clave del registro [Ref.- 63]:

```
HKEY_LOCAL_MACHINE\Comm\Tcpip\Parms
```

Nota: todas los parámetros de configuración especificados a continuación para los que no se especifica una clave del registro pertenecen a esta clave de configuración general de TCP/IP.

698. Los parámetros de configuración TCP/IP de cada adaptador de red, por ejemplo “Broadcom 802.11 DHD Network Adapter”, están disponibles bajo la siguiente clave del registro:

```
HKEY_LOCAL_MACHINE\Comm\BCMSDDHD1\Parms\TcpIp
```

699. Se recomienda deshabilitar el procesamiento de paquetes de ping, es decir, paquetes *ICMP echo request* entrantes y sus respuestas asociadas, paquetes *ICMP echo response* salientes, con el objetivo de limitar el descubrimiento del dispositivo móvil en la red.

Nota: no se ha identificado ningún mecanismo, ni opción de configuración, en Windows Mobile 6.5 que permita deshabilitar el procesamiento de *ping*, la recepción de paquetes *ICMP echo request* y sus respuestas asociadas, *ICMP echo response*.

700. Windows Mobile 6.5 no responde a otros tipos de mensajes ICMP de petición y respuesta, como por ejemplo *ICMP timestamp* o *ICMP address subnet mask*.

701. Se recomienda deshabilitar el procesamiento de mensajes *ICMP redirect*, enviados desde un router para notificar la existencia de otras rutas más óptimas, y que pueden modificar la tabla de rutas del dispositivo móvil (habilitado por defecto):

```
[HKEY_LOCAL_MACHINE\Comm\Tcpip\Parms]  
"EnableICMPRedirects"=dword:00000000
```

702. Mediante la captura de tráfico y, en concreto del protocolo ICMP, es posible identificar la existencia de dispositivos Windows Mobile 6.5, ya que las peticiones *ICMP echo request* generadas desde el dispositivo móvil periódicamente (cada 60 minutos), por ejemplo para verificar la disponibilidad del router por defecto obtenido mediante DHCP [Ref.- 66], contienen un mensaje característico de 5 bytes, “DHCP”.

703. La identificación del dispositivo móvil también se puede llevar a cabo a través del protocolo DHCP, ya que en las peticiones DHCP (*DHCP Request*) se incluye la opción 60, identificación del vendedor, con el mensaje “Microsoft Windows CE”.

704. La opción 60 de DHCP está definida en la siguiente clave del registro:

```
HKEY_LOCAL_MACHINE\Comm\Tcpip\Parms\DhcpSendOptions
```

705. Se recomienda eliminar dicha opción o clave del registro con el objetivo de ocultar el tipo de dispositivo móvil en las peticiones DHCP.

Nota: las claves del registro pueden ser eliminadas mediante un fichero XML de aprovisionamiento de configuración del dispositivo móvil (ver apartado “5.8. Modificación

local de políticas de seguridad”). El siguiente fichero permite eliminar la opción “60” del cliente DHCP de Windows Mobile 6.5 mediante la directiva “noparm”:

```
<wap-provisioningdoc>
  <characteristic type="Registry">
    <characteristic type="HKLM\Comm\Tcpip\Parms\DhcpSendOptions">
      <noparm name="60" />
    </characteristic>
  </characteristic>
</wap-provisioningdoc>
```

Esta acción permite eliminar una clave del registro, en lugar de modificar su valor.

706. Se recomienda que el dispositivo móvil no actúe de *router*, es decir, no pueda enrutar tráfico entre las distintas redes de datos a las que está conectado. El parámetro “IPEnableRouter” (deshabilitado por defecto) permite activar esta funcionalidad:

```
"IPEnableRouter"=dword:00000000
```

707. Se recomienda deshabilitar las capacidades de *multicast* (IGMP, *Internet Group Management Protocol*) en el dispositivo móvil, fijando el valor de la siguiente clave del registro. El valor “0” (recomendado desde el punto de vista de seguridad) deshabilita el soporte multicast, el valor “1” permite enviar pero no recibir paquetes multicast, y el valor “2” permite participar completamente en las comunicaciones multicast:

```
"IGMPLevel"=dword:00000000
```

5.21.4 ESCANEOS DE PUERTOS TCP Y UDP

708. A continuación se analiza el comportamiento de la pila TCP/IP de Windows Mobile 6.5 frente a intentos de conexión TCP y UDP a través del interfaz Wi-Fi. El análisis se ha realizado en la configuración por defecto del dispositivo móvil, es decir, sin haber realizado ninguna configuración específica o instalación adicional de software.

709. Windows Mobile 6.5 responde con un paquete *TCP Reset* a las peticiones de conexión en puertos TCP cerrados.

710. Por defecto, Windows Mobile 6.5 únicamente dispone de dos puertos TCP no cerrados:

- TCP/21 (FTP): El puerto parece estar abierto. Tras establecer la conexión inicial TCP, la sesión es automáticamente cerrada por el dispositivo móvil (*TCP Reset*).
- TCP/514 (r-login): El puerto está filtrado, ya que no se recibe ninguna respuesta a los intentos de conexión.

711. Windows Mobile 6.5 responde con un paquete ICMP de tipo 3 y código 3 (destino inalcanzable, puerto inalcanzable) a las peticiones de conexión en puertos UDP cerrados.

712. Por defecto, Windows Mobile 6.5 únicamente dispone de tres puertos UDP no cerrados:

- UDP/67 (DHCP): El puerto parece estar abierto o filtrado, ya que no se recibe ninguna respuesta a los intentos de conexión.
- UDP/137 (NetBIOS Name Service): El puerto está abierto y se recibe respuesta a los intentos de conexión.

- UDP/138 (NetBIOS Datagram): El puerto parece estar abierto o filtrado, ya que no se recibe ninguna respuesta a los intentos de conexión.

- 713.El comportamiento por defecto de la pila TCP/IP, la ausencia de mecanismos de filtrado de tráfico (cortafuegos personal) y sus peculiaridades a nivel de TCP y UDP, hacen posible la identificación de los dispositivos móviles basados en Windows Mobile 6.5 de forma sencilla.
- 714.Este tipo de identificación remota a través de la red facilita a un potencial atacante la realización de ataques dirigidos sobre vulnerabilidades conocidas, por lo que se enfatiza la necesidad de mantener el software del dispositivo móvil completamente actualizado en todo momento.

Nota: el comportamiento de la pila TCP/IP frente a escaneos de puertos a través del interfaz de telefonía móvil de datos no puede ser analizado de forma fiable. Este comportamiento a través del interfaz de telefonía móvil de datos está condicionado por la infraestructura de comunicaciones y los mecanismos de filtrado de los operadores de telefonía móvil, que por ejemplo, pueden no permitir comunicaciones mediante ping (*ICMP echo request y reply*) o pueden disponer de proxies transparentes en la red, por ejemplo para protocolos como FTP o HTTP.

5.21.5 SSL/TLS

- 715.Windows Mobile 6.5 permite configurar el módulo de seguridad SCHANNEL encargado de la implementación de los protocolos SSL, *Secure Socket Layer*, y TLS, *Transport Layer Security*, siendo posible definir los algoritmos de cifrado disponibles (AES 128 ó 256, DES, Triple DES, RC2, RC4, etc), de hashing (MD5 ó SHA), y de intercambio de claves (PKCS).
- 716.Adicionalmente, es posible habilitar o deshabilitar las diferentes versiones de los protocolos disponibles, como PCT 1.0, SSL 2.0, SSL 3.0 ó TLS 1.0.

- 717.La información de configuración se almacena en la siguiente clave del registro [Ref.- 59]:

```
HKEY_LOCAL_MACHINE\Comm\SecurityProviders\SCHANNEL
```

- 718.Se recomienda deshabilitar el uso de SSL 2.0, principalmente para el role de cliente (y opcionalmente para el role servidor), debido a que esta versión del protocolo es vulnerable frente a ataques MitM, y emplearse en su lugar SSL 3.0 ó TLS 1.0. Para ello es necesario fijar el valor "Enable" a "0" en la siguiente clave del registro:

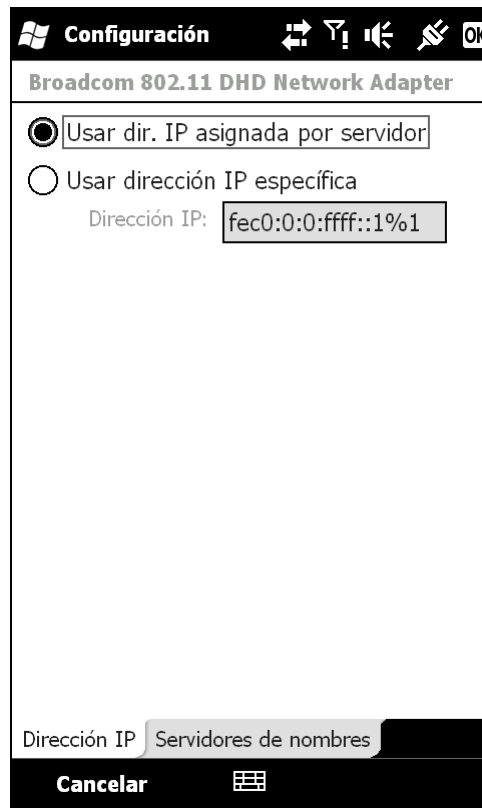
```
[HKLM\Comm\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]  
"Enabled"=dword:00000000
```

- 719.En entornos de un nivel de seguridad más alto sería recomendable deshabilitar de forma más específica los algoritmos criptográficos más débiles para evitar hacer uso de ellos, como por ejemplo DES o Triple DES para el cifrado o MD5 para la integridad o *hashing*.

5.21.6 IPV6

- 720.El protocolo IP versión 6 (IPv6) está soportado por defecto en Windows Mobile 6.5 para las comunicaciones de datos mediante Wi-Fi, y no así para las comunicaciones de datos a través de la infraestructura de telefonía móvil. El usuario no dispone de ninguna opción de configuración disponible relacionada con IPv6 en el interfaz gráfico.

721. Una de las indicaciones de la disponibilidad de IPv6 es el valor de la dirección IP de la pantalla de configuración de los adaptadores de red (ver apartado “5.21.1. Adaptadores de red”), y en concreto del interfaz Wi-Fi, cuando no dispone de conectividad IPv4:



722. La disponibilidad de IPv6, y en concreto del cliente DHCPv6 Lite, está indicada por la existencia de la clave del registro:

```
HKEY_LOCAL_MACHINE\Comm\Devices\TCPIP6\DHCPV6L
```

723. Durante el proceso de inicialización de conectividad de datos, el dispositivo móvil genera consultas DNS en busca de la dirección IP asociada al host “isatap”. ISATAP, *Intra-Site Automatic Tunnel Addressing Protocol*, es un mecanismo de transición a IPv6 que permite transmitir tráfico IPv6 sobre una red IPv4 desde dispositivos con pila de comunicaciones dual, es decir, con soporte para IPv4 e IPv6.

724. La información de configuración de IPv6 se almacena en la siguiente clave del registro [Ref.- 60]:

```
HKEY_LOCAL_MACHINE\Comm\Tcpip6\Parms
```

725. Se recomienda deshabilitar la disponibilidad de IPv6 en Windows Mobile 6.5 por completo, salvo que se vaya hacer uso de sus capacidades de comunicación, para lo que es necesario deshabilitar la pila de comunicaciones IPv6 en el gestor de protocolos (AFD, *Auxiliary Function Driver*).

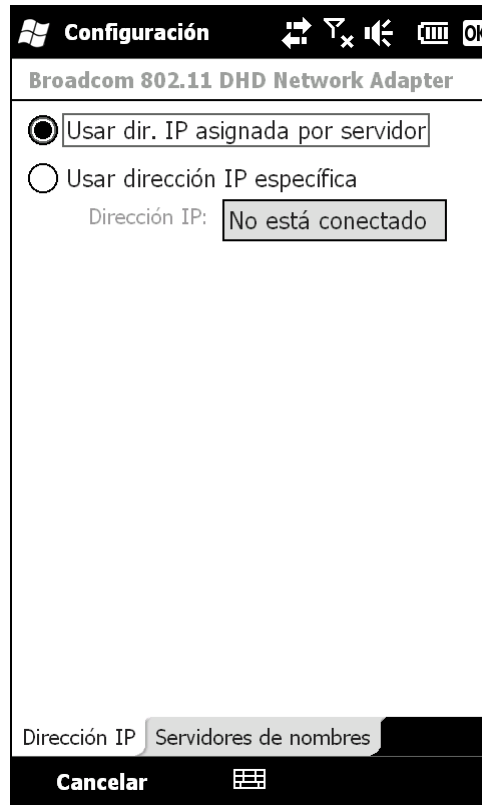
726. El gestor de protocolos activa las pilas de comunicaciones de IPv4 (tcpstk), IPv6 (tcpip6), IrDA (irdastk) y Bluetooth (btd) por defecto (la pila Bluetooth gestionada por AFD es la de Microsoft y no la de otros fabricantes, como WIDCOMM).

727. Su configuración se lleva a cabo a través de la siguiente clave del registro, correspondiente a la cadena de caracteres de las 4 pilas, “tcpstk tcpip6 irdastk btd”:

```
[HKEY_LOCAL_MACHINE\Comm\AFD]
```

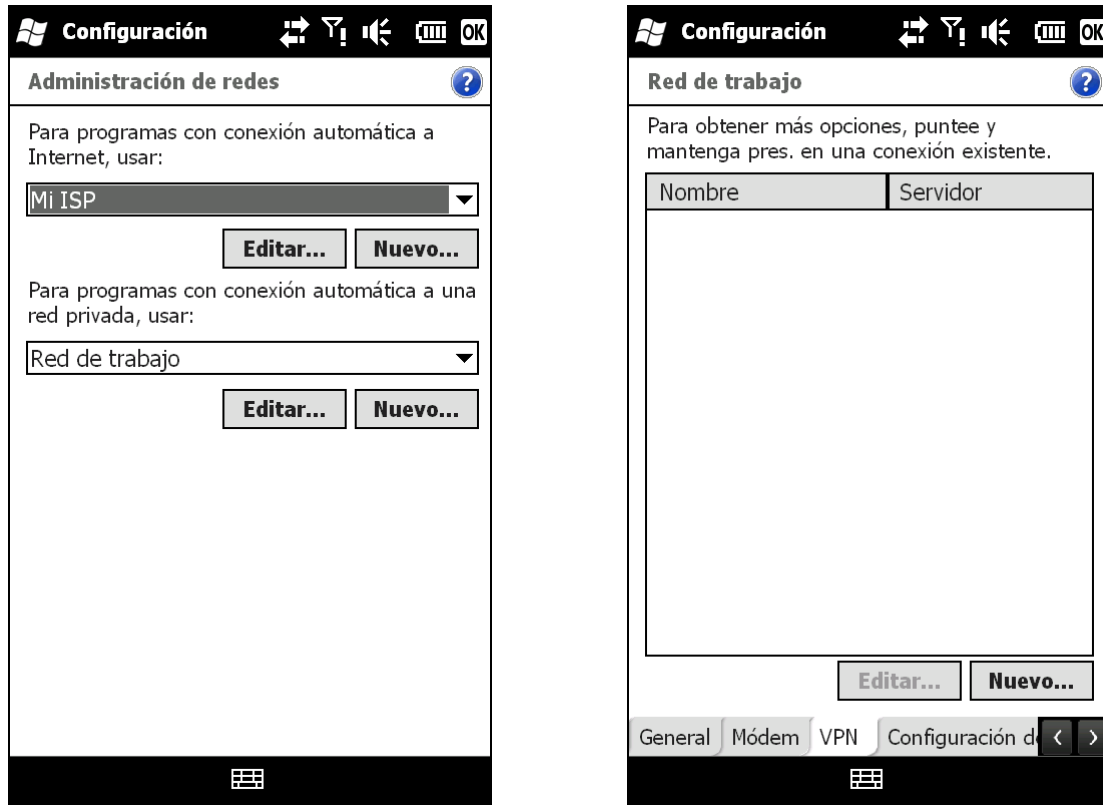
```
"Stacks"=hex(7):\
74,63,70,73,74,6B,00,74,63,70,69,70,36,00,69,72,64,61,73,74,6B,00,62,74,\
64,00,00
```

728. Para eliminar la disponibilidad de IPv6 basta con eliminar su pila asociada (cadena “tcpip6”: “74,63,70,69,70,36”) de la lista de AFD en el registro. Una vez deshabilitada el dispositivo móvil no generará peticiones DNS en busca del host “isatap” y la dirección IP del adaptador de red Wi-Fi no mostrará ninguna dirección IPv6 cuando no está conectado, sino el mensaje “No está conectado”:

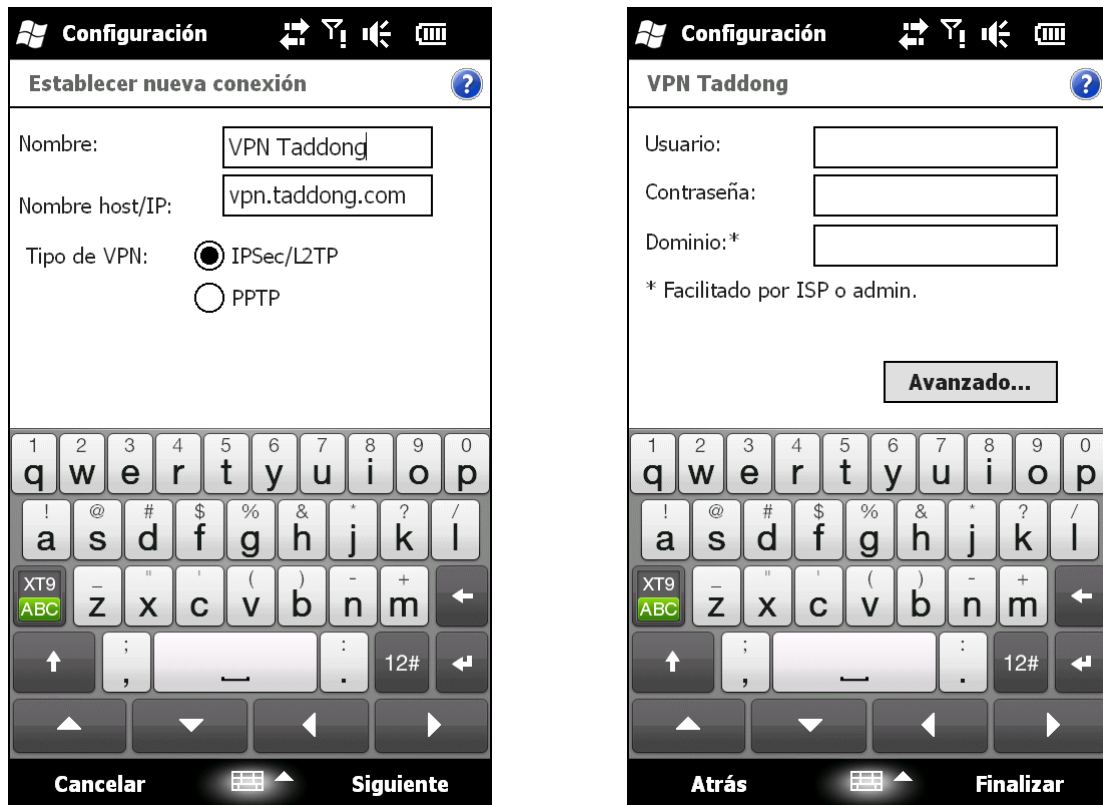


5.21.7 VPN

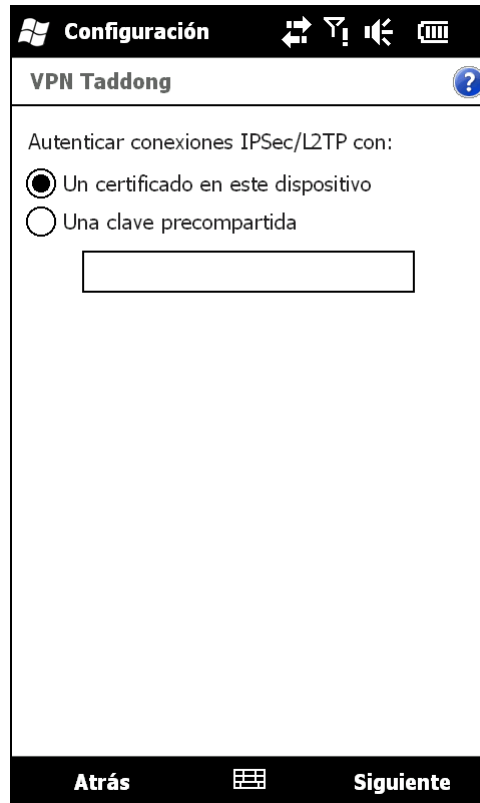
729. La conexión VPN del Connection Manager en Windows Mobile 6.5 (ver apartado “5.21.2. Perfil de conexión: Internet o Trabajo”) es empleada cuando se dispone de conexión a Internet, actualmente no se dispone de conexión a la red de “Trabajo”, y se necesita conectar a un equipo sin puntos en su nombre (o a alguna de las excepciones definidas). En ese caso se establecerá la VPN empleando la configuración de VPN definida en la red de “Trabajo”.
730. Una vez establecida la conexión con la VPN, el Connection Manager restringe las comunicaciones para que todo el tráfico sea cursado a través de la VPN hasta que ésta sea desconectada [Ref.- 54], es decir, no soporta *split horizon* (conexiones simultáneas directas hacia Internet y a través de la VPN).
731. La configuración de VPN (pestaña “VPN”) sólo está disponible al editar una red (o crear una nueva red) desde el perfil de conexión a una red privada o de “Trabajo”, disponible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Conexiones – Conexiones”, desde la pestaña “Avanzado” y a través del botón “Selec. redes”, accediendo a la pantalla de “Administración de redes”:



732. Windows Mobile 6.5 proporciona soporte para las siguientes tecnologías VPN: Point-to-Point Tunneling Protocol (PPTP, TCP/1723) y Layer Two Tunneling Protocol con Internet Protocol Security (L2TP/IPSec, en combinación). Windows Mobile 6.5 no dispone de soporte nativo para IPSec (sin L2TP), siendo necesario un cliente VPN de otra compañía para este tipo de conexiones.
733. Pese a que el algoritmo criptográfico AES es soportado por Windows Mobile 6.x para SSL/TLS, redes Wi-Fi basadas en WPA2, y el cifrado de la memoria del dispositivo móvil y de las tarjetas de almacenamiento externas, no está soportado en las VPN IPSec/L2TP. En su lugar se emplea ISAKMP e IPSec con 3DES.
734. A través del botón “Nuevo...” de la pestaña “VPN” es posible crear una nueva configuración de conexión VPN, para lo que es necesario especificar el nombre de la conexión (“VPN Taddong”), el nombre o dirección IP del servidor VPN (“vpn.taddong.com”) y el tipo de VPN según su tecnología:



735. Para completar la configuración, tanto para VPN's basadas en IPSec/L2TP como en PPTP, es necesario proporcionar las credenciales de acceso a la VPN, especificando el usuario, contraseña y/o dominio (imagen superior derecha), empleándose MS-CHAPv2, Microsoft Challenge Handshake Authentication Protocol versión 2. El botón "Avanzado..." permite especificar la dirección IP del dispositivo móvil y de los servidores DNS y WINS para la VPN.
736. En el caso de PPTP es posible habilitar el protocolo de encapsulamiento SLIP, *Serial Line Internet Protocol*. De ser viable (según la infraestructura VPN disponible), se recomienda no hacer uso del mismo, ya que es más inseguro que el protocolo PPP (empleado por PPTP por defecto).
737. Adicionalmente (y como paso previo), en el caso de VPN's basadas en IPSec/L2TP, se debe definir el método de autenticación: certificado o clave precompartida.
738. Se recomienda emplear un certificado para la autenticación de IPSec/L2TP al ser un mecanismo más seguro que el establecimiento de una clave precompartida entre el servidor de VPN y el dispositivo móvil (conocida por todos los usuarios de la VPN):

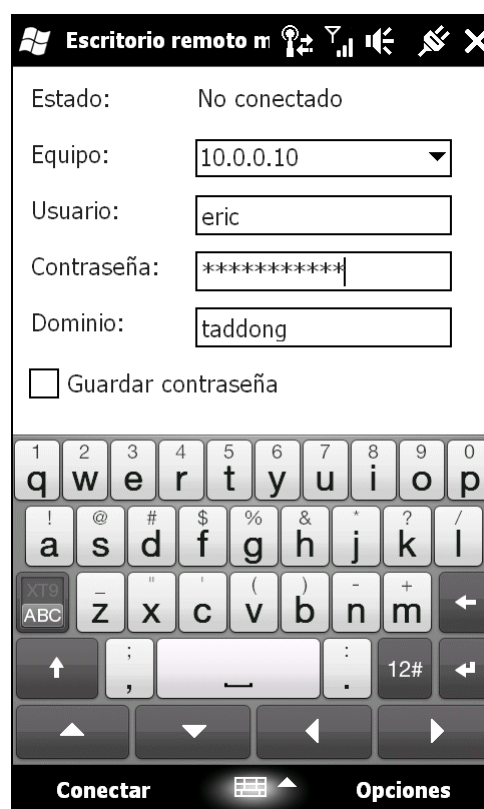


739. El certificado digital necesario para IPsec/L2PT es de tipo personal, y permitirá autenticar al dispositivo móvil y su propietario [Ref.- 75]. Adicionalmente es necesario instalar un certificado raíz, asociado a la generación del certificado digital empleado por el servidor de VPN.
740. Para instalar el certificado personal basta con transferir el fichero del certificado digital personal (.PFX o .P12) al dispositivo móvil y pulsar sobre él desde el explorador de ficheros, proporcionando la contraseña de protección del fichero que contiene el certificado personal [Ref.- 75].
741. Para instalar el certificado raíz basta con transferir el fichero del certificado digital (.CER, .DER o .P7B) al dispositivo móvil y pulsar sobre él desde el explorador de ficheros.
742. Una vez los certificados han sido importados en el dispositivo móvil, estarán disponibles a través del menú “Inicio – Configuración – Seguridad – Certificados”, en las pestañas “Personal” y “Raíz” respectivamente.

5.22 COMUNICACIONES EN ENTORNOS DE RED MICROSOFT

743. Los dispositivos móviles basados en Windows Mobile 6.5 pueden establecer conexiones a través de una red TCP/IP con carpetas compartidas en redes Microsoft y con recursos Microsoft Sharepoint.
744. Es posible configurar a través de Microsoft Exchange (y en concreto de la Exchange Management Console), si se permite el acceso a estos recursos, mediante las opciones “Windows Files Shares” y “Windows SharePoint Services”, respectivamente, de la pestaña “General” de la política de seguridad [Ref.- 34].

745. Windows Mobile 6.5 puede acceder a carpetas compartidas en redes Microsoft mediante el uso de NetBIOS sobre TCP/IP desde el explorador de ficheros, Internet Explorer Mobile, o aplicaciones de terceros, como Resco File Explorer (www.resco.net).
746. En caso de que dicho tipo de acceso no sea necesario, se recomienda deshabilitar su disponibilidad a través de las opciones de configuración de Microsoft Exchange mencionadas.
747. Windows Mobile 6.5 proporciona un cliente de acceso al escritorio remoto de otros equipos Windows (servicio también conocido como RDP, *Remote Desktop Protocol*, o *Terminal Services*), disponible desde el menú “Inicio – Herramientas (“Herram.”) – Escritorio remoto móvil”:



748. Pese a que el tráfico de la sesión de escritorio remoto se envía cifrado, un potencial atacante que capture el tráfico de escritorio remoto puede obtener el nombre del dispositivo móvil (en la trama “connect-initial”; por ejemplo, “HTC_HD2”) y el nombre de usuario (trama “Connection Request”; “eric” en el ejemplo inferior):

Cookie: msthash=eric

749. Se recomienda hacer uso del cliente de acceso a escritorio remoto en redes seguras dónde el riesgo de que un potencial atacante capture el tráfico de la sesión sea reducido.
750. Los dispositivos móviles basados en Windows Mobile 6.5 pueden hacer uso de los mecanismos de autenticación NTLM [Ref.- 59] disponible en entornos Microsoft.
751. La siguiente clave del registro permite definir el nivel de compatibilidad empleado para la autenticación NTLM, pudiendo emplear Microsoft Windows NT LAN Manager (LM) challenge-response o NTLM versión 2 (NTLMv2, protocolo que ofrece mayor nivel de seguridad). Los valores posibles son “0”, usar autenticación LM, “1” usar NTLMv2 si el servidor lo soporta, sino usar LM (valor por defecto para mayor

compatibilidad en versiones previas) y “3”, usar NTLMv2 (valor por defecto en Windows Mobile 6.5):

```
[HKEY_LOCAL_MACHINE\Comm\SecurityProviders\NTLM]  
"LmCompatibilityLevelClient"=dword:00000003
```

752. Se recomienda emplear únicamente NTLM versión 2 para la autenticación NTLM, la versión más segura del protocolo.
753. Adicionalmente se recomienda que el dispositivo móvil no caché (almacene en memoria) el hash LM empleado para la autenticación, parámetro configurable a través de la siguiente clave del registro:

```
[HKEY_LOCAL_MACHINE\Comm\SecurityProviders\NTLM]  
"NoLmHash"=dword:00000001
```

5.23 COPIAS DE SEGURIDAD

754. Microsoft proporciona una aplicación que debe ser instalada en un ordenador para la gestión y sincronización con el dispositivo móvil, y la realización de copias de seguridad locales entre el dispositivo móvil y el ordenador.
755. En el caso de ordenadores con Windows XP la aplicación se denomina Microsoft ActiveSync [Ref.- 8], mientras que en el caso de ordenadores con Windows Vista y Windows 7 debe emplearse el Centro de Dispositivos de Windows Mobile (Windows Mobile Device Center) [Ref.- 9].
756. En el caso de disponer de Microsoft Outlook en el ordenador, es posible sincronizar correos electrónicos (e-mail), el calendario, los contactos, las tareas y las notas (ver apartado “5.3. Microsoft ActiveSync”). Debe tenerse en cuenta que sólo es posible sincronizar a través de Outlook con un único ordenador.
757. Adicionalmente es posible sincronizar con Outlook de forma remota a través de Microsoft Exchange [Ref.- 67], empleando para ello una conexión de datos desde el dispositivo móvil, por ejemplo, a través de Internet, y protegida mediante SSL (ver apartado “5.9. Gestión empresarial de dispositivos basados en Windows Mobile”).
758. Se recomienda sincronizar el dispositivo móvil a través de alguno de los métodos mencionados, local, remoto o “en la nube” (analizado a continuación), con el objetivo de disponer de una copia de seguridad de los datos almacenados en el terminal y poder restaurarlos en caso de cualquier eventualidad relativa a la pérdida de dichos datos.

5.23.1 MICROSOFT MY PHONE

759. El servicio Microsoft My Phone [Ref.- 5], en adelante My Phone, proporciona diversas funcionalidades a los usuarios de dispositivos móviles basados en Windows Mobile, entre otras, la posibilidad de realizar copias de seguridad a través de Internet, constituyéndose como el principal servicio de sincronización “en la nube” de Microsoft para este tipo de dispositivos móviles (gratuito actualmente y con una capacidad de almacenamiento de 200MB).
760. My Phone permite realizar copias de seguridad y restaurar la información almacenada en el dispositivo móvil, incluyendo contactos, citas de calendario, tareas, mensajes de texto, música, fotos, vídeos, documentos, lista de favoritos del navegador y (algunos de estos datos almacenados en) tarjetas de almacenamiento.

-
761. Los contactos, citas de calendario y tareas sólo pueden sincronizarse si no se dispone de otra sincronización con un servidor Microsoft Exchange.
762. El acceso al servicio web de My Phone (<http://myphone.microsoft.com>) está protegido mediante usuario y contraseña, asociados a una cuenta Windows Live (<http://www.live.com>), y es utilizado empleando cualquier conexión de datos a Internet desde el dispositivo móvil.
763. Adicionalmente es posible acceder al servicio desde cualquier ordenador conectado a Internet para gestionar los dispositivos móviles sincronizados y sus datos, aunque debe tenerse en cuenta que el servicio emplea una conexión HTTP sin cifrar (excepto para el proceso de autenticación), por lo que la sesión puede ser interceptada por un potencial atacante.
764. El servicio My Phone está disponible para dispositivos móviles basados en Windows Mobile 6, Windows Mobile 6.1, y Windows Mobile 6.5.
765. My Phone puede ser accedido desde el menú “Inicio – Microsoft My Phone”. El asistente de configuración, tras aceptar los acuerdos de licencia y privacidad del servicio, permite introducir las credenciales de acceso al servicio (e-mail y contraseña) o crear una nueva cuenta de Windows Live.
766. Para poder hacer uso de las capacidades de sincronización automática es necesario guardar la contraseña en el dispositivo móvil, indicado por la correspondiente opción en la pantalla de acceso.
767. Pese a que la contraseña se almacena cifrada en el registro de Windows Mobile 6.5 bajo “HKEY_LOCAL_MACHINE\Comm\Security\CredMan\Creds”, se recomienda no almacenar la contraseña si sólo se va a hacer uso de las capacidades de sincronización manuales (y no automáticas).
768. A continuación se puede seleccionar el tipo de sincronización, automática (una al día; aconsejada para una conexión de datos permanente y sin limitaciones de transferencia de datos) o manual. Asimismo, deben definirse los elementos a sincronizar: contactos, citas de calendario, etc (mencionados exhaustivamente previamente).
769. Se recomienda evaluar en detalle la importancia y confidencialidad de cada uno de los tipos de datos a sincronizar con My Phone, considerando que la información privada almacenada en el dispositivo móvil podría ser accedida por un potencial atacante en caso de que dispongan de acceso al servicio My Phone y sus servidores asociados.
770. Las comunicaciones entre el dispositivo móvil y My Phone se realizan a través de sesiones HTTPS (TCP/443), cifradas con SSL/TLS.
771. Al final del proceso de actualización, se comprueba la disponibilidad de una actualización del cliente de acceso al servicio My Phone, y en caso de estar disponible, se ofrece u obliga al usuario a proceder a su descarga, ya que existen actualizaciones opcionales y obligatorias. Tras la instalación de la misma (MyPhone.cab) se debe reiniciar el dispositivo móvil.
772. La descarga de la actualización emplea conexiones HTTP (no cifradas, TCP/80) desde el dispositivo móvil hacia el servidor web “download.microsoft.com”, por lo que se recomienda emplear una red segura para realizar el proceso de configuración inicial y los posteriores procesos de actualización. En cualquier caso, en algún momento la transferencia de la actualización viajará por parte de la infraestructura de Internet sin cifrar, viéndose expuesta a su posible manipulación por un potencial atacante.
-

773. A través del botón “Menú”:

- Mediante “Opciones Sincronización”, es posible definir los elementos a sincronizar, incluyendo la activación de la ubicación actual mediante el GPS (deshabilitada por defecto).
- Mediante “Program. sincronización”, es posible definir el momento para realizar las sincronizaciones (manual, diaria, semanal, día y hora), y establecer configuración en itinerancia (*roaming*).
- Mediante “Cuenta – Dejar de usar el servicio” es posible dejar de usar el servicio, no eliminándose los datos en el dispositivo móvil o en el servidor My Phone.

774. My Phone permite sincronizar la localización actual del dispositivo móvil con el objetivo de poder obtener a través del interfaz web del servicio, en caso de pérdida, la ubicación del terminal la última vez que realizó la sincronización:



775. Para que la funcionalidad de localización del dispositivo móvil esté disponible es necesario que el terminal disponga de su ubicación precisa a través de su GPS en el momento de la sincronización, no siendo válida la información de ubicación estimada obtenida mediante otros métodos, como *Assisted-GPS* (A-GPS) o los servicios de localización de Google o HTC (ver apartado “5.15.3. Servicios de localización: Google y HTC”).

776. Para que la funcionalidad de localización sea efectiva es necesario configurar el dispositivo móvil para realizar la sincronización con My Phone automáticamente, preferiblemente con una frecuencia diaria. El proceso de sincronización se realiza de manera silenciosa, tanto si el terminal está siendo usado como si no (*standby*), y activándose la conexión de datos a través de las redes de telefonía móvil en caso de ser necesario (tras la sincronización la conexión de datos no es desactivada).

777. Asimismo, a través de las capacidades Premium del servicio My Phone (de pago), es posible conocer la ubicación actual del dispositivo móvil, hacer que el teléfono suene para localizarlo tras su pérdida, y proteger la información que almacena mediante el

bloqueo del terminal o incluso mediante la eliminación de los datos almacenados en el dispositivo móvil:

Características premium

Puedes usar el paquete de características premium hasta el **martes, 17 de agosto de 2010** a las **1:28**.

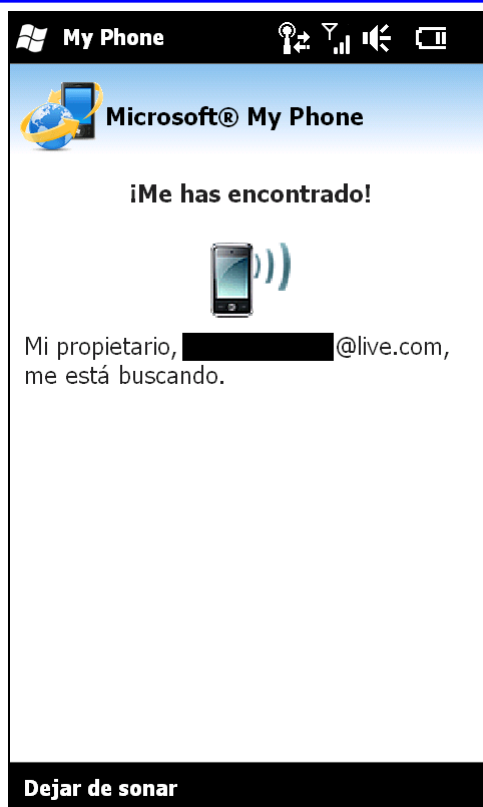
 **Hacer sonar el teléfono**
El teléfono sonará a un volumen alto durante 60 segundos, aun cuando esté establecido en modo "Silencio" o "Vibración".
[Hacer sonar](#) (3 restantes)

 **Bloquear el teléfono**
Bloquea el teléfono para que nadie más pueda usarlo. También puedes escribir un mensaje para mostrar en la pantalla para indicar un modo de contacto a la persona que lo encuentre.
[Bloquear](#) (1 restantes)

 **Borrar el teléfono**
Borra el teléfono y la tarjeta de almacenamiento para garantizar que los datos estén seguros. El teléfono se restaura a la configuración predeterminada de fábrica.
[Borrar](#) (1 restantes)

Nota: el servicio My Phone hace uso de mensajes de texto ocultos (SMS no visibles por el usuario) para establecer la comunicación con el dispositivo móvil y llevar a cabo las acciones descritas. Para ello es necesario proporcionar el número de teléfono móvil (en formato internacional, ej.+34-609123456) y My Phone comprobará si el operador de telefonía empleado es compatible con el servicio.

778. Al hacer sonar el teléfono remotamente (durante 60 segundos), el dispositivo móvil muestra un mensaje indicando que su propietario, identificado por la dirección de e-mail de la cuenta de Windows Live asociada a My Phone, está buscando el terminal:



779. El bloqueo del teléfono remotamente permite fijar el PIN a emplear para su desbloqueo, así como mostrar un mensaje en pantalla para la devolución del terminal al propietario:

Bloquear y mostrar un mensaje en la pantalla del teléfono

Escribe un PIN de 4 dígitos para desbloquear el teléfono. Durante los próximos 7 días se intentará bloquear el teléfono. Puedes consultar el estado de la solicitud en esta página.

PIN:

Confirmar PIN:

Muestra un mensaje opcional en la pantalla del teléfono. Por ejemplo, un modo de contacto para que puedan devolverte el teléfono.

43/52

780. A través del interfaz web de My Phone es posible conocer el estado de la operación de bloqueo:



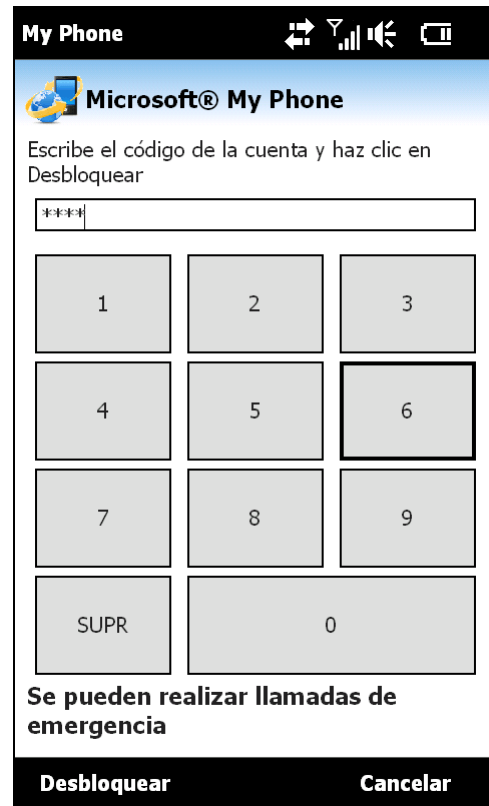
Bloquear el teléfono

Bloquea el teléfono para que nadie más pueda usarlo. También puedes escribir un mensaje para mostrar en la pantalla para indicar un modo de contacto a la persona que lo encuentre.

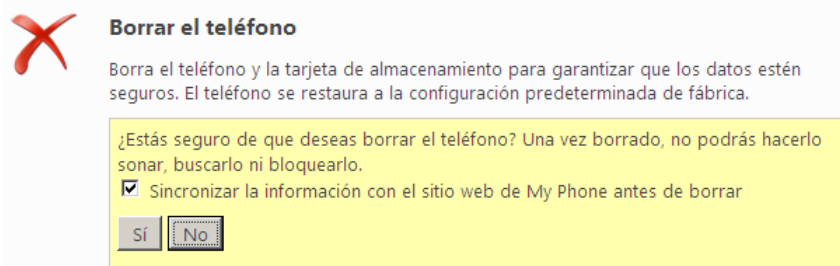
El bloqueo solicitado el martes, 10 de agosto de 2010 a las 1:38 se ha realizado correctamente

PIN: 9876

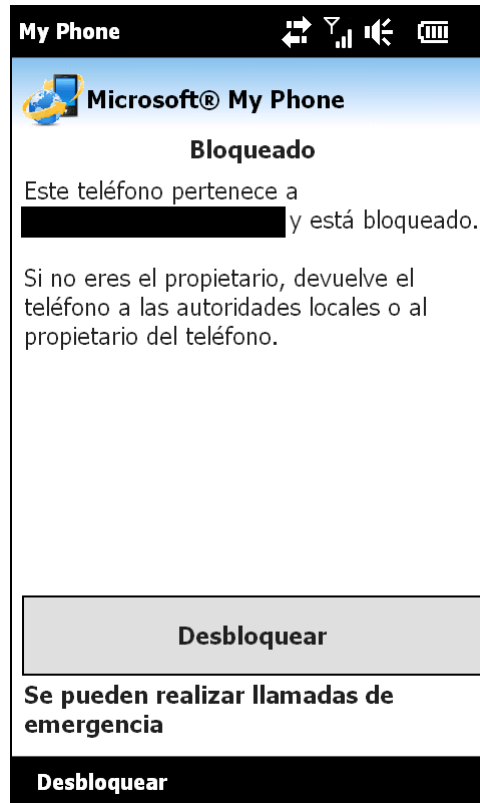
781. Tan pronto el terminal está disponible a través de la red de telefonía móvil, será bloqueado por My Phone, permitiendo únicamente la realización de llamadas de emergencia. Al desbloquear el dispositivo móvil, éste es reiniciado, pudiendo ser desbloqueado mediante el PIN del propietario existente previamente a la pérdida:



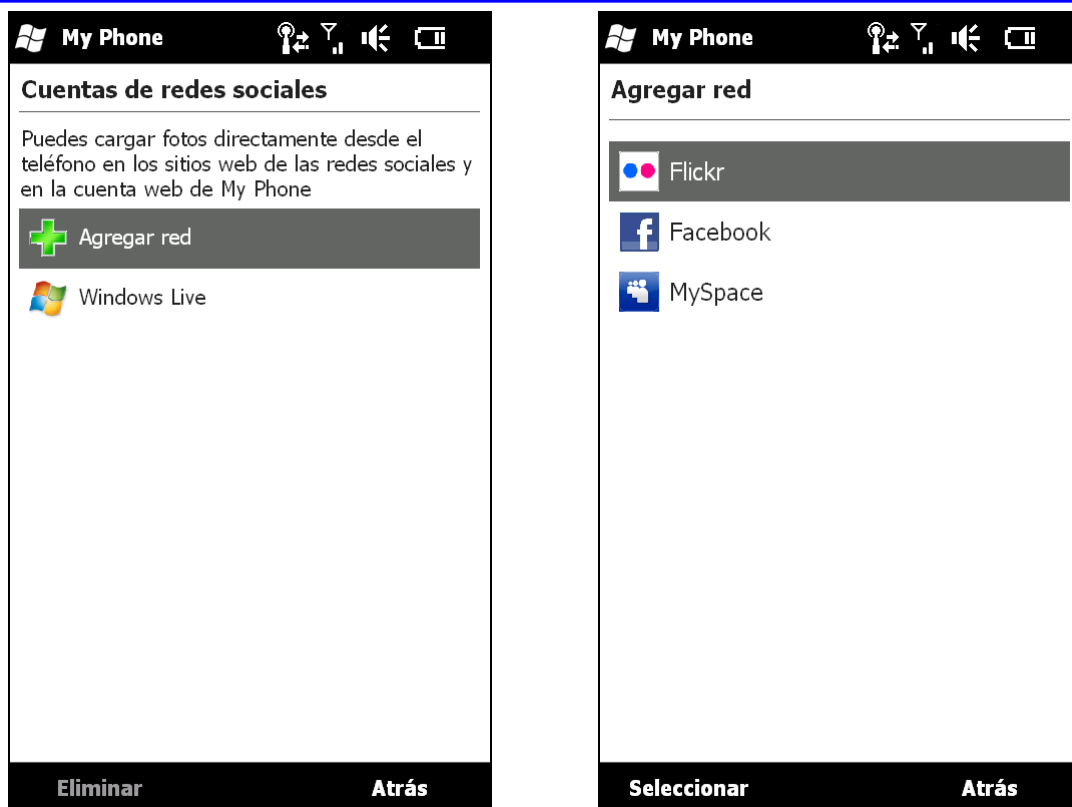
782. El proceso remoto de borrado de datos afecta tanto al contenido del dispositivo móvil como de las tarjetas de almacenamiento externas que éste pueda tener conectadas.
783. Antes de realizar el borrado es posible sincronizar los datos con My Phone para poder disponer de la última copia de seguridad actualizada:



784. Temporalmente durante unos segundos, mientras se realiza la sincronización, el dispositivo móvil muestra la pantalla de bloqueo de My Phone, indicando quién es su propietario mediante la cuenta de Windows Live, e instando a quien lo posee actualmente a la devolución del mismo:



785. Una vez ejecutada la operación de borrado, el teléfono es eliminado de la cuenta My Phone, y se realiza el restablecimiento de fábrica o *hard reset*.
786. Con el objetivo de recuperar un dispositivo móvil perdido se recomienda hacer uso de las capacidades Premium del servicio My Phone (en caso de estar disponibles) en el siguiente orden: localizar la ubicación del teléfono, bloquear el teléfono para evitar su uso, hacerlo sonar para notificar su búsqueda y, finalmente, borrar los datos del mismo.
787. En el caso de que el objetivo principal no sea la recuperación del dispositivo móvil sino la eliminación de sus datos, debido a su carácter confidencial y privado, se puede proceder a la operación de borrado directamente tras intentar obtener su ubicación.
788. My Phone permite enviar fotografías desde el dispositivo móvil a diferentes redes sociales, como Facebook, Flickr, MySpace y Windows Live. Antes de poder hacer uso de esta funcionalidad es necesario añadir la red social a My Phone, a través del botón “Menú” y las opciones “Compartir Fotos – Redes Sociales”:



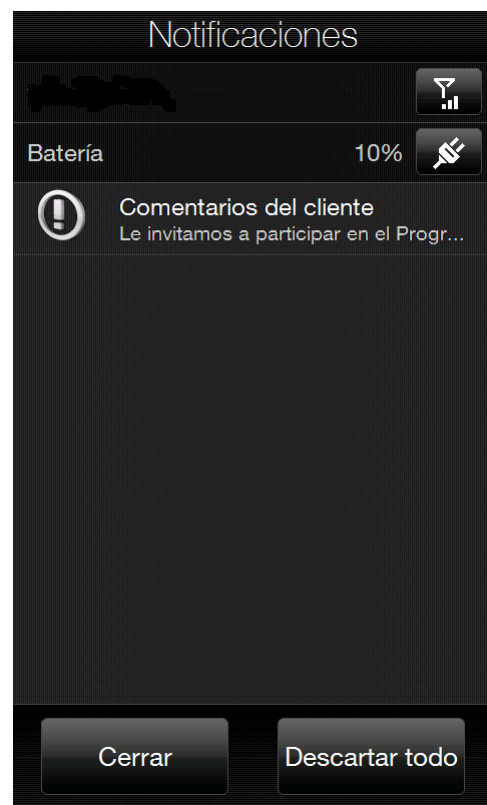
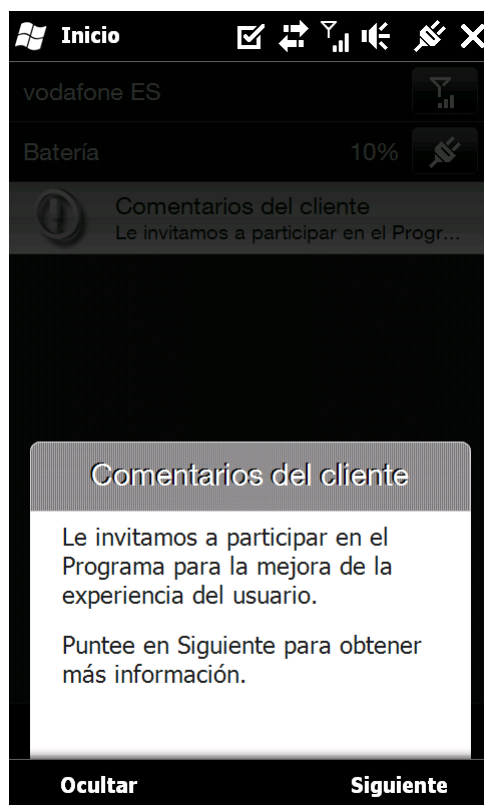
789. Al agregar el vínculo entre My Phone y una red social es necesario proporcionar las credenciales de acceso a la red social elegida:



790. Se recomienda evaluar los riesgos de compartir las credenciales de acceso en una red social con el servicio de otra compañía, como My Phone, y los riesgos de suplantación de identidad que esta compartición de información pudiera tener asociados.
791. La configuración de las redes sociales en My Phone está disponible en la siguiente clave del registro:
- ```
HKEY_LOCAL_MACHINE\Software\Microsoft\My Phone\Publish\Services
```
792. Las fotografías pueden ser enviadas a través del botón “Menú” y las opciones “Compartir fotos - Compartir”, seleccionando la fotografía a enviar (mediante una pulsación larga), y la opción “Compartir”. Se mostrarán los destinos con los que se puede compartir la fotografía, incluyendo My Phone y las diferentes redes sociales dadas de alta previamente. Al llevarse a cabo la siguiente sincronización, la fotografía será compartida en la red social.
793. Se recomienda evaluar en detalle el uso de esta funcionalidad para la distribución y publicación de fotografías en redes sociales, especialmente aquellas tomadas con información de localización o GPS (ver apartado “5.15.5. Información geográfica en fotografías”), que desvelarían detalles de la ubicación del usuario en el momento de su obtención.

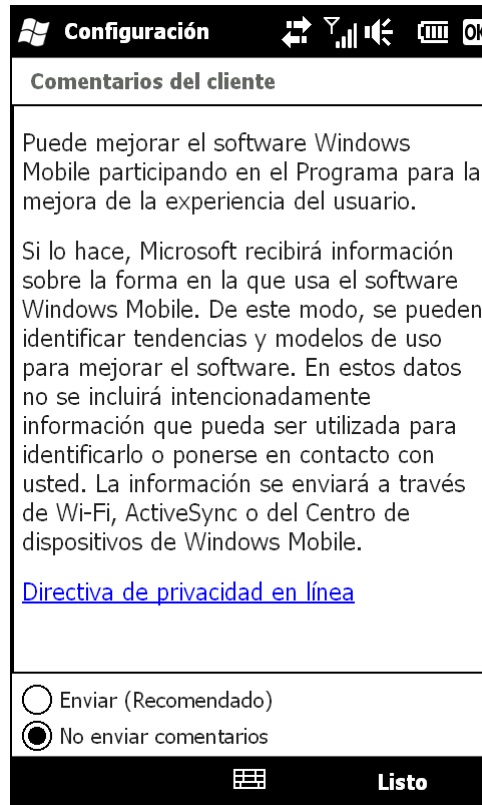
## 5.24 SERVICIOS DE NOTIFICACIÓN OPCIONALES

794. Se recomienda no hacer uso de ningún servicio opcional del dispositivo móvil que pueda revelar información sobre el mismo o su propietario, como por ejemplo el “Programa para la mejora de la experiencia del usuario”, presentado a través del mensaje mostrado en la imagen inferior, que aparecerá adicionalmente en las notificaciones generales del dispositivo móvil (accesible tras pulsar en la barra superior de Windows Mobile 6.5):

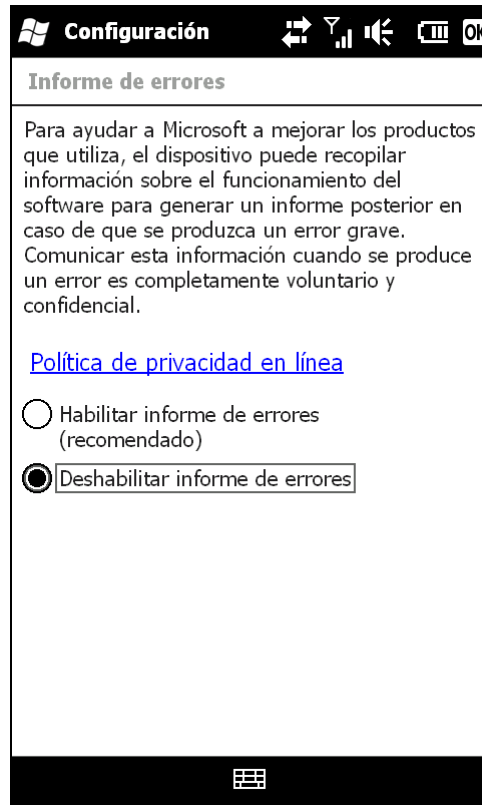


795. El botón “Ocultar” permite eliminar el mensaje y no participar en dicho programa.

796. A través del menú “Inicio – Configuración – Actualizaciones y comentarios – Comentarios del cliente” es posible deshabilitar este servicio de forma permanentemente al seleccionar la opción “No enviar comentarios”, no recomendada por Microsoft, pero sí recomendada desde el punto de vista de seguridad y privacidad del usuario:



797. Igualmente, se recomienda deshabilitar de forma permanente el servicio de envío de informes de errores a Microsoft, mediante la opción “Deshabilitar informe de errores” del menú “Inicio – Configuración – Actualizaciones y comentarios – Informes de errores”, habilitado por defecto. De nuevo, esta opción no es recomendada por Microsoft, pero sí está recomendada desde el punto de vista de seguridad y privacidad del usuario:



798. La siguiente clave del registro gestiona la configuración del programa para la mejora de la experiencia del usuario, activándose al emplear el valor “1” en ambos parámetros:

```
[HKEY_LOCAL_MACHINE\System\SQM]
"Enabled"=dword:00000000
"UploadEnabled"=dword:00000000
```

799. La siguiente clave del registro gestiona la configuración del servicio de envío de informes de errores a Microsoft, activándose al emplear el valor “1”:

```
[HKEY_LOCAL_MACHINE\System\ErrorReporting\DumpSettings]
"DumpEnabled"=dword:00000000
```

## 5.25 SERVICIOS DE DATOS

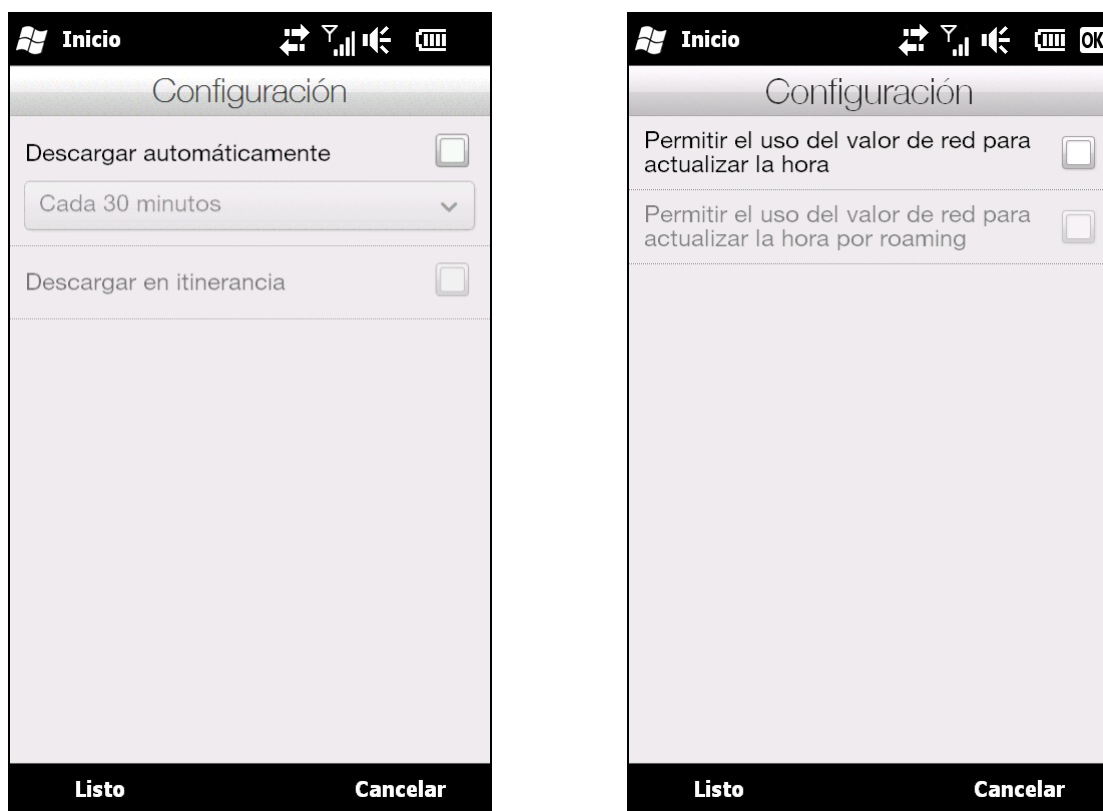
800. La configuración individualizada de los servicios de datos, y las aplicaciones cliente que hacen uso de éstos, está disponible a través del menú “Inicio – Configuración – Servicios de datos”:



801. La aplicación principal a nivel empresarial que hace uso de servicios de datos es ActiveSync, asociada a Exchange ActiveSync, que permite al usuario autenticarse con su dirección de correo electrónico y una contraseña para realizar la sincronización de correo electrónico (e-mail), contactos, citas de calendario y tareas (ver apartado “5.30. correo electrónico” y “5.9.1. Gestión empresarial de dispositivos basados en Windows Mobile”).
802. En la sección “Utilidades” se dispone de la lista de aplicaciones cliente que hacen uso de los servicios de datos, como por ejemplo “Valores bursátiles” (o “Bolsa”), “Tiempo” (o “Clima”, analizado en detalle en el apartado “5.15.3. Servicios de localización: Google y HTC” junto a los servicios de localización) o “Sincronización de hora”.
803. La aplicación de bolsa, “Valores bursátiles”, realiza peticiones HTTP (no cifradas) desde el dispositivo móvil hacia “api.htc.go.yahoo.com”, revelando información de la versión de la aplicación y la lista de símbolos de los que se desea obtener información bursátil:
- ```
POST /dgw?apptype=finance&imei=HTCMOBILE&src=HTC01
...
<request devtype="HTC_Model" deployver="HTCFinanceWidget 0.1"
app="HTCFinanceWidget" appver="0.1.0"...
```
804. La aplicación de sincronización de hora emplea peticiones de información horaria (TCP/13) a través de Internet, por ejemplo con los servidores “time.nist.gov” y “time-nw.nist.gov”, para actualizar la hora del dispositivo móvil.
805. La configuración de los servicios de datos de todas las aplicaciones cliente permite habilitar o deshabilitar la descarga automática, fijar el intervalo de tiempo entre descargas, y habilitar o deshabilitar de forma independiente su utilización en el extranjero, *roaming*, al estar conectado a otras redes de telefonía móvil.

806. Salvo que se realice un uso frecuente de las aplicaciones cliente mencionadas, se recomienda deshabilitar la descarga de datos automática y su utilización en itinerancia (deshabilitada por defecto) para todas ellas (imagen inferior izquierda). Además de por limitar los gastos asociados al servicio de datos, desde el punto de vista de seguridad se recomienda minimizar su utilización en redes extranjeras, ya que en algunos países (por ejemplo de África y Asia) no se hace uso de mecanismos de cifrado en las redes de los operadores de telefonía móvil [Ref.- 1]:

Nota: los servicios de datos son utilizados a través de cualquiera de las redes de datos disponibles desde el dispositivo móvil, como por ejemplo las redes de telefonía 2G/3G o las redes Wi-Fi. Las recomendaciones de seguridad aplican igualmente a todas ellas, por lo que la ausencia de cifrado en las comunicaciones de un servicio o aplicación puede tener impacto tanto en redes de telefonía no cifradas, como en redes Wi-Fi no cifradas.



Nota: las opciones de descarga automática de datos están también disponibles para cada una de las aplicaciones mencionadas (“Tiempo” (o “Clima”) y “Valores bursátiles” (o “Bolsa”)) a través de su propio menú de configuración, disponible una vez se accede a la aplicación, desde el botón “Menú” y la opción “Configuración”.

807. Las siguientes claves del registro gestionan los parámetros de configuración de la descarga automática y en itinerancia de las aplicaciones cliente, “Tiempo” (primeros 3 parámetros) y “Valores bursátiles” (últimos 3 parámetros). El valor “0” es empleado al ser activada la descarga automática, “X.AutoDownloadOff”, y el valor “1” al ser activada la descarga en itinerancia, “X.DownloadWhenRoaming” (ambas opciones no recomendadas). El intervalo de tiempo entre actualizaciones para la información

meteorológica y la información bursátil está definido en minutos con su valor hexadecimal, es decir, 1 hora (60 minutos, 0x3C):

```
[HKEY_CURRENT_USER\Software\HTC\Manila]
"Data.AutoDownloadOff"=dword:00000001
"Data.DownloadWhenRoaming"=dword:00000000
"Weather.AutoDownloadInterval"=dword:0000003C
"StockData.AutoDownloadOff"=dword:00000001
"StockData.DownloadWhenRoaming"=dword:00000000
"StockManagerAUMInterval"=dword:0000003C
```

808. Se recomienda deshabilitar la sincronización horaria del dispositivo móvil a través de Internet (imagen superior derecha). La siguiente clave del registro gestiona los dos parámetros de configuración de la sincronización horaria. El valor “2” indica que ambas opciones están deshabilitadas (configuración recomendada), el valor “1” que ambas están activas y el valor “0” indica que la opción de itinerancia ha sido deshabilitada:

```
[HKEY_LOCAL_MACHINE\Software\HTC\TimeZoneAutoFix]
"CreatePDPAlways"=dword:00000002
```

809. La sección de redes sociales permite activar o desactivar mediante los botones deslizantes la utilización de cada una de las redes sociales soportadas por el dispositivo móvil, Facebook, Twitter y YouTube, habilitando así las notificaciones desde éstas y la posibilidad de descargar o subir contenidos.

810. Las siguientes claves del registro gestionan la activación o desactivación de las aplicaciones cliente de acceso a las redes sociales. Para su activación es necesario introducir las credenciales de acceso a la red social, o que éstas estén almacenadas en el dispositivo móvil (ver apartado “5.31. Redes sociales”):

- Facebook emplea el parámetro “IsLogin”, con valor “1” al estar activado, y almacena la cuenta (e-mail) empleada para el servicio:

```
[HKEY_CURRENT_USER\Software\HTC\Manila]
"Facebook.Account"="usuario@dominio.es"
"Facebook.IsLogin"=dword:00000001
```

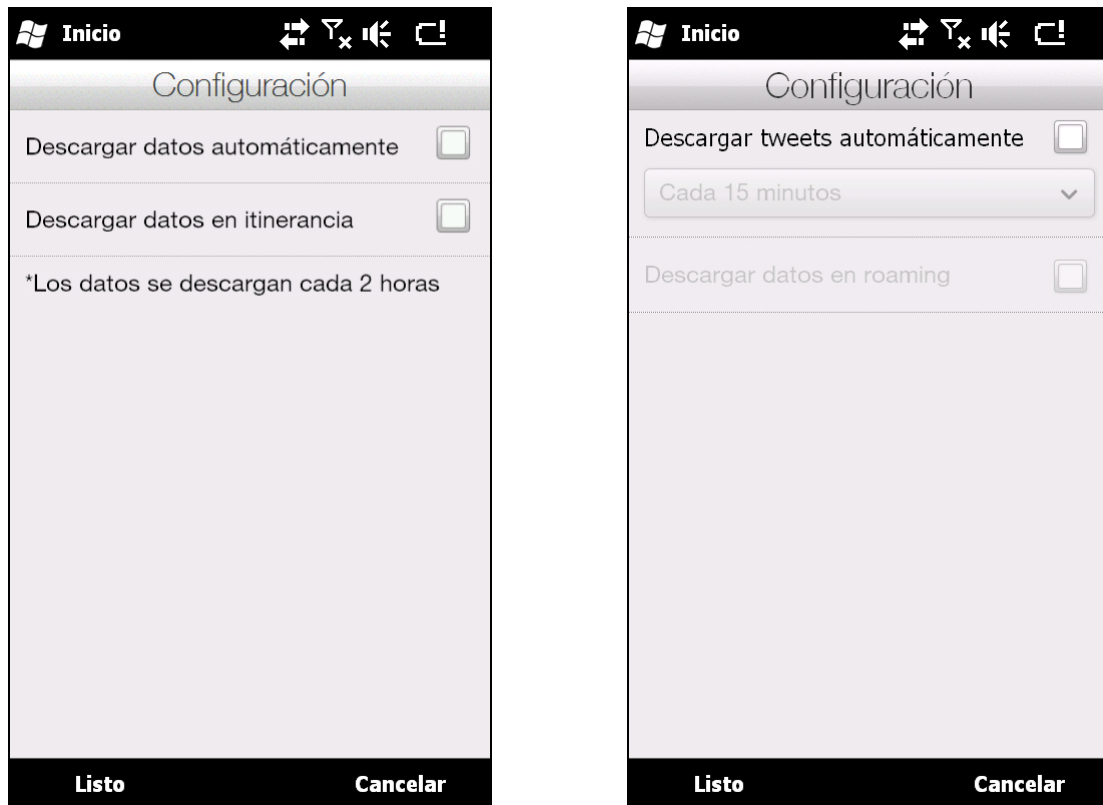
- Twitter no dispone de un parámetro de activación o desactivación en el registro; el estado de activación está asociado a la existencia de un valor en la siguiente clave del registro, que almacena el nombre de usuario (y no tiene valor asignado al desconectarse):

```
[HKEY_LOCAL_MACHINE\Software\HTC\HTCAccountManager]
"TwitterUsername"="Ana Garcia"
```

- YouTube no dispone de un parámetro de activación o desactivación en el registro; el estado de activación está asociado a la existencia de un valor en la siguiente clave del registro, que almacena el token de sesión (y no tiene valor asignado al desconectarse):

```
[HKEY_LOCAL_MACHINE\Software\HTC\HTCAccountManager]
"YoutubeToken"="JJSSVV...2010nto"
```

811. Seleccionando los botones de las aplicaciones Facebook (imagen inferior izquierda) y Twitter (imagen inferior derecha), no así con YouTube, es posible configurar las actualizaciones automáticas para estas redes sociales:



Nota: las opciones de descarga automática de datos están también disponibles para la aplicación de acceso a la red social Twitter (no así para Facebook o YouTube) a través de su propio menú de configuración, disponible una vez se accede a la aplicación, desde el botón “Menú” y la opción “Configuración”.

812. Se recomienda desactivar la conexión automática a todas las redes sociales disponibles, salvo que se haga un uso frecuente de sus servicios. La activación de las diferentes redes sociales en los servicios de datos prevalece incluso tras reiniciar el dispositivo móvil, o tras un restablecimiento software o *soft reset*.
813. Las siguientes claves del registro gestionan los parámetros de configuración de la descarga automática y en itinerancia de las aplicaciones cliente de redes sociales, “Facebook” (primeros 2 parámetros) y “Twitter” (últimos 3 parámetros). Para Facebook, el valor “0” indica que no se permite la descarga automática, ni estándar ni en itinerancia (opción recomendada), el valor “1” indica que no se permite en itinerancia, y el valor “3” que se permiten ambas descargas automáticas. Para Twitter, el valor “1” es empleado por los dos parámetros para activar tanto la descarga automática y como la descarga en itinerancia (ambas opciones no recomendadas). El intervalo de tiempo entre actualizaciones para Twitter está definido en minutos con su valor hexadecimal, es decir, 15 minutos (0xF):

```
[HKEY_CURRENT_USER\Software\HTC\Manila]
"Facebook.ConnectionSetting"=dword:00000000

[HKEY_CURRENT_USER\Software\HTC\TwitterApp]
"dwAutoCheckTweetsPeriod"=dword:0000000F
"IsCheckTweetAuto"=dword:00000000
"IsDownloadWhenRoaming"=dword:00000000
```

814. Los detalles del proceso de conexión y autenticación, así como las vulnerabilidades de seguridad, de cada una de las redes sociales disponibles están disponibles en el apartado “5.31. Redes sociales”.

5.26 GESTIÓN EMPRESARIAL DE SEGURIDAD DE LAS APLICACIONES

815. Desde el punto de vista empresarial, Windows Mobile 6.5 permite disponer de un control detallado de la ejecución de las aplicaciones instaladas en el dispositivo móvil, como por ejemplo bloquear la ejecución del navegador web (*browser*), o de las aplicaciones no firmadas.

816. Su configuración es posible a través de Microsoft Exchange (y en concreto de la Exchange Management Console), mediante múltiples opciones disponibles en la pestaña “Advanced” de la política de seguridad [Ref.- 34] [Ref.- 37]:

- *Allow browser*: permitir al dispositivo móvil el uso del navegador web, Internet Explorer Mobile.
- *Allow consumer mail*: permitir al dispositivo móvil el acceso a cuentas de correo no hospedadas en Microsoft Exchange, como por ejemplo, cuentas accedidas a través de IMAP4 o POP3 (AOL, Gmail, etc).
- *Allow unsigned applications*: permitir la ejecución de aplicaciones no firmadas en el dispositivo móvil.
- *Allow unsigned installation packages*: permitir la instalación de aplicaciones no firmadas en el dispositivo móvil.
- *Allowed applications*: lista de aplicaciones permitidas, tanto para su instalación como para su ejecución.
- *Blocked applications*: lista de aplicaciones bloqueadas, tanto para su instalación como para su ejecución.

817. Las propiedades de la pestaña “Advanced” de la política de seguridad de Microsoft Exchange para dispositivos móviles constituyen capacidades avanzadas de configuración de Exchange ActiveSync, por lo que sólo están disponibles si se dispone de la licencia Exchange Enterprise Client Access License (CAL).

5.27 APLICACIONES CLIENTE

818. Windows Mobile 6.5 incluye por defecto las siguientes aplicaciones (aunque las mismas pueden variar en función del fabricante u operador de telefonía móvil):

- Internet Explorer Mobile, previamente conocido como Pocket Internet Explorer (Pocket IE).
- Office Mobile: Word, Excel, PowerPoint y OneNote (Mobile).
- Windows Media Player.
- .NET Compact Framework 2.0.
- Windows Live para Windows Mobile (Hotmail y Messenger).
- Buscador Bing.
- Microsoft My Phone.

- Adobe Reader LE (ver apartado “5.29.4. Contenidos Adobe PDF”).
 - Opera Mobile (navegador web por defecto en dispositivos móviles HTC).
819. Windows Mobile 6.5 incluye la opción de actualizar la apariencia visual del dispositivo móvil a través de temas (*Designer themes*). Los usuarios deben prestar especial atención al origen de un tema antes de su instalación, con el objetivo de instalar únicamente temas desde fuentes fiables y evitar así la instalación de *malware*.
820. Windows Mobile 6.5 incorpora nuevos componentes (*MSN Widgets*), disponible en función del fabricante u operador de telefonía móvil, para el acceso a información meteorológica y a información bursátil en tiempo real a través de Internet.
821. Otros ejemplos de software opcional incluido en Windows Mobile 6.5 por defecto, disponible en función del fabricante u operador de telefonía móvil, son:
- Plugin de Adobe Flash Lite, que permite la visualización de contenidos Flash desde el navegador web, Internet Explorer Mobile (ver apartado “5.29.3. Contenidos Adobe Flash”).
 - Lector RSS para el acceso a noticias de páginas web y blogs en Internet, denominado NewsBreak Lite (creado por Illium).
 - Cliente de acceso a YouTube (“YouTube para Pocket PC”) de HTC.

5.28 ACTUALIZACIÓN DE APLICACIONES MICROSOFT

822. Con el objetivo de disponer del mayor nivel de seguridad posible en el dispositivo móvil, se recomienda disponer de la última versión de todas las aplicaciones instaladas, especialmente aquellas desarrolladas por Microsoft (propietario del sistema operativo).
823. La información de Microsoft respecto a actualizaciones de software y descargas disponibles para Windows Mobile puede obtenerse de los siguientes enlaces:
- Mobile apps from Microsoft:
<http://www.microsoft.com/windowsmobile/es-es/meet/microsoft-applications.msp>
 - Windows Phone Downloads:
<http://www.microsoft.com/windowsmobile/es-es/downloads/default.msp>

824. La instalación de actualizaciones software en Windows Mobile conlleva un proceso manual y poco homogéneo respecto a su equivalente en equipos de escritorio, dificultando el proceso de actualización para usuarios no experimentados y disminuyendo el nivel de seguridad de los dispositivos móviles debido a la existencia y utilización de software vulnerable.

5.28.1 BING

825. Algunas aplicaciones de Microsoft disponibles en el dispositivo móvil comprueban automáticamente la última versión disponible, la comparan con la versión instalada en el terminal, y ofrecen o fuerzan al usuario a instalar la nueva versión.
826. Por ejemplo, la aplicación para acceder al buscador de Internet Bing (de Microsoft), disponible desde el menú “Inicio – Bing”, realiza este tipo de comprobación mediante una conexión HTTP (TCP/80), no cifrada, a “mobile.search.live.com”, enviando

información muy detallada del dispositivo móvil (“en-USIWM 4.6.9179.1 (OEM) (en-US) (WinCE 5.2.21869) () (PocketPC HTC HD2 T8585)”) y de su localización GPS. La aplicación se identifica como “User-Agent: Windows Live Mobile Local Search”.



Nota: La información de localización de GPS es empleada por los servicios de localización de Bing (ver apartado “5.15.4. Servicios de localización: Bing”).

827. La respuesta HTTP recibida incluye el mensaje de actualización, y el enlace para la descarga de la nueva versión - “We've made some improvements to Bing. To continue using the Bing app, you must update now”:

<http://static.appserver.m.bing.net/binaries/winmo/v1/Bing.CAB>

828. Tras solicitar confirmación por parte del usuario para seleccionar la ubicación dónde se almacenará la actualización, el fichero es descargado mediante HTTP y se procede a su instalación.

829. La comunicación HTTP no cifrada puede ser interceptada y manipulada por un potencial atacante para ejecutar la instalación de software malicioso, por lo que se recomienda evaluar en detalle cuándo y dónde se lleva a cabo la actualización, y si el fichero de instalación recibido genera algún mensaje de error asociado a su firma digital.

5.28.2 OFFICE MOBILE

830. La actualización de otras aplicaciones, como Microsoft Mobile Office, en adelante Office Mobile (Word, Excel, PowerPoint y OneNote Mobile), debe realizarse manualmente, descargando la nueva versión (versión 6.1) de la web de Microsoft [Ref.- 93] o a través

de Microsoft Marketplace (versión 6.5) [Ref.- 94] (ver apartado “5.32. Aplicaciones de terceros: Windows Marketplace for Mobile”).

831. La versión actual de Office Mobile puede obtenerse desde el menú “Inicio”, accediendo a “Office Mobile” y ejecutando “OneNote Mobile”. A través del botón “Menú” es posible acceder a la opción “Acerca de”: “Versión de compilación 12.0.4518.1155” (asociada a Office Mobile 6.1).

832. La versión real de Office Mobile está disponible en la siguiente clave del registro, por ejemplo, para la versión 6.1:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Office Mobile\Version]
"Major"=dword:00000006
"Minor"=dword:00000001
```

833. Se recomienda actualizar Office Mobile a la versión 6.5 desde Microsoft Marketplace, operación que requiere reiniciar el dispositivo móvil. El icono “Office Mobile” es reemplazado por “Office Mobile 2010” y se añade soporte para “Sharepoint Workspace Mobile 2010”.

834. Tras actualizar a Office Mobile 2010 la versión en el registro es la 14.0 (0xE.0x0):

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Office Mobile\Version]
"Major"=dword:0000000E
"Minor"=dword:00000000
```

Nota: la numeración de versiones de Microsoft Office Mobile puede crear cierta confusión con la numeración de versiones de Windows Mobile, no existiendo ninguna relación entre ellas. Microsoft Office Mobile 6.1 puede ser instalado en dispositivos Windows Mobile 5.0 y 6.x, mientras que Office Mobile 2010 (versión 6.5) es una actualización compatible con dispositivos basados en Windows Mobile 6.5 y con una versión previa de Office Mobile.

5.28.3 .NET COMPACT FRAMEWORK

835. La versión de .NET Compact Framework está disponible en el registro (por ejemplo “2.0.7045.00”, correspondiente al Service Pack 2):

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\NETCompactFramework]
"2.0.7045.00"=dword:00000001
```

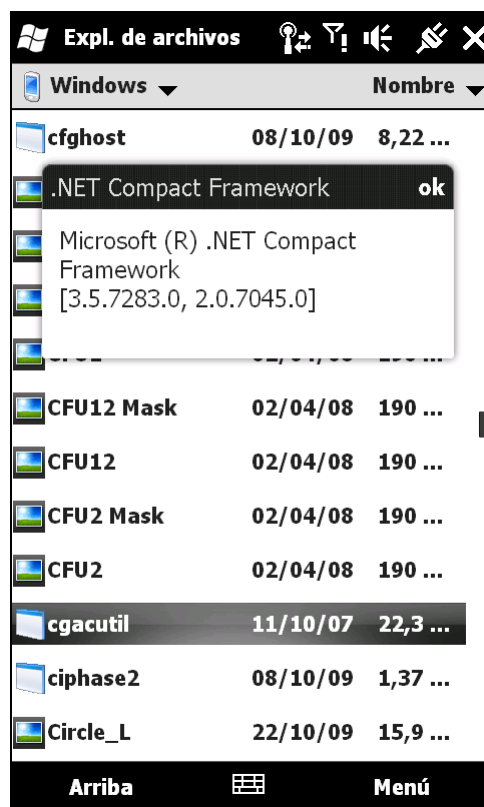
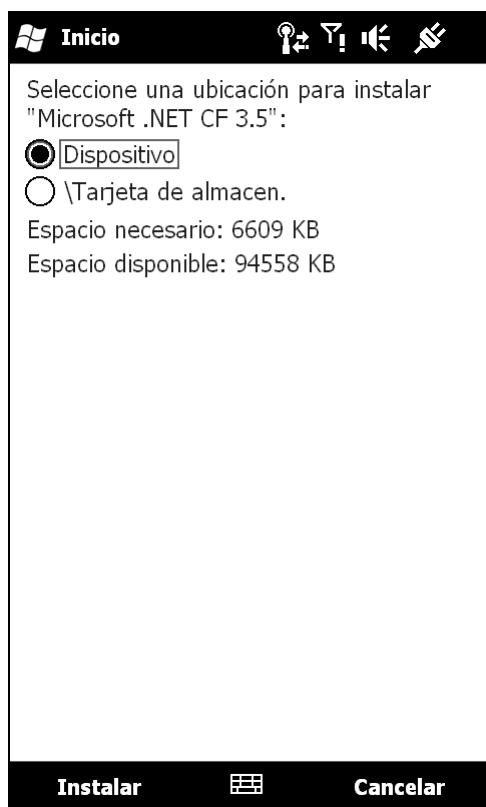
836. Las versiones de .NET Compact Framework son [Ref.- 98]:

- v2.0 - 2.0.5238.00
- v2.0 SP1 - 2.0.6129.00
- v2.0 SP2 - 2.0.7045.00
- v3.5 - 3.5.7283.0

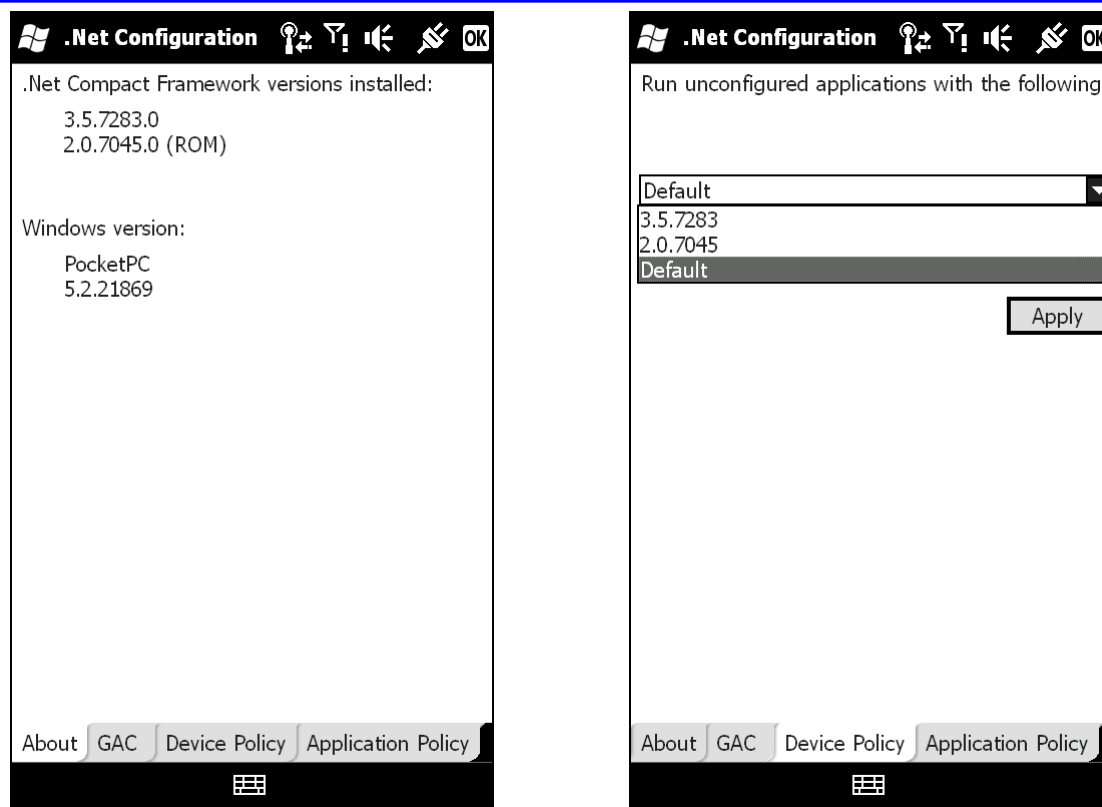
837. Se recomienda actualizar manualmente a la versión del Service Pack 1 ó 2 de .NET 2.0 [Ref.- 95] [Ref.- 96], o mejor aún, a la versión 3.5 (Redistributable) de .NET Compact Framework (con soporte para .NET 1.0, 2.0 y 3.5) [Ref.- 97].

838. Tras la instalación del fichero .MSI correspondiente a .NET Compact Framework versión 3.5 en un ordenador, junto a la opción de “Deployment”, para su instalación en dispositivos móviles que se conecten a éste mediante ActiveSync (imagen inferior izquierda), es posible verificar la disponibilidad de la nueva versión a través del registro, pese a que la versión por defecto sigue siendo la 2.0 SP2:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\ .NETCompactFramework]
"2.0.7045.00"=dword:00000001
"3.5.7283.00"=dword:00000000
```



839. Mediante la ejecución del binario “\Windows\cgacutil.exe” (imagen superior derecha) es posible ver las versiones de .NET Compact Framework disponibles en el dispositivo móvil, pero sin indicación de la versión activa por defecto.
840. Es posible fijar la versión 3.5 como versión .NET por defecto modificando los valores de las versiones en el registro, y asignando el valor “1” al parámetro “3.5.7283.00” y el valor “0” al parámetro “2.0.7045.00”.
841. También es posible seleccionar la versión de .NET empleada por defecto a través de la utilidad “NetCFcfg.exe” del paquete “Microsoft's Power Toys for .NET Compact Framework” [Ref.- 99]. Tras su instalación en un ordenador, debe copiarse el fichero “C:\Program Files\Microsoft.NET\SDK\CompactFramework\v3.5\WindowsCE\wce500\armv4i\NetCFcfg.exe” en el dispositivo móvil mediante ActiveSync.
842. Su ejecución permite verificar las versiones .NET instaladas, la versión .NET por defecto (pestaña “Device Policy”; aunque para fijar la versión no modifica la clave del registro previamente mencionada) y las excepciones para aplicaciones particulares:

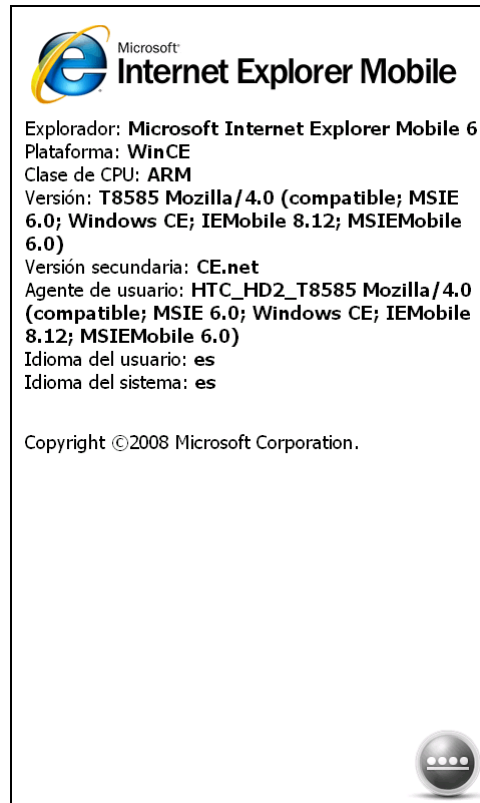


5.29 NAVEGACIÓN WEB: INTERNET EXPLORER MOBILE

843. Una de las tareas más comunes realizadas desde los dispositivos móviles es la de navegación web por Internet. Windows Mobile 6.5 incluye por defecto el navegador web Internet Explorer Mobile 6.

Nota: algunos fabricantes de dispositivos móviles incluyen otros navegadores web por defecto. Por ejemplo, HTC incluye el navegador web Opera en sus terminales. En concreto, el dispositivo móvil empleado en la elaboración de la presente guía disponía de Opera versión 9.7 (compilación 35627) para Windows Mobile (“opera:about”). El análisis detallado de seguridad del navegador web Opera está fuera del alcance de la presente guía.

844. Todos los detalles de la versión de Internet Explorer Mobile disponible, en este caso la versión 6 (conocida como MSIEMobile 6.0 ó IEMobile 8.12), pueden ser obtenidos navegando desde la aplicación a la URL “about:versión”:



845. Internet Explorer Mobile soporta autenticación HTTP “Basic” y NTLM, definidas en el registro: “HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Security”. Se recomienda hacer uso de autenticación NTLM siempre que sea posible (opción que viene determinada por el servidor web), ya que la autenticación HTTP “Basic” revela las credenciales de acceso sin cifrar en el tráfico de red intercambiado entre cliente y servidor, especialmente al no emplearse HTTPS.
846. Para una navegación web más segura, se recomienda deshabilitar los controles ActiveX en el navegador web con el objetivo de mitigar los ataques asociados a vulnerabilidades en componentes ActiveX. Esta configuración podría dificultar la visualización de páginas web que hacen uso de esta tecnología.
847. La opción está disponible a través del menú de configuración de Internet Explorer Mobile, opción “Ver – Habilitar controles ActiveX” (habilitados por defecto):



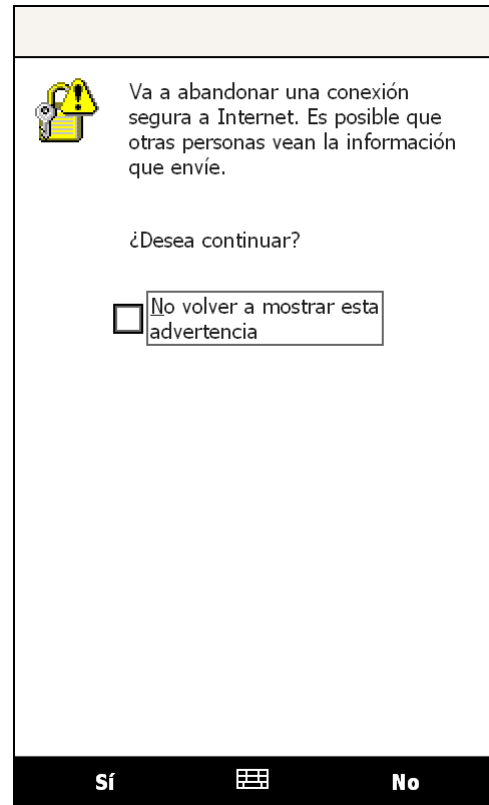
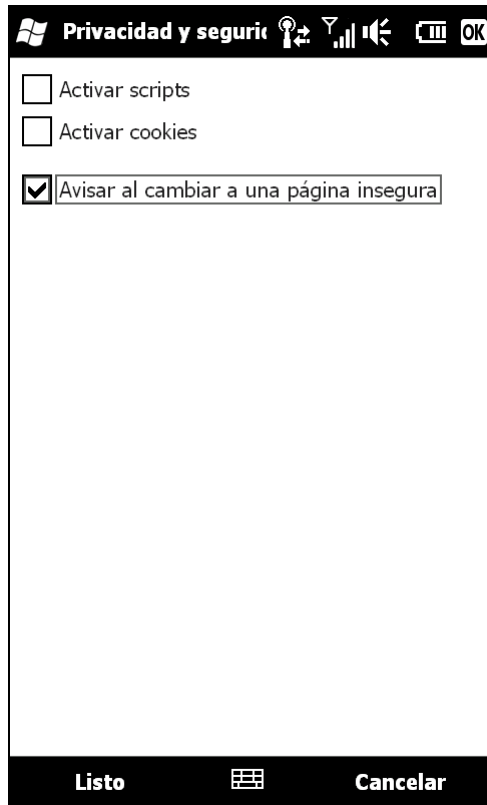
848. La siguiente clave del registro permite deshabilitar los controles ActiveX (sin valor por defecto, indicando que se permite ActiveX):

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]  
"Disable ActiveX"=dword:00000001
```

Nota: es posible habilitar que se muestre una ventana de aviso cada vez que un control ActiveX es cargado mediante el siguiente parámetro del registro (que por defecto no está habilitado):

```
"BlockStaticActiveX"=dword:00000001
```

849. Para una navegación web más segura, se recomienda deshabilitar la ejecución de scripts (Microsoft Jscript) y el uso de cookies en el navegador web con el objetivo de mitigar los ataques asociados a la ejecución de scripts maliciosos en el navegador y a la privacidad del usuario a través de las cookies. Esta configuración podría dificultar la visualización de páginas web que utilizan scripts y cookies en sus contenidos web y para su funcionamiento (la mayoría de páginas web en Internet).
850. Ambas opciones están disponibles a través del menú de configuración de Internet Explorer Mobile, opción “Herramientas – Opciones – Privacidad y seguridad”, junto al aviso al cambiar de una página cifrada (HTTPS) a una no cifrada (HTTP) (imagen inferior izquierda). Las tres opciones están habilitadas por defecto:



851. Se recomienda dejar habilitados los avisos de transición de una página cifrada (HTTPS) a una no cifrada (HTTP), para advertir al usuario del riesgo de que la información intercambiada con el servidor web se envíe sin cifrar (imagen superior derecha).
852. Las siguientes claves del registro permiten gestionar los tres parámetros, asociadas a la zona de Internet en Internet Explorer ("3"). El parámetro "1400" define la activación de scripts, con valor "3" si no están activos, valor "1" si se desea preguntar al usuario (no configurable desde el interfaz de usuario) y valor "0" si se permite su ejecución. Los parámetros "1a02-1a10" definen si se permite el uso de cookies, con los mismos valores [Ref.- 83]. El parámetro "WarnOnZoneCrossing" define si se habilitan los avisos desde HTTP a HTTPS (valor "1"; o valor "0" en caso contrario):

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3]
"1400"=dword:00000003

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3]
"1a02"=dword:00000003      # cookies persistentes
"1a03"=dword:00000003      # cookies de sesión
"1a05"=dword:00000003      # cookies persistentes de terceros
"1a06"=dword:00000003      # cookies de sesión de terceros
"1a10"=dword:00000003      # privacidad: bloquear todas las cookies

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings]
"WarnOnZoneCrossing"=dword:00000001
```

Nota: se recomienda consultar en detalle las guías CCN-CERT de seguridad para aplicaciones cliente en entornos Windows, dónde se detalla en profundidad la configuración

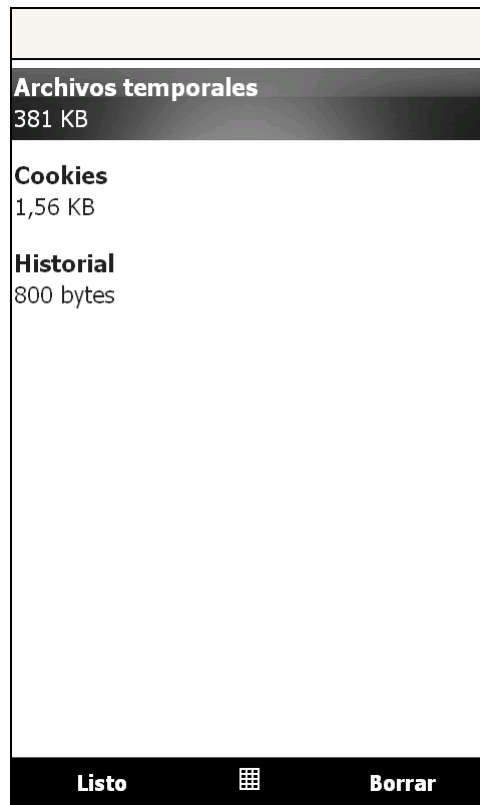
de seguridad del navegador web Internet Explorer: CCN-STIC-502, CCN-STIC-502B y CCN-STIC-519A [Ref.- 85].

853. Adicionalmente, las siguientes claves del registro especifican si ActiveX y scripting (JScript) están habilitados o no (con valor “1” por defecto, activos). La desactivación global de ActiveX puede afectar a la lectura de correos electrónicos en Outlook Mobile:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
"Security_RunActiveXControls"=dword:00000000
"Security_RunScripts"=dword:00000000
```

854. Se recomienda borrar de forma frecuente el historial de navegación de Internet Explorer Mobile, que incluye los archivos temporales, las cookies y las referencias a los sitios web visitados previamente (historial), con el objetivo de proteger la privacidad del usuario.

855. Cada uno de estos elementos puede ser eliminado individualmente mediante el botón “Borrar” desde el menú de configuración de Internet Explorer Mobile, opción “Herramientas – Opciones – Historial de navegación”:



856. Los parámetros de configuración, y las carpetas dónde se ubican cada uno de estos tres elementos (“Cache”, “Cookies” y “History”), se definen en las dos siguientes claves del registro, respectivamente:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache
```

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
```

5.29.1 PROVEEDOR DE BÚSQUEDAS AUTOMÁTICO

857. Cuando se introduce un término en la barra de navegación de Internet Explorer Mobile, si éste no corresponde con un servidor web, de forma automática se realiza una búsqueda de dicho término a través del buscador de Microsoft Bing.
858. Este comportamiento tiene implicaciones de seguridad relevantes al revelar en Internet la información introducida en la barra de navegación, como el nombre de servidores internos (ver apartado “5.21.2.1. Wi-Fi: perfil de conexión Internet o Trabajo”).
859. La siguiente clave del registro determina el proveedor de búsqueda predeterminado en Internet Explorer Mobile, empleado para las búsquedas automáticas:

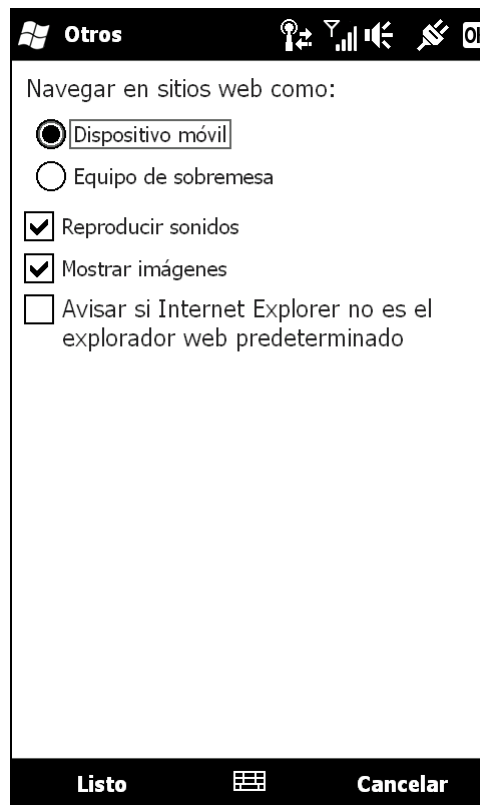
```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
"AutoSearchProvider"="http://m.live.com/Search/Results.aspx?mid=8002&lc=es&q="
```

860. Se recomienda eliminar la disponibilidad de un proveedor de búsqueda, con el objetivo de mitigar la revelación de la información introducida en la barra de navegación. Para ello simplemente debe eliminarse el valor del parámetro “AutoSearchProvider”:

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
"AutoSearchProvider"=""
```

5.29.2 IDENTIFICACIÓN DEL NAVEGADOR WEB

861. Internet Explorer Mobile permite la navegación web en Internet como si fuera un equipo de escritorio o un dispositivo móvil. Ambas opciones están disponibles a través del menú de configuración de Internet Explorer Mobile, opción “Herramientas – Opciones – Otros – Navegar en sitios web como: Dispositivo móvil o Equipo de sobremesa” (también configurable desde la opción “Ver”):



862. La siguiente clave del registro determina si se actúa como equipo de sobremesa (valor “1”, empleado por defecto) o dispositivo móvil (valor “0”):

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
"User Agent"=dword:00000001
```

863. Cuando Internet Explorer Mobile actúa como dispositivo móvil, la cadena de caracteres que identifica al navegador web o agente de usuario (User-Agent) tiene el siguiente valor, revelando excesivos detalles sobre la versión del navegador web y la plataforma:

```
User-Agent: HTC_HD2_T8585 Mozilla/4.0 (compatible; MSIE 6.0; Windows CE; IEMobile 8.12; MSIEMobile 6.0)
```

864. Cuando se actúa como equipo de sobremesa, el User-Agent tiene el siguiente valor, simulando a un equipo con Windows XP con IE6 (“MSIE 6.0; Windows NT 5.1;”), aunque revela detalles del tipo de dispositivo móvil y la plataforma Windows Mobile 6.5:

```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; HTC_HD2_T8585; Windows Phone 6.5)
```

865. La identificación del navegador web Internet Explorer Mobile en Windows Mobile 6.5, a través de la cabecera HTTP “User-Agent”, está definida por las siguientes claves del registro, empleadas para la versión de escritorio:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent]
"Template"="Same as Windows XP"
"Platform"="Windows CE"
"Version"="MSIE 6.0"
"Compatible"="compatible"
@="Mozilla/4.0"
```

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Templates\Same as Windows XP]
"Platform"="Windows NT 5.1"
"Version"="MSIE 6.0"
"Compatible"="compatible"
@="Mozilla/4.0"
```

866. El parámetro “Template” especifica la plantilla a utilizar: “Same as Windows XP”. Los valores de la plantilla sustituyen a los valores por defecto. Windows Mobile 6.5 también incluye una plantilla en el registro que permite emular a “Pocket PC” (MSIE 4.01).

867. La identificación del navegador web Internet Explorer Mobile en Windows Mobile 6.5, a través de la cabecera HTTP “User-Agent”, está definida por la siguiente clave del registro, empleada al actuar como dispositivo móvil:

```
[HKEY_LOCAL_MACHINE\Security\Internet Explorer\User Agent]
"CustomBase"="HTC_HD2_T8585 Mozilla/4.0"
```

Nota: cuando Internet Explorer Mobile 6 actúa como dispositivo móvil el User-Agent incluye detalles de versiones, “IEMobile 8.12; MSIEMobile 6.0”. No se ha identificado ningún parámetro del registro que permita ocultar esta información.

868. Se recomienda modificar el valor del User-Agent para que no desvele información adicional, al menos, al actuar como equipo de sobremesa. Si se eliminan los dos siguientes parámetros del registro (disponibles por defecto), al actuar como equipo de sobremesa se emularía a un ordenador con Windows XP con IE6 (“User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)”):

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\User Agent\Templates\Same as Windows XP\Post Platform]
"HTC_HD2_T8585"=""
"Windows Phone 6.5"=""
```

Nota: la modificación o eliminación de información de las cabeceras HTTP puede afectar a la funcionalidad de servidores y aplicaciones web que hacen uso de dichos datos para procesar y mostrar contenidos web personalizados para el tipo de dispositivo cliente. Estas implicaciones se han mencionado igualmente a lo largo de la presente sección al deshabilitar otras funcionalidades del navegador web.

Las recomendaciones de seguridad descritas a lo largo de toda la sección pretenden incrementar el nivel de seguridad y privacidad del dispositivo móvil y de su usuario, pudiendo afectar por tanto a la funcionalidad, por lo que deben ser aplicadas únicamente si no es necesario hacer uso de la funcionalidad asociada.

869. Adicionalmente al User-Agent, Internet Explorer Mobile incluye en ambos casos otras cabeceras HTTP en sus peticiones que revelan la utilización de un dispositivo móvil para la navegación web basado en Windows Mobile 6.5 [Ref.- 86]:

```
UA-OS: Windows CE (Pocket PC) - Version 5.2
UA-color: color16
UA-pixels: 480x800
UA-Voice: TRUE
UA-CPU: ARM
```

870. Mediante el análisis de las cabeceras HTTP, en concreto la cabecera “UA-OS” y la cabecera HTTP “UA-Voice”, para saber si el dispositivo móvil dispone de capacidades de telefonía (capacidad “CanInitiateVoiceCall”), un potencial atacante puede determinar la versión de Windows Mobile 6.x empleada (*Professional*, *Classic* o *Standard*) [Ref.- 88], información relevante para llevar a cabo ataques dirigidos contra una versión concreta de Windows Mobile.

Nota: no se ha identificado ningún parámetro del registro que permita ocultar las cabeceras “UA-*”, por lo que esta información siempre desvela la existencia de un dispositivo móvil y su versión de forma detallada.

871. En el caso de actuar como dispositivo móvil, el navegador web también añade la siguiente cabecera WAP que permite identificar el tipo de terminal (fabricante y modelo):

```
x-wap-profile: "http://www.htcmms.com.tw/gen/HTC_HD2_T8585-1.0.xml"
```

872. El UAProf (*User-Agent Profile*) [Ref.- 84] es un documento XML que contiene información sobre las características y capacidades de un dispositivo móvil, estándar definido por OMA, *Open Mobile Alliance*. El documento está especificado en la cabecera HTTP “x-wap-profile” (o “Profile”), apuntando normalmente a una web del fabricante del terminal (repositorio de perfiles).

873. El perfil contiene información muy detallada del dispositivo móvil, incluyendo los perfiles Bluetooth, los tipos y formatos de datos soportados, protocolos de seguridad y de transferencia de datos soportados, capacidades *push*, WAP, MMS y de *streaming*.

874. Este perfil WAP está definido en la siguiente clave del registro para Internet Explorer Mobile (en otras claves para otros clientes y aplicaciones web). Se recomienda deshabilitar su envío en las cabeceras HTTP, para lo que es necesario eliminar el parámetro “UAProf” del registro:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
"UAProf"="http://www.htcmms.com.tw/gen/HTC_HD2_T8585-1.0.xml"
```

875. Se recomienda modificar el valor del User-Agent para evitar proporcionar información detallada sobre el dispositivo móvil a todos los servidores web accedidos mediante Internet Explorer Mobile y a un potencial atacante que capture el tráfico web no cifrado generado por el dispositivo móvil.

876. Se recomienda evaluar si habitualmente se desea realizar la navegación web como equipo de sobremesa (opción recomendada), más expuesto a ataques genéricos sobre todas las versiones del navegador Internet Explorer pero que probablemente no tengan éxito en el dispositivo móvil, o como dispositivo móvil, más expuesto a ataques dirigidos a este tipo de terminales y con posibilidad mayor de éxito.

877. Debe tenerse en cuenta que la modificación del User-Agent, y especialmente el parámetro “Platform”, podría afectar a la presentación de los contenidos web de ciertos servidores y aplicaciones que personalizan las respuestas en función de si el cliente es un dispositivo móvil o un ordenador (de sobremesa o portátil).

Nota: el agente de usuario, o User-Agent, de otros clientes y aplicaciones disponibles en Windows Mobile 6.5, y en concreto en dispositivos móviles HTC, es:

- Información meteorológica (Clima), servicio de ubicación de HTC e información bursátil:

User-Agent: HTC HTTP Service

- Google Location:

User-Agent: WINM-TEST-USER-AGENT

- QuickGPS:

User-Agent: Ephemeris_Download

- Actualización BD operadores:

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows CE)

5.29.3 CONTENIDOS ADOBE FLASH

878. Windows Mobile 6.5 dispone de un complemento o *plugin* para la visualización de contenidos Flash, denominado Adobe Flash Lite (AFL), y vinculado al navegador web Internet Explorer Mobile 6.

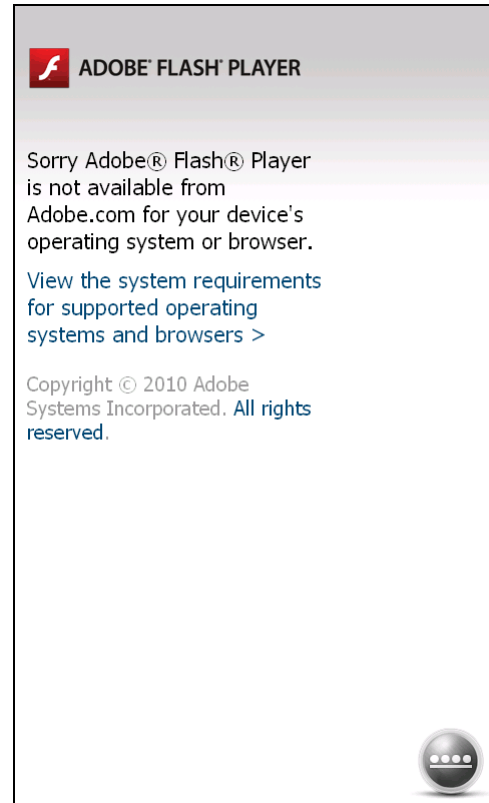
879. Este *plugin* es opcional y puede ser proporcionado por el fabricante del dispositivo móvil (integrado en su versión de firmware) [Ref.- 91], como en el caso del empleado para la elaboración de la presente guía, y es compatible con contenidos para Flash Player 8 o anterior y soporta ActionScript 2.0 (no la versión 3.0) [Ref.- 87].

880. La disponibilidad de Flash Lite, o capacidades de reproducción Flash, pueden verificarse accediendo a la siguiente página desde el navegador web:

<http://www.adobe.com/mena/products/flashlite/>

881. Las recomendaciones de seguridad asociadas a las aplicaciones web basadas en Flash, así como las medidas de seguridad propias de Flash Player 8 y de su modelo de seguridad aplican también a Flash Lite [Ref.- 89].

882. Debe tenerse en cuenta que las mejoras de seguridad incorporadas en las últimas versiones de Flash Player para los equipos de escritorio, por ejemplo en la versión 10.1, no están disponibles en Flash Lite.
883. Se recomienda actualizar Flash Lite a la última versión de Flash Player, por ejemplo 10.1, desde “<http://m.flash.com>” cuando esté disponible para Windows Mobile [Ref.- 90], con el objetivo de eliminar las vulnerabilidades de seguridad conocidas:



884. La versión de Flash instalada se puede obtener de la siguiente clave del registro. En el caso del dispositivo móvil empleado para la elaboración de la presente guía es la 1.0.1920.1622 (OEM), asociada al fichero “\Windows\FLPlayer.exe”:

```
[HKEY_LOCAL_MACHINE\Software\OEM\MASD]
"FlashLiteShareDLL"="1_0_19201927_0"
```

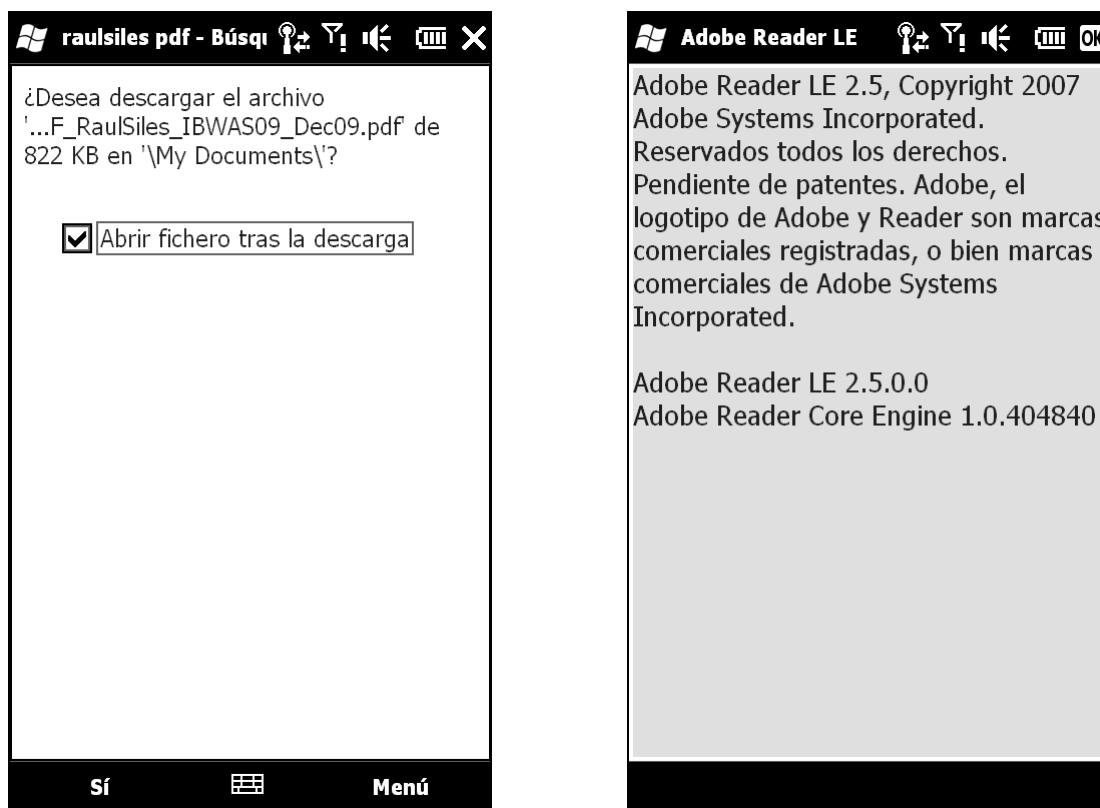
Nota: no se ha identificado ningún método para desinstalar Flash Lite en Windows Mobile 6.5. El fichero “\Windows\FLPlayer.exe” no puede ser modificado o eliminado al encontrarse ubicado en la ROM (firmware) del dispositivo móvil.

La solución para bloquear la reproducción de contenidos Flash en el navegador web (no afectando al cliente independiente de YouTube) pasa por reducir a cero en el registro la memoria utilizada por el *plugin* Flash Lite. Los valores por defecto para estos dos parámetros son 32 (MB) y 128 (KB) respectivamente:

```
[HKEY_LOCAL_MACHINE\Software\Adobe\FlashLite ActiveX\Memory Settings]
"Dynamic Memory(in MB)"=dword:00000000
"Static Memory(in KB)"=dword:00000000
```

5.29.4 CONTENIDOS ADOBE PDF

885. Windows Mobile 6.5 puede disponer de un cliente para la visualización de contenidos en formato PDF, por ejemplo Adobe Reader LE (versión 2.5) en el caso del dispositivo móvil para la elaboración de la presente guía (proporcionado por el fabricante del terminal en su versión de firmware).
886. Al acceder a contenidos PDF desde el navegador web Internet Explorer Mobile 6, éste consultará al usuario si desea almacenar el fichero PDF, por defecto en “\My Documents\”, y si quiere abrirlo automáticamente tras la descarga:

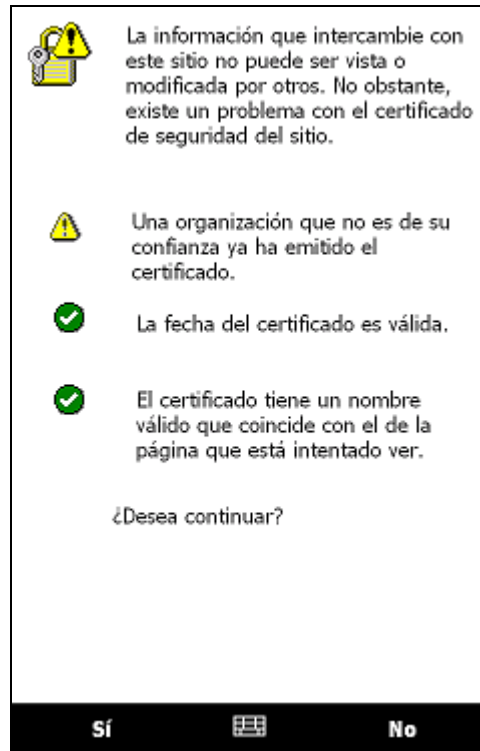


887. El visor de ficheros PDF está disponible desde el menú “Inicio – Herramientas (Herram.) – Adobe Reader LE” (información de versión detallada en la imagen superior derecha).
888. Debido a las numerosas vulnerabilidades de seguridad en las aplicaciones cliente de visualización de ficheros PDF (Adobe Acrobat, Adobe Reader, Foxit, etc) durante los últimos años, se recomienda mantener actualizada la aplicación de visualización de ficheros PDF a la última versión [Ref.- 92].

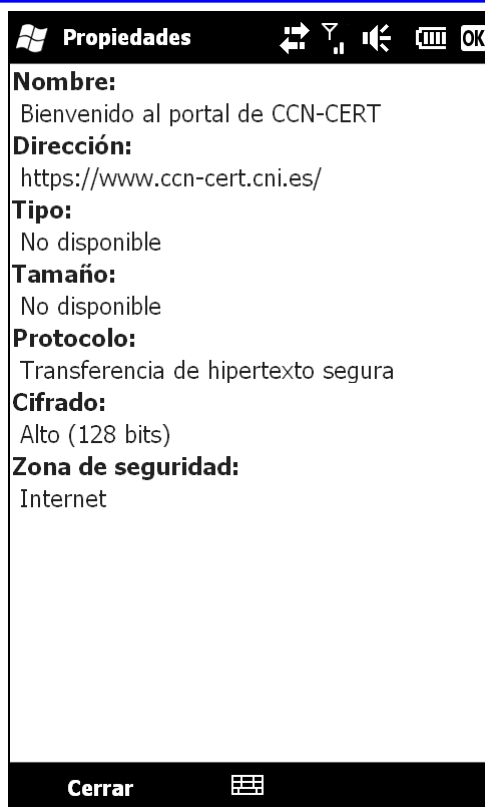
5.29.5 SSL/TLS

889. Windows Mobile 6.5, y por tanto Internet Explorer Mobile, dispone de soporte para SSL/TLS y el establecimiento de sesiones web HTTPS cifradas (ver apartado “5.21.5. SSL/TLS”).
890. Al acceder a un servidor web mediante HTTPS que emplea un certificado digital emitido por una autoridad certificadora (CA) no reconocida por Windows Mobile (ver apartado “5.5. Modelo de seguridad de Windows Mobile”), se genera un mensaje de error indicando que no es posible verificar la validez del certificado digital. El mensaje especifica si el problema con el certificado digital está asociado a la imposibilidad de

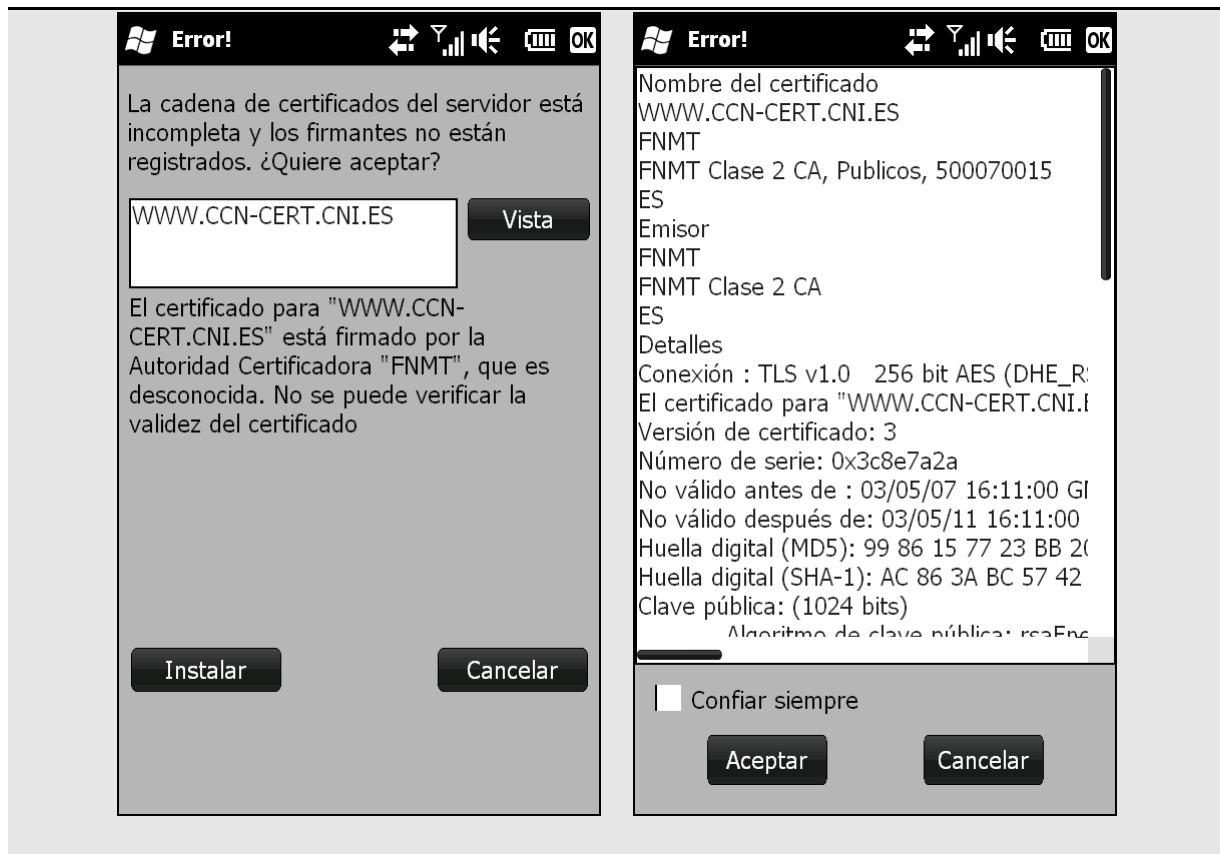
verificar quién ha emitido el certificado (ejemplo inferior), si éste ha expirado, o si está asociado a otra entidad o servidor web:



891. Como puede apreciarse en la imagen superior, Internet Explorer Mobile no ofrece ninguna opción para visualizar los detalles del certificado digital y poder así determinar el motivo que ha generado el error y la autenticidad del certificado digital. El usuario puede únicamente aceptar o denegar el mismo, permitiendo así (o no) la conexión con el servidor web.
892. Dado que el usuario está interesado en conectar con el servidor web, en la mayoría de los casos pulsará el botón “Sí”, aceptando el certificado y estableciendo la conexión con el servidor web. Esta acción tiene el riesgo asociado de que el certificado digital aceptado, y desconocido, pertenezca a un potencial intruso que se encuentra realizando un ataque de interceptación, MitM (*Man-in-the-Middle*), sobre el protocolo SSL/TLS y las comunicaciones (supuestamente) cifradas del usuario.
893. Una vez la conexión ha sido establecida, tampoco es posible verificar los detalles del certificado digital. A través del menú de configuración de Internet Explorer Mobile, opción “Herramientas – Propiedades” se puede acceder a las propiedades de la página web actual, que sólo indican que se está empleando el protocolo de “transferencia de hipertexto segura” y un cifrado clasificado como “alto” (128 bits):



Nota: la implementación de la verificación de certificados digitales en otros navegadores web, como por ejemplo Opera (incluido por defecto en dispositivos móviles HTC y mencionado previamente), sí permite analizar los detalles del certificado, por lo que representa una opción más adecuada para la navegación web en Windows Mobile 6.5 desde el punto de vista de seguridad:



894. Internet Explorer Mobile permite hacer uso de mecanismos de autenticación web basados en certificados cliente, para lo que es necesario importar un certificado digital personal (normalmente en formato PKCS12) en el dispositivo móvil (al igual que para la conexión a redes Wi-Fi basadas en EAP-TLS, o redes VPN basadas en IPSec/L2TP y certificados).

5.30 CORREO ELECTRÓNICO (E-MAIL)

895. Windows Mobile 6.5 proporciona capacidades para la lectura de correos electrónicos (e-mails) desde el dispositivo móvil, disponibles a través del icono “E-mail” del menú “Inicio”, desde dónde es posible configurar una o varias cuentas de correo electrónico.

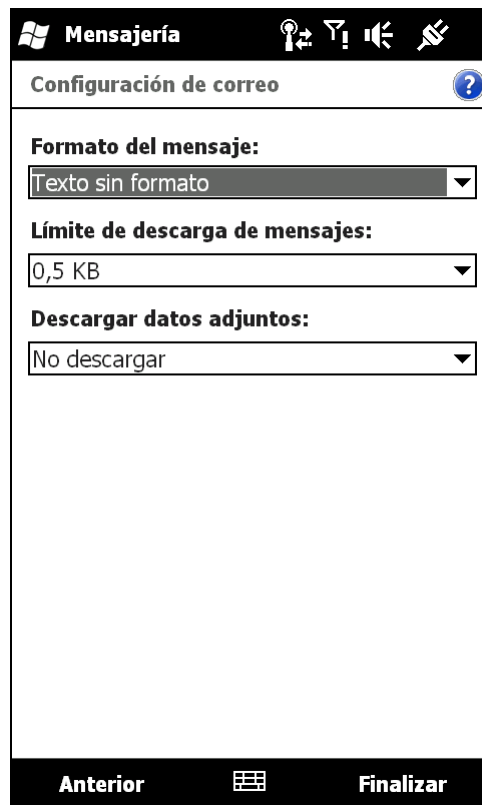
896. La configuración de una nueva cuenta de correo electrónico dispone de la opción “Guardar contraseña” habilitada por defecto.

897. Desde el punto de vista de seguridad, se recomienda no almacenar la contraseña en el dispositivo móvil, mitigando así el riesgo de que un potencial atacante obtenga acceso al dispositivo móvil, y como consecuencia, a todas las cuentas de correo electrónico configuradas en el mismo. Esta configuración más segura tiene un impacto directo en la funcionalidad, ya que requiere que el usuario introduzca la contraseña cada vez que se conecte al servicio.

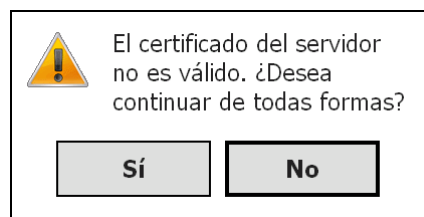
Nota: durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía (activado automáticamente la primera vez que se enciende el terminal), si se dispone de conectividad (por ejemplo, vía Wi-Fi) se ofrece la posibilidad de configurar cuentas de correo electrónico de Outlook, Gmail (@gmail.com), AOL Mail (@aol.com) u otras (cuenta de e-mail genérica).

La configuración de una nueva cuenta de correo electrónico, para todos los proveedores disponibles por defecto, dispone de la opción “Guardar contraseña” habilitada por defecto.

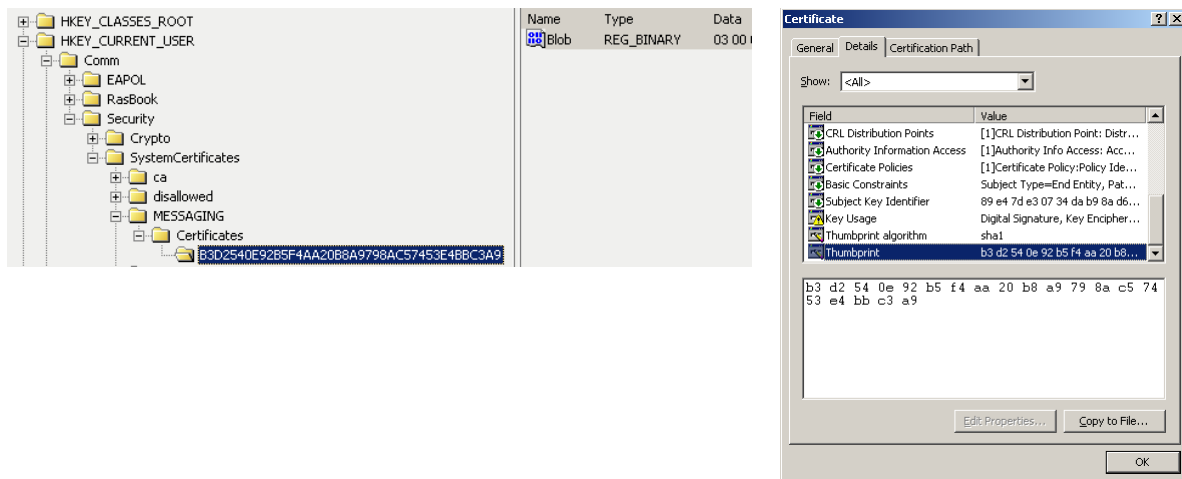
898. Durante el proceso de configuración de una nueva cuenta de correo electrónico (para Gmail, no así para AOL), la opción del formato de los mensajes por defecto es “HTML”. Se recomienda modificar el formato de los mensajes a “Texto sin formato”, con el objetivo de evitar ataques asociados a la manipulación del contenido HTML de los mensajes, por ejemplo, en ataques de *phishing*. Adicionalmente, por defecto, los ficheros adjuntos de los mensajes no serán descargados (opción recomendada desde el punto de vista de seguridad):



899. La plantilla de configuración para las cuentas de correo electrónico de los proveedores disponibles por defecto, como por ejemplo Gmail, hace uso de IMAPS (basado en SSL/TLS, TCP/993) al establecer la conexión con el servidor “imap.gmail.com”. El mismo escenario se presenta con las cuentas de AOL y el servidor “imap.aol.com”.
900. En caso de que el certificado digital empleado por el servidor IMAPS para establecer la sesión SSL no pueda ser verificado por el dispositivo móvil se generará un mensaje de error, pero no será posible obtener detalles del certificado para su validación manual:



901. Se recomienda emplear medios externos al dispositivo móvil para validar el certificado digital del servidor IMAPS y obtener los posibles detalles del error (como por ejemplo la ausencia del certificado raíz de la autoridad certificadora que emitió el certificado en Windows Mobile 6.5), y en ningún caso continuar con la comunicación, ya que el tráfico está expuesto a una posible interceptación y manipulación por un potencial atacante.
902. En caso de responder con “Si” al mensaje de validez del certificado, éste es almacenado en el registro como un certificado válido, por lo que el mensaje de aviso no volverá a ser mostrado (salvo que se elimine manualmente del registro y se reinicie el dispositivo móvil) y se establecerá siempre la conexión SSL/TLS con ese certificado sin validar, exponiendo todo el tráfico a un potencial atacante.
903. El certificado es almacenado en el registro con un nombre de clave igual al “Thumbprint” (o firma) del certificado digital y con un parámetro “Blob” de tipo binario, bajo “HKEY_CURRENT_USER\Comm\Security\SystemCertificates\MESSAGING\Certificates”:



Nota: el error del certificado digital anterior corresponde al servidor IMAPS de AOL. Este servidor dispone de un certificado emitido por una CA intermedia, “AOL Member CA”, cuya CA raíz es “America Online Root Certification Authority 1”. El certificado digital problemático, junto a todos sus detalles, puede ser obtenido mediante el comando [Ref.- 100]:

```
$ openssl s_client -connect imap.aol.com:993
```

Dado que los certificados de estas CA’s no están disponibles en Windows Mobile 6.5 por defecto, es necesario obtenerlos desde “https://pki-info.aol.com/AOL/” y “https://pki-info.aol.com/AOLMSPKI/” respectivamente, verificar los identificadores de los certificados digitales [Ref.- 100], e instalarlos en el dispositivo móvil (simplemente pulsando sobre los ficheros tras renombrarlos de .DER a .CER).

En el caso de Gmail el certificado digital ha sido emitido por “Equifax Secure Certificate Authority”, CA disponible por defecto en Windows Mobile 6.5, por lo que puede ser validado correctamente por el dispositivo móvil.

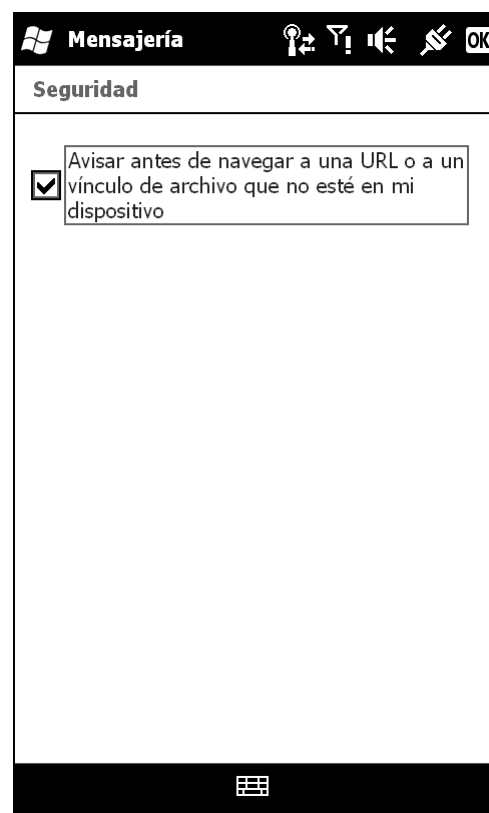
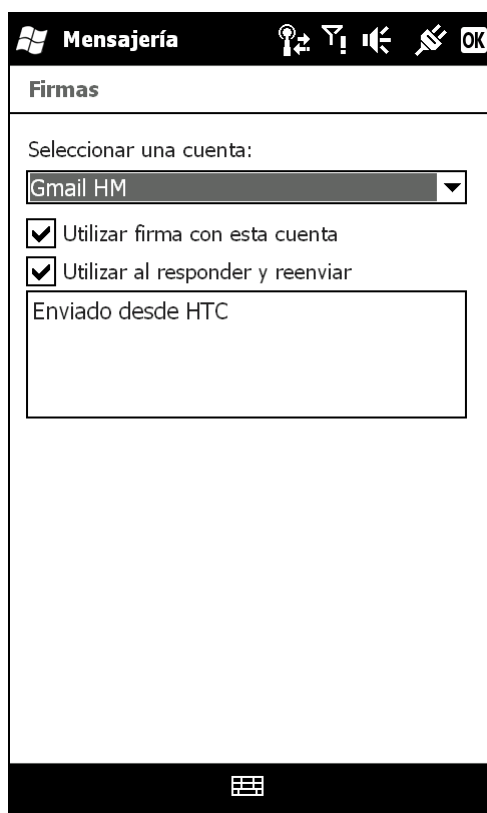
904. Por defecto, al escribir un nuevo mensaje el dispositivo móvil añade una firma indicando desde dónde se realiza el envío, como por ejemplo “Enviado desde HTC”. Se recomienda

eliminar dicha firma existente por defecto para no revelar información del fabricante o tipo de dispositivo móvil.

905. La gestión de las firmas se puede realizar desde el menú “Inicio – E-mail”, botón “Menú”, y la opción “Opciones”. Desde la pestaña “Cuentas” y el botón “Firmas...” es posible modificar la firma para cada una de las cuentas disponibles, incluyendo si se usará o no una firma, y si será empleada tanto al enviar nuevos correos (siempre en el caso de usarse) como en las respuestas y reenvíos (imagen inferior izquierda).

906. La siguiente clave del registro permite configurar el mensaje empleado por defecto como plantilla para la firma al crear una nueva cuenta de correo. Posteriormente las firmas se pueden gestionar individualmente para cada cuenta:

```
[HKEY_LOCAL_MACHINE\Software\HTC\Signature]
"Name"="Enviado desde HTC"
```



907. El dispositivo móvil puede generar un mensaje de aviso antes de navegar a un recurso externo, recomendado desde el punto de vista de seguridad (y activo por defecto). Esta funcionalidad está disponible desde el menú “Inicio – E-mail”, botón “Menú”, y la opción “Opciones”. Desde la pestaña “Cuentas” y el botón “Seguridad...” (imagen superior derecha).

908. La siguiente clave del registro permite configurar y habilitar esta opción de aviso:

```
[HKEY_LOCAL_MACHINE\System\Inbox\Settings]
"ShowUrlConfSecurityDialog"=dword:00000001
```

5.30.1 DIRECT PUSH

909. La tecnología *Direct Push* [Ref.- 101] permite sincronizar los datos de un dispositivo móvil basado en Windows Mobile (desde la versión 5.0 con MSFP, *Messaging and*

- Security Feature Pack*) con Microsoft Exchange, y en concreto con Exchange ActiveSync (disponible desde Microsoft Exchange Server 2003 Service Pack 2), no siendo necesario el uso de mensajes SMS para la sincronización (como en el pasado).
910. Mediante direct push el dispositivo móvil mantiene una sesión activa a través de un canal HTTP con el servidor Microsoft Exchange. Las actualizaciones que tienen lugar en el servidor son enviadas automáticamente e inmediatamente al dispositivo móvil, como por ejemplo los correos electrónicos, aunque también puede ser empleado para la distribución de políticas de seguridad.
911. Se recomienda que el canal de comunicación HTTP empleado por direct push esté cifrado mediante SSL/TLS (HTTPS), ya que en caso contrario las credenciales del usuario serán enviadas en claro por la red [Ref.- 102].
912. Dado que la tecnología direct push ajusta dinámicamente el tiempo de conexión para optimizar el consumo de batería en el dispositivo móvil y minimizar el consumo de ancho de banda [Ref.- 80], se recomienda configurar los cortafuegos existentes en la red (de la organización o del operador de telefonía móvil) para permitir sesiones HTTP (TCP) sin actividad durante al menos 30 minutos [Ref.- 101].
913. La configuración de direct push en el dispositivo móvil está disponible a través del menú “Inicio – Configuración – Controles inalámbricos” (que proporciona acceso al “Comm Manager”), mediante la sección “Microsoft Direct Push”.
914. Direct push puede ser desactivado en Windows Mobile 6.5 a través del botón deslizante de activación y desactivación asociado a la sección “Microsoft Direct Push” del “Comm Manager”.
915. Para su utilización es necesario proporcionar las credenciales de acceso a Microsoft Exchange, mediante dirección de correo electrónico y contraseña, así como el dominio, la dirección del servidor y si requiere conexiones cifradas mediante SSL (opción recomendada). Posteriormente se definirán los elementos a sincronizar (correo electrónico, contactos, calendario y/o tareas) y si la sincronización de datos debe realizarse automáticamente:

The screenshot shows the 'Config. correo' (Configure Mail) screen in Windows Mobile 6.5. The screen has a title bar with the Windows logo and the text 'Config. correo'. Below the title bar, there are several icons: a key, a signal strength indicator, a volume icon, a battery icon, and a close button. The main content area contains the following fields and options:

- Nombre de usuario:** A text box containing 'usuario@taddong.com'.
- Contraseña:** A text box containing a series of asterisks '*****'.
- Dominio:** A text box containing 'taddong'.
- Guardar contraseña (requerido para sincronización automática):** A checkbox that is checked, with a green checkmark icon to its left.
- Dirección del servidor:** A text box containing 'exchange.taddong.com'.
- Este servidor requiere una conexión cifrada (SSL):** A checkbox that is checked, with a green checkmark icon to its left.

At the bottom of the screen, there are three buttons: 'Atrás' (Back), a keyboard icon, and 'Siguiente' (Next).

916. Por defecto, la opción “Guardar contraseña” está habilitada, con las implicaciones de seguridad mencionadas previamente que esto conlleva, aunque en el caso de direct push es un requisito necesario para hacer uso de los mecanismos de sincronización automática.

Nota: Windows Mobile 6.x (desde la versión 5.x [Ref.- 76]) dispone de capacidades para cifrar y firmar correos electrónicos mediante S/MIME [Ref.- 103]. Los detalles de implementación y configuración de S/MIME en Windows Mobile 6.5, y su integración con Microsoft Exchange y el directorio activo de Windows, están fuera del alcance de la presente guía.

5.31 REDES SOCIALES

917. Windows Mobile 6.5 incluye por defecto las siguientes aplicaciones cliente para el acceso a redes sociales en Internet, disponibles en función del fabricante u operador de telefonía móvil del dispositivo móvil:

- Facebook para Windows Mobile
- HTC Peep (cliente Twitter)
- YouTube
- Windows Live

Nota: otros dispositivos móviles basados en Windows Mobile 6.5 incluyen adicionalmente capacidades de acceso a MySpace mediante el cliente MySpace Mobile.

Nota: durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía (activado automáticamente la primera vez que se enciende el

terminal), si se dispone de conectividad (por ejemplo, vía Wi-Fi), se ofrece la posibilidad de configurar cuentas de las diferentes redes sociales: Facebook, YouTube y Twitter.

918. La ejecución de las aplicaciones de acceso a las redes sociales está disponible a través del menú “Inicio” y los iconos correspondientes (en la parte superior de la imagen inferior):



5.31.1 GESTIÓN DE CREDENCIALES DE LAS REDES SOCIALES

919. En el caso de Facebook y Twitter no es posible almacenar la contraseña en el dispositivo móvil desde la pantalla de acceso a los servicios de datos de HTC (ver apartado “5.25. Servicios de datos”), siendo necesario introducirla cada vez que se establece una conexión con estas redes sociales.

Nota: la aplicación de acceso a YouTube (de HTC) disponible desde el menú “Inicio” sólo permite ver contenidos de este servicio, sin necesidad de autenticación, y no está relacionada con el servicio de datos de YouTube de HTC, que requiere autenticación para poder subir los vídeos grabados con el dispositivo móvil a YouTube.

920. Sin embargo, la aplicación de Facebook disponible desde “Inicio – Facebook” (desarrollada por Microsoft) sí permite recordar la contraseña. Desde el punto de vista de seguridad, se recomienda no almacenar la contraseña en el dispositivo móvil, mitigando así el riesgo de que un potencial atacante obtenga acceso al dispositivo móvil, y como consecuencia, a la cuenta de Facebook configurada en el mismo.

921. La siguiente clave del registro determina si se debe (valor “1”) o no (valor “0”) almacenar la contraseña:

[HKEY_CURRENT_USER\Software\Microsoft\Facebook]

```
"SaveLogin"= dword:00000000
```

922. La contraseña es almacenada en formato binario en el parámetro “Login” de la misma clave del registro.

923. La configuración de una nueva cuenta de YouTube desde la pantalla de acceso a los servicios de datos de HTC (ver apartado “5.25. Servicios de datos”), por defecto, dispone de la opción “Recordar mi contraseña” habilitada por defecto.

924. La siguiente clave del registro especifica si se debe (valor “1”) o no (valor “0”) almacenar la contraseña para el acceso a YouTube:

```
[HKEY_LOCAL_MACHINE\Software\HTC\HTCAccountManager]  
"YoutubeSavePassword"=dword:00000000
```

925. La contraseña es almacenada como cadena de caracteres “oculta” (con símbolos de “?”) en el parámetro “YoutubePassword” de la misma clave del registro.

926. Desde el punto de vista de seguridad, se recomienda no almacenar la contraseña en el dispositivo móvil, mitigando así el riesgo de que un potencial atacante obtenga acceso al dispositivo móvil, y como consecuencia, a la cuenta de YouTube configurada en el mismo. Esta configuración más segura tiene un impacto directo en la funcionalidad, ya que requiere que el usuario introduzca la contraseña cada vez que se conecte al servicio.

927. Aún cuando la contraseña está almacenada en el registro, al activar el acceso a YouTube (ver apartado “5.25. Servicios de datos”), la aplicación cliente no accede automáticamente al servicio, sino que rellena automáticamente las credenciales de acceso y espera confirmación por parte del usuario, mitigando el impacto de almacenar la contraseña en el dispositivo móvil:



928. Sin embargo, al hacer uso de las capacidades del dispositivo móvil para subir videos grabados con la videocámara del terminal a YouTube sí se accede automáticamente al servicio, sin solicitar confirmación al usuario.

929. La siguiente clave del registro almacena información sobre las cuentas empleadas para el acceso a las diferentes redes sociales desde las aplicaciones de HTC, y contiene numerosos detalles, especialmente al disponer de una sesión activa:

`HKEY_LOCAL_MACHINE\Software\HTC\HTCAccountManager`

Entre otros datos, se almacena:

- Facebook: la cuenta (e-mail) y contraseña (campo vacío), junto al secreto, identificador de sesión, token, identificador de usuario y nombre de usuario.
- Twitter: la cuenta y contraseña (contiene N caracteres “?”, dónde N es el número de caracteres de la contraseña empleada), junto al token, secreto del token y nombre de usuario.
- YouTube: la cuenta (o identificador de usuario) y contraseña (contiene N caracteres “?”, dónde N es el número de caracteres de la contraseña empleada), junto al token y nombre de usuario.

930. Las credenciales de Windows Live son gestionadas de forma independiente, y empleadas para múltiples aplicaciones, como My Phone o Marketplace (ver apartados “5.23.1. Microsoft My Phone” y “5.32. Aplicaciones de terceros: Windows Marketplace for Mobile”).

Nota: las aplicaciones de acceso a las redes sociales utilizan el registro para almacenar información de configuración para su funcionamiento y detalles del perfil de usuario:

- La información del perfil del usuario de Facebook se almacena en “HKEY_LOCAL_MACHINE\Software\HTC\FacebookSDK”.
- La aplicación cliente de HTC para Twitter almacena los parámetros de configuración del servicio en “HKEY_CURRENT_USER\Software\HTC\TwitterApp”.

Se recomienda revisar que dichas claves del registro no dispongan de más información de la deseada con el objetivo de gestionar la privacidad del usuario.

5.31.2 AUTENTIFICACIÓN Y SEGURIDAD DE LAS COMUNICACIONES DE LAS REDES SOCIALES

931. El proceso de autenticación y conexión a cada una de las redes sociales disponibles por parte de las aplicaciones cliente instaladas en el dispositivo móvil es crítico de cara a evaluar el nivel de protección existente y las recomendaciones de seguridad a aplicar.

932. Facebook emplea una conexión cifrada con SSL/TLS (TCP/443) desde el dispositivo móvil hacia “api.facebook.com” para el envío de las credenciales durante el proceso de autenticación. La sesión posterior con Facebook se realiza mediante HTTP (TCP/80) sin cifrar con el mismo servidor y otros servidores de contenidos, como “static.ak.fbcdn.net”. La aplicación se identifica como “User-Agent: HTC Agent”. En el caso del cliente de Facebook (de Microsoft), frente al servicio de datos de Facebook de HTC, el cliente se identifica como “User-Agent: WM FBService”.

933. Twitter emplea una conexión HTTP (TCP/80), no cifrada, desde el dispositivo móvil hacia “twitter.com” para el envío de las credenciales mediante OAuth durante el proceso

de autenticación. Por tanto, al no emplear HTTPS, las credenciales de acceso son reveladas en el tráfico web de autenticación, pese a utilizarse OAuth. La sesión posterior con Twitter se realiza mediante HTTP (TCP/80) sin cifrar con el mismo servidor y otros servidores de contenidos, como “s.twimg.com”. Durante la misma se emplea OAuth en combinación con autenticación HTTP “Basic”, revelándose en la red las credenciales de acceso a Twitter sin cifrar (ej. “/direct_messages.json” o “/favorites.json”). La aplicación se identifica como “User-Agent: TwitterEngine”.

Nota: estas dos vulnerabilidades en el proceso de autenticación del cliente HTC Peep han sido notificadas a HTC [Ref.- 110].

934. YouTube emplea una conexión cifrada con SSL/TLS (TCP/443) desde el dispositivo móvil hacia “www.google.com” para el envío de las credenciales durante el proceso de autenticación. La sesión posterior con YouTube se realiza mediante HTTP (TCP/80) sin cifrar hacia otros servidores de Google, como “gdata.youtube.com” o “i.ytimg.com”. La aplicación se identifica como “User-Agent: HTCYouTube”.
935. Windows Live emplea una conexión cifrada con SSL/TLS (TCP/443) desde el dispositivo móvil hacia “login.live.com” para el envío de las credenciales durante el proceso de autenticación. Las sesiones posteriores se establecen mediante HTTP (TCP/80) y múltiples servidores, como “go.microsoft.com” o “m.live.com”, donde el cliente se identifica como “User-Agent: WLMHttpTransport”. Las sesiones de Messenger se realizan mediante SSL (TCP/50001) con el servidor de mensajería “tcp.mws.mobile.live.com”.
936. Se recomienda limitar el uso de las aplicaciones de acceso a redes sociales desde el dispositivo móvil, ya que un potencial atacante mediante la interceptación del tráfico HTTP no cifrado podría obtener toda la información intercambiada con la red social (los detalles del perfil del usuario, su estado, mensajes, peticiones de amistad, invitaciones a grupos y eventos, etc), así como el identificador (o cookie) de sesión (información suficiente para la realización de ataques de suplantación de la sesión en la red social).
937. La recomendación de no acceder a las redes sociales, en el caso de Twitter, es imperativa, ya que el tráfico contiene incluso las credenciales de acceso sin cifrar, por lo que un potencial atacante dispondría de acceso completo a la cuenta del usuario.

5.32 APLICACIONES DE TERCEROS: WINDOWS MARKETPLACE FOR MOBILE

938. El servicio “Windows Marketplace for Mobile” [Ref.- 4], en adelante Marketplace, es empleado por Microsoft para la distribución y venta de aplicaciones y software para la plataforma Windows Mobile.
939. Windows Mobile 6.5 incluye una nueva aplicación, denominada “Marketplace”, disponible en función del fabricante u operador de telefonía móvil, para el acceso a este servicio directamente desde el terminal.
940. El icono de la aplicación está disponible desde el menú “Inicio”, y la primera vez que se utiliza, permite la descarga y ejecución de la aplicación. La verificación de la versión disponible y la descarga se realiza con los servidores “client.” y “cdnclient.” de “.marketplace.windowsmobile.com”, respectivamente, mediante HTTPS.

941. Para instalar y/o comprar aplicaciones en Marketplace es necesario emplear una cuenta Windows Live (usuario y contraseña), no así para consultar las aplicaciones disponibles. La pantalla de acceso (imagen inferior derecha), disponible desde el menú “My Applications” (o el botón “Menu” y la opción “Sign in”), ofrece almacenar la contraseña por defecto (“Save Password”):



942. La siguiente clave del registro almacena la información de acceso y sesión de Marketplace, como por ejemplo los identificadores del dispositivo móvil, ficheros de instalación, token de sesión, etc:

```
HKEY_CURRENT_USER\Security\Software\Microsoft\Marketplace
```

Si se almacena la contraseña, las credenciales son almacenadas de forma segura en:

```
HKEY_LOCAL_MACHINE\Comm\Security\CredMan\Creds
```

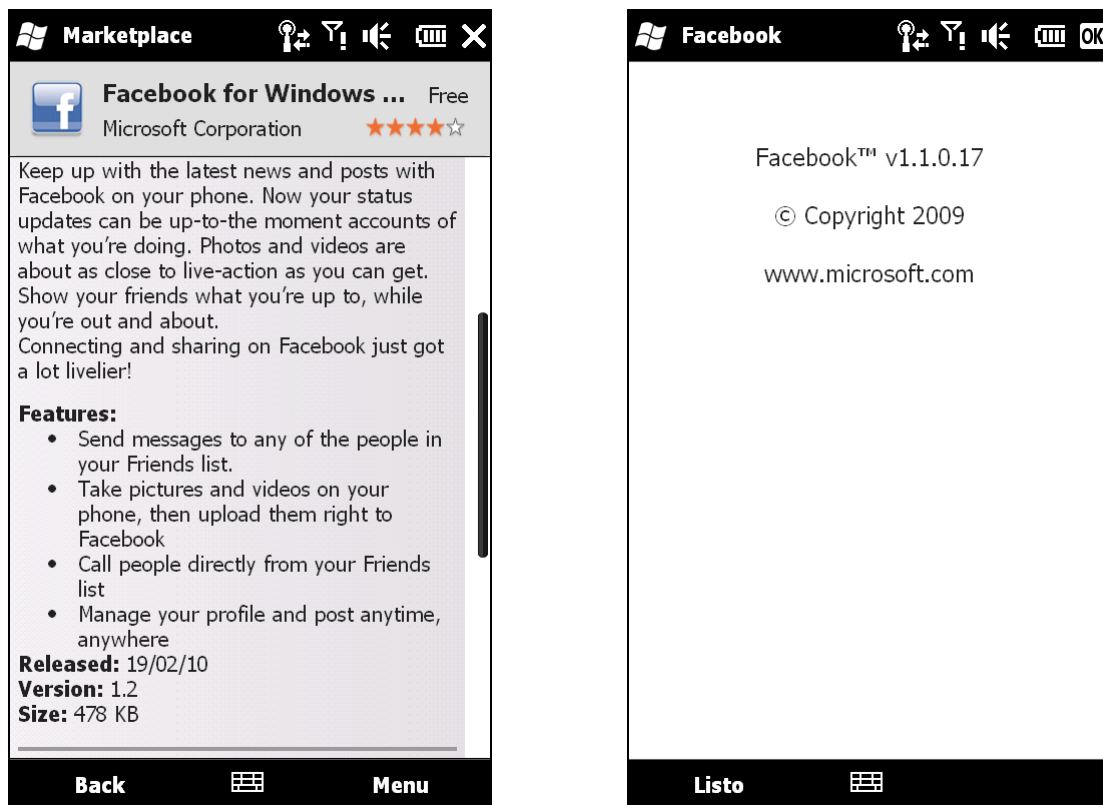
El último identificador (e-mail) empleado para acceder a Windows Live se almacena en:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Live\LastId\PassportName
```

943. Desde el punto de vista de seguridad, se recomienda no almacenar la contraseña en el dispositivo móvil, mitigando así el riesgo de que un potencial atacante obtenga acceso al dispositivo móvil, y como consecuencia, a la cuenta de Marketplace (y potencialmente a la compra de aplicaciones de pago).
944. En caso de haber almacenado la contraseña, es posible modificar la configuración de acceso (y no almacenarla) cerrando la sesión con Marketplace a través del botón “Menú” y la opción “Sign out”.
945. El proceso de autenticación de Windows Live se realiza a través de una conexión HTTPS (TCP/443) con “login.live.com”, mientras que la comunicación con Marketplace se realiza mediante HTTP (TCP/80), sin cifrar, con los servidores web “api.marketplace.windowsmobile.com”, “files.marketplace.windowsmobile.com” y

“msnportalmobilemarketplace.112.2o7.net”. La aplicación se identifica como “User-Agent: SkyMarket”. La descarga de aplicaciones desde Marketplace se lleva a cabo a través de una conexión HTTPS (TCP/443) con “files.marketplace.windowsmobile.com”.

946. La utilización de HTTP frente a HTTPS podría permitir a un potencial atacante la manipulación del tráfico y la redirección del usuario hacia otros servidores para la descarga de aplicaciones maliciosas.
947. Se recomienda actualizar a la última versión de las aplicaciones ya instaladas en el dispositivo móvil. Por ejemplo, en el momento de elaboración de la presente guía Marketplace disponía de la versión 1.2 (19/02/2010; v1.1.0.17) de la aplicación “Facebook for Windows Mobile” (siendo la versión instalada por defecto la v1.007, 2009). Su instalación requiere reiniciar el dispositivo móvil:



Nota: tras realizar la instalación, por defecto, el perfil de Facebook del usuario mostrará un mensaje indicando este hecho, y desvelando el momento de la instalación y la plataforma móvil empleada, información relevante para un potencial atacante:



Esta funcionalidad puede ser desactivada desde la opción “Account - Application Settings (Recently Used)” de Facebook (disponible a través del interfaz web estándar), y en concreto, editando la configuración para “Windows Phone” y deshabilitando la opción “Publish content to my Wall” de la pestaña “Additional Permissions”.

948. La lista de programas o aplicaciones instaladas desde Marketplace es accesible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Sistema – Quitar programas”:



Nota: los desarrolladores interesados en la creación de aplicaciones para Windows Mobile disponen de todos los detalles e información en el portal para desarrolladores de Windows Phone (<http://developer.windowsphone.com>).

949. Debe tenerse en cuenta que la disponibilidad de una aplicación en Marketplace no asegura que la misma no sea maliciosa y pueda llevar a cabo acciones desde el dispositivo móvil donde ha sido instalada que afecten a la seguridad y privacidad del usuario [Ref.- 1].
950. Se recomienda analizar en detalle el contenido y procedencia de una aplicación de terceros antes de instalarla desde Marketplace en el dispositivo móvil.

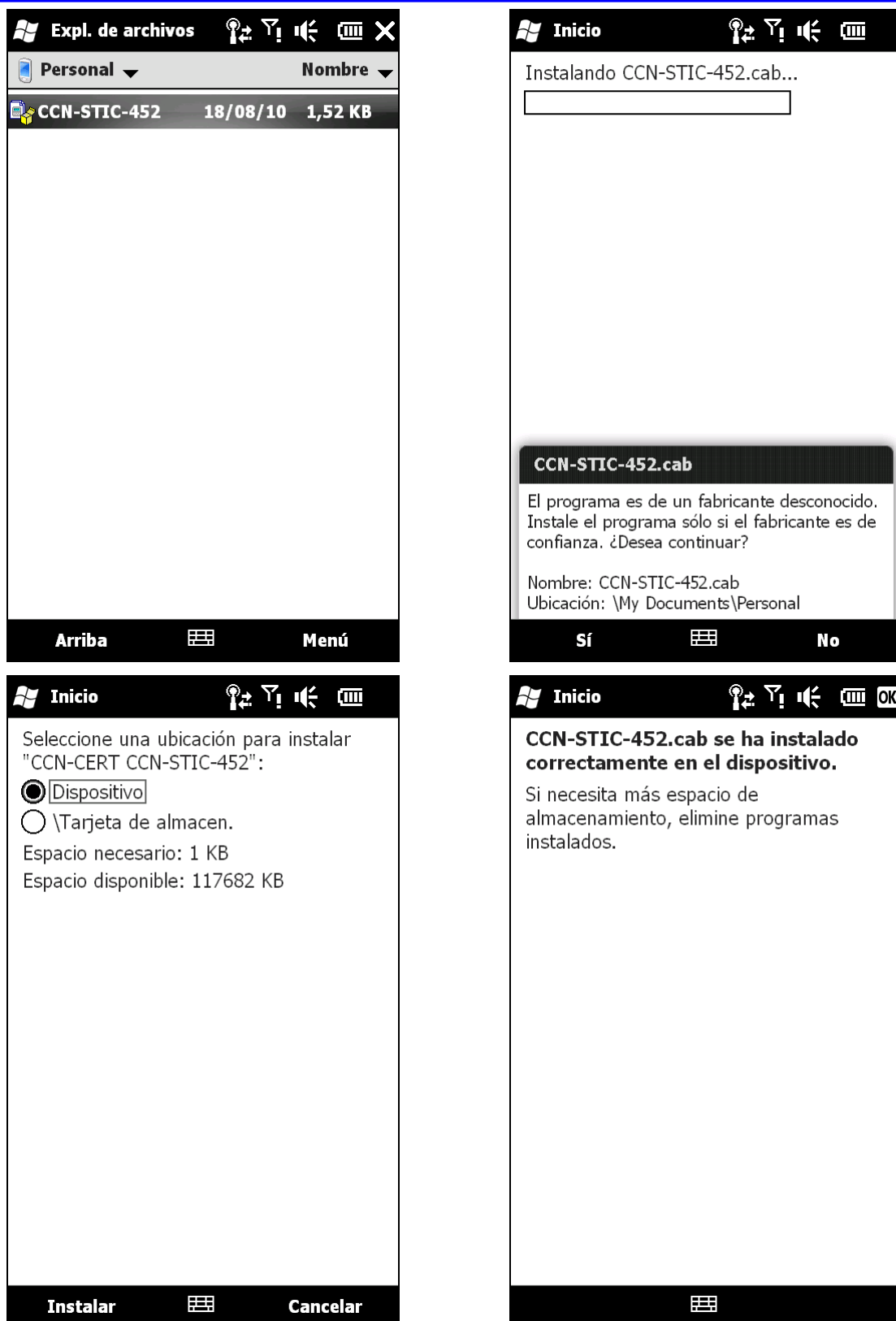
Nota: el número de aplicaciones cliente instaladas por defecto por Microsoft, el fabricante del dispositivo móvil o el operador de telefonía móvil, así como la variedad de aplicaciones cliente de otras compañías que pueden ser instaladas posteriormente manualmente o desde Marketplace, hace inviable su análisis de seguridad dentro del alcance de la presente guía.

Para todas las aplicaciones instaladas, o a instalar, en el dispositivo móvil se recomienda realizar un análisis similar al efectuado previamente, identificando la versión actualmente instalada, evaluando la gestión de credenciales de acceso (almacenamiento y utilización), así como los protocolos empleados durante el proceso de autenticación y durante el resto de la sesión, así como cualquier otra característica de seguridad ofrecida por la aplicación.

6 APLICACIÓN DE LA GUÍA DE SEGURIDAD CCN-STIC-452

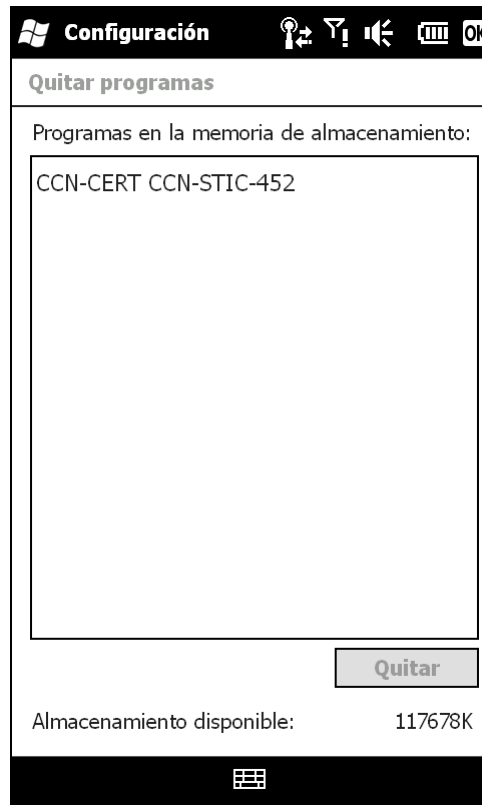
951. Para aplicar la configuración de seguridad de referencia sugerida por la presente guía deben seguirse los pasos definidos a continuación, que conllevan tanto acciones manuales como automáticas sobre el dispositivo móvil. Ciertas acciones manuales deben realizarse antes de las acciones automáticas, indicándose claramente en ese supuesto.
952. Debe tenerse en cuenta que los scripts de aplicación de la guía no son exhaustivos, y por tanto no cubren todas las recomendaciones de seguridad sugeridas a lo largo del presente documento, ya que muchas de ellas pueden interferir en la funcionalidad del dispositivo móvil, y es el propietario del mismo el que debe determinar su aplicación.
953. La aplicación de la guía de seguridad puede eliminar los datos existentes en el dispositivo móvil, por lo que debe ser aplicada antes de hacer uso y almacenar datos en el mismo.
954. Las modificaciones manuales de configuración a realizar adicionalmente a las acciones automáticas llevadas a cabo por el script de aplicación de la presente guía son:
- Actualización del sistema operativo Windows Mobile 6.5 y las aplicaciones asociadas mediante las actualizaciones software disponibles en Microsoft y/o el fabricante del dispositivo móvil. *Este paso se deberá realizar previamente a la aplicación de la guía de seguridad.*
 - En el caso de dispositivos que soporten los dos modelos de seguridad disponibles en Windows Mobile (one-tier y two-tier), se recomienda analizar y seleccionar el modelo adecuado que se desea utilizar. *Este paso se deberá realizar previamente a la aplicación de la guía de seguridad.*
 - En los dispositivos que no soportan ambos modelos, se recomienda analizar el modelo soportado actualmente (política de seguridad 4123). Esta información es proporcionada por el script de aplicación de la presente guía.
 - Se recomienda analizar los certificados digitales disponibles en los contenedores o *stores* existentes.
 - Se recomienda fijar un PIN de acceso a la tarjeta SIM.
 - Se recomienda fijar una contraseña de acceso al dispositivo móvil suficientemente compleja. El script de aplicación de la presente guía está diseñado para condicionar esta selección.
 - Se recomienda habilitar el cifrado de los datos del dispositivo móvil mediante la instalación y configuración de las opciones de gestión empresariales o de la utilidad DojoCrypt (ver apartado “5.12.1. Cifrado del dispositivo móvil”).
 - Se recomienda definir el perfil de conexión de datos a Internet y a Trabajo en función de las capacidades de conectividad disponibles, así como la definición particular de redes privadas virtuales (VPNs).
 - Se recomienda añadir una conexión de datos vacía al dispositivo móvil, tal como se describe en el apartado “5.20. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”.
 - Se recomienda analizar los dispositivos Bluetooth existentes en la lista de dispositivos emparejados.

- Se recomienda analizar las redes Wi-Fi disponibles en la lista de redes preferidas (o PNL).
 - Se recomienda evaluar la gestión del dispositivo móvil desde el punto de vista empresarial, de copias de seguridad, de aplicaciones cliente, y de servicios avanzados, como Microsoft MyPhone, y su integración con otras aplicaciones y servicios, como por ejemplo redes sociales.
 - Debe recordarse que los dispositivos móviles basados en Windows Mobile 6.5 son vulnerables a diferentes problema mencionados a lo largo de la presente guía y para los que no existe solución disponible en el momento de la elaboración de la misma, como por ejemplo TAD-2010-002, TAD-2010-003 y TAD-2011-001.
955. Para llevar a cabo la aplicación de la presente guía es necesario únicamente conectar el dispositivo móvil al ordenador (Windows XP, Vista o 7) que dispone de Microsoft AcitveSync o Windows Mobile Device Center, y proceder a ejecutar el script “CCN-STIC-452_WindowsMobile_6.5.bat”.
956. El script dirige al usuario a través de los diferentes pasos que son necesarios como parte del proceso de aplicación de la guía, e indicará cuando son necesarias acciones manuales por parte del usuario, por ejemplo, para la instalación de los ficheros .CAB que contienen las modificaciones del registro de Windows Mobile.
957. El fichero “CCN-STIC-452.cab” contiene todas las configuraciones de registro generales de Windows Mobile 6.5 recomendadas desde el punto de vista de seguridad.
958. El fichero “CCN-STIC-452_HTC.cab” contiene todas las configuraciones de registro propias de dispositivos móviles HTC recomendadas desde el punto de vista de seguridad.
959. Debe tenerse en cuenta que existen modificaciones que no pueden ser automatizadas, ya que los valores a emplear son propios de cada usuario o propietario del terminal, como por ejemplo las conexiones VPN existentes, por lo que (como se ha indicado previamente) se recomienda su modificación manual.
960. Al instalar y ejecutar un fichero .CAB en el dispositivo móvil para aplicar los cambios de configuración de seguridad, como por ejemplo modificaciones en el registro de Windows Mobile 6.5, el fichero .CAB o programa queda registrado en la lista de programas instalados.
961. Las siguientes cuatro imágenes muestran el proceso de instalación tras copiar el fichero “CCN-STIC-452.cab” a la carpeta “\My Documents\Personal” del dispositivo móvil, pulsar sobre él, aceptar su instalación y seleccionar la ubicación para la instalación:



962. La instalación del fichero "CCN-STIC-452.cab", y sus directivas de seguridad (política 4131), puede requerir que se renueve el valor de la contraseña de acceso al dispositivo móvil de forma inmediata tras su aplicación. Debe procederse a fijar el nuevo valor de la contraseña si así se indica.

963. El mismo proceso de instalación descrito previamente debe ser llevado a cabo con el fichero “CCN-CERT-452_HTC.cab” en dispositivos móviles HTC.
964. La lista de programas en la memoria de almacenamiento es accesible a través del menú “Inicio – Configuración”, mediante el botón “Menú” y la opción “Más”, y el icono “Sistema – Quitar programas”, desde dónde es posible quitar los programas disponibles a través del botón “Quitar”:



965. La imagen superior muestra la instalación del fichero .CAB con el nombre “CCN-STIC-452”, cuyo autor es “CCN-CERT”.
966. Los programas listados asociados a ficheros de configuración de seguridad .CAB pueden ser eliminados para liberar memoria de almacenamiento sin ninguna implicación adicional, ya que su eliminación no afecta a los cambios que el programa llevó a cabo, por ejemplo, en el registro de Windows Mobile.

Nota: debe tenerse especial cuidado en la selección de entradas de la lista de programas, ya que la eliminación de otros programas (en lugar de los asociados a ficheros .CAB) llevará a cabo la desinstalación completa del programa, no siendo posible su utilización salvo que vuelva a ser instalado.

967. Una vez instalados los ficheros .CAB, debe continuarse la ejecución del script de aplicación de la presente guía. Tras su finalización, es necesario reiniciar el dispositivo móvil para que todos los cambios surtan efecto.

7 APÉNDICE A: TABLA DE POLÍTICAS DE SEGURIDAD DE WINDOWS MOBILE

La siguiente tabla incluye las políticas de seguridad o parámetros de configuración posibles en Windows Mobile, incluyendo el identificador (ID) de política (en decimal), el valor por defecto, y los roles [Ref.- 15].

Policy ID	Policy Setting	Description
2	Auto Run Policy SECPOLICY_CFAUTORUN	This setting indicates whether applications stored on a Multimedia Card (MMC) are allowed to auto-run when inserted into the device. Defecto value is 0 for Windows Mobile Professional. The value is not set for Windows Mobile Standard. The following list shows the possible values: • 0 indicates that applications are allowed to run automatically • 1 indicates that applications are restricted from running automatically The required role to modify this policy is SECROLE_MANAGER.
4097 (0x1001)	RAPI Policy SECPOLICY_RAPI	This setting restricts the access of remote applications that are using Remote API (RAPI) to implement ActiveSync operations on Windows Mobile devices. Default value is 2 for Windows Mobile. The following list shows the possible values: • 0 indicates that the ActiveSync service is shut down. RAPI calls are rejected. • 1 indicates full access to ActiveSync is provided. RAPI calls are allowed to process without restrictions. • 2 indicates that access to ActiveSync is restricted to the SECROLE_USER_AUTH (User Authenticated) role. RAPI calls are checked against this role mask before they are granted. The required role to modify this policy is

		SECROLE_MANAGER.
4101	Unsigned CABS Policy SECPOLICY_UNSIGNDCABS	This setting indicates whether unsigned .cab files can be installed on the device. On Windows Mobile Standard, accepted unsigned .cab files are installed with the role mask specified by the policy value. For Windows Mobile Standard, if a signed .cab file does not have a matching root certificate in the Software Publisher Certificate (SPC) store, the file is unsigned. You should always use SECPOLICY_UNSIGNDCABS together with SECPOLICY_UNSIGNDCAPPS. This means that when you block unsigned application from running, you should also block unsigned cab files from getting installed. Note: CAB Provisioning Format files — files with a .cpf extension — are processed the same as .cab files when the files are signed. However, when the .cpf file is unsigned the loader processes the .cpf files in silent mode, which means that the user will not get a prompt asking if the user wants to proceed with loading the unsigned file. In this case, the loading process fails. Default value is SECROLE_USER_AUTH for Windows Mobile. The following list shows the possible values: • SECROLE_USER_AUTH indicates that Unsigned .cab files will be installed under the SECROLE_USER_AUTH role. • 0 is equivalent to having none of the role mask bits set, and means that no unsigned .cab files can be installed. • A specified role mask indicates accepted unsigned .cab files are installed with the role mask specified. The required role to modify this policy is SECROLE_MANAGER.
4102	Unsigned Applications Policy SECPOLICY_UNSIGNEDA	This setting indicates whether unsigned applications are allowed to run on Windows Mobile devices. If a signed application does not

	PPS	have a matching root certificate in the Privileged Execution Trust Authorities or the Unprivileged Execution Trust Authorities certificate store, the application is unsigned. You should always use SECPOLICY_UNSIGNDCABS together with SECPOLICY_UNSIGNDAPPS policy. This means that when you block unsigned applications from running, you should also block unsigned cab files from getting installed on the device. Default value is 1 for Windows Mobile. The following list shows the possible values: • 0 indicates that unsigned applications are not allowed to run on the device. • 1 indicates that unsigned applications are allowed to run on the device. • Any value other than 1 is treated as 0. The required role to modify this policy is SECROLE_MANAGER.
4103	Unsigned Themes Policy SECPOLICY_UNSIGNDTHEMES	This setting indicates whether theme files can be installed on the device. Theme files are used for processing home screens. Accepted unsigned theme files are installed with the role mask specified by the policy value. For Windows Mobile devices, if a signed theme file does not have a matching root certificate in the Software Publisher Certificate (SPC) store, the file is unsigned. Default value is SECROLE_USER_UNAUTH for Windows Mobile. The following list shows the possible values: • SECROLE_USER_UNAUTH indicates that Unsigned Theme files will be installed under the SECROLE_USER_UNAUTH role. • 0 is equivalent to having none of the role mask bits set, and means that no unsigned Theme files can be installed. • A specified role mask indicates accepted unsigned Theme files are installed with

		the role mask specified. The required role to modify this policy is SECROLE_MANAGER.
4104	Trusted Provisioning Server (TPS) Policy SECPOLICY_TPSCARRIER ROLE	This setting indicates whether mobile operators can be assigned the Trusted Provisioning Server (TPS) role. Default value is 1 for Windows Mobile. The following list shows the possible values: • 0 indicates assigning TPS role assignment is disabled. • 1 indicates TPS role assignment is enabled. Thus, the TPS role can be assigned to mobile operators. The required role to modify this policy is SECROLE_MANAGER.
4105	Message Authentication Retry Number Policy SECPOLICY_MAXAUTHENTICATIONRETRY	This setting specifies the maximum number of times the user is allowed to try authenticating a Wireless Application Protocol (WAP) PIN-signed message. Default value is 3 for Windows Mobile. Possible values are 1 through 256. The required role to modify this policy is SECROLE_MANAGER.
4107	WAP Signed Message Policy SECPOLICY_WAPSIGNMSG	This policy has been deprecated. Use SECPOLICY_OMACPNETWPINMSG (4141), SECPOLICY_OMACPUSERPINMSG (4142), and SECPOLICY_OMACPUSERNETWPINMSG (4143) instead. While this policy is still supported, you cannot query for 4107 policy value. Note: You cannot use the new security policies (4141, 4142, 4143) and 4107 in the same provisioning document. The required role to modify this policy is SECROLE_MANAGER.
4108	Service Loading (SL) Message Policy	This setting indicates whether SL messages are accepted. An SL message downloads new services or provisioning XML to the Windows

	SECPOLICY_SL_MESSAGE	Mobile device. You specify the security roles that can accept SL messages as a role mask. Default value is SECROLE_PPG_TRUSTED for Windows Mobile. The required role to modify this policy is SECROLE_MANAGER.
4109	Service Indication (SI) Message Policy SECPOLICY_SI_MESSAGE	This setting indicates whether SI messages are accepted. An SI message is sent to Windows Mobile Standard to notify users of new services, service updates, and provisioning services. You specify the security roles that can accept SI messages as a role mask. Default is SECROLE_PPG_AUTH SECROLE_PPG_TRUSTED for Windows Mobile. The required role to modify this policy is SECROLE_MANAGER.
4110	Unauthenticated Message Policy SECPOLICY_UNAUTHMESSAGES	This setting indicates whether to accept unsigned WAP messages processed by the default security provider in the Security Module (Push Router), based on their origin. The message source must have one of the security roles specified by this policy. You specify the security roles that the unsigned messages will be accepted from as a role mask. Default value is SECROLE_USER_UNAUTH for Windows Mobile. The required role to modify this policy is SECROLE_MANAGER.
4111	OTA Provisioning Policy SECPOLICY_OTAPROVISIONING	This setting specifies which provisioning messages are accepted by the configuration host based on the roles assigned to the messages. This policy limits the provisioning messages that come from the push router. The default is SECROLE_OPERATOR_TPS SECROLE_PPG_TRUSTED SECROLE_PPG_AUTH SECROLE_TRUSTED_PPG

		SECROLE_USER_AUTH SECROLE_OPERATOR for Windows Mobile. A specified role mask indicates system administrative privileges are given to the role mask specified. The required role to modify this policy is SECROLE_MANAGER.
4113	WSP Push Policy SECPOLICY_WSPNOTIFICATIONS	This setting indicates whether Wireless Session Protocol (WSP) notifications from the WAP stack are routed. Default value is 1 for Windows Mobile. The following list shows the possible values: • 0 indicates that routing of WSP notifications is not allowed. • 1 indicates Routing of WSP notifications is allowed. The required role to modify this policy is SECROLE_MANAGER.
4119	Grant Manager Policy SECPOLICY_GRANTMANAGER	This setting grants the system administrative privileges held by SECROLE_MANAGER to other security roles, without modifying metabase role assignments. The configuration manager enforces the Grant Manager policy. Default value is SECROLE_OPERATOR_TPS for Windows Mobile Professional, SECROLE_USER_AUTH for Windows Mobile Classic, and OPERATOS_TPS for Windows Mobile Standard. The following list shows the possible values: • SECROLE_USER_AUTH indicates system administrative privileges are given to the SECROLE_USER_AUTH mask. • SECROLE_NONE indicates that only the manager is granted the Manager role. • A specified role mask indicates system administrative privileges are given to the role mask specified.

		The required role to modify this policy is SECROLE_MANAGER.
4120	Grant User Authenticated Policy SECPOLICY_GRANTUSERAUTH	This setting grants privileges held by SECROLE_USER_AUTH to other security roles without modifying metabase role assignments. Default value is SECROLE_USER_AUTH for Windows Mobile. The following list shows the possible values: • SECROLE_USER_AUTH indicates that no additional administrative privileges are given. • A specified role mask indicates system administrative privileges are given to the role mask specified. Configuration Manager enforces the Grant User Authenticated policy. The required role to modify this policy is SECROLE_MANAGER.
4121	Trusted WAP Proxy Policy SECPOLICY_TRUSTED_WAP_PROXY	This setting specifies the level of permissions required to create, modify, or delete a trusted proxy. WAP proxies are configured by means of the PXLOGICAL characteristic element in a WAP provisioning XML document. A WAP proxy is trusted when the TRUST parameter is specified in the PXLOGICAL characteristic element. You specify the security roles that can have Trusted WAP Proxy level permissions as a role mask. Default value is SECROLE_OPERATOR SECROLE_OPERATOR_TPS SECROLE_MANAGER for Windows Mobile. The required role to modify this policy is SECROLE_MANAGER.
4122	Unsigned Prompt Policy SECPOLICY_UNSIGNEDPROMPT	This setting indicates whether a user is prompted to accept or reject unsigned .cab, theme, .dll and .exe files. Default value is 0 for Windows Mobile. If the value is not set in the registry, then the behavior is

		the same as setting it to 0. The following list shows the possible values: • 0 indicates user will be prompted. • 1 indicates user will not be prompted. • Any value other than 1 is treated as 0. The required role to modify this policy is SECROLE_MANAGER.
4123	Privileged Applications Policy SECPOLICY_PRIVILEGED APPS	This setting specifies which security model is implemented on the device. Note: This policy applies only to Windows Mobile Standard. Default value is 1 for Windows Mobile Professional. The default value is 0 for Windows Mobile Standard. If the value is not set in the registry, then the behavior is the same as setting it to 0. The following list shows the possible values: • 0 indicates that a two-tier security model is enabled. • 1 indicates that a one-tier security model is enabled. • Any value other than 1 is treated as 0. The required role to modify this policy is SECROLE_MANAGER. For information about how the one-tier and two-tier security models affect applications, see Windows Mobile Device Security Model.
4124	SL Security Policy SECPOLICY_SLSECURED OWNLOAD	This setting allows the operator to override https to use http, or wsps to use wsp. The following list shows the possible values: • 0 use https or wsps. • 1 use http or wsp. Default value is 1. The required role to modify this policy is SECROLE_MANAGER.

4125	Signed Mail Policy SECPOLICY_USESIGN	This policy has been deprecated. Use SECPOLICY_SMIMESIGNING (4137) and SECPOLICY_SMIMESIGNINGALGORITHM (4139) instead.
4126	Encrypted Message Policy SECPOLICY_USEENCRYPT	This setting has been deprecated. Use SECPOLICY_SMIMEENCRYPTION (4138) and SECPOLICY_SMIMEENCRYPTIONALGORITHM (4140) instead.
4127	Software Certificates Policy SECPOLICY_SOFTCERTS	This setting determines whether an outbound message that is sent over Secure/Multipurpose Internet Mail Extensions (SMIME) can be signed with a software certificate. You can use this security policy with a tool that you create to allow people to import certificates. The following list shows the possible values: • 0 indicates that software certificates cannot be used to sign messages. • 1 indicates that software certificates can be used to sign messages. The Default value is 1.
4129	DRM Security Policy SECPOLICY_DRM_WAPRIGHTS	This setting specifies which DRM rights messages are accepted by the DRM engine based on the role assigned to the message. Default is SECROLE_PPG_AUTH SECROLE_PPG_TRUSTED.
4131 (0x1023)	Password Required Policy SECPOLICY_LASS_PWD_REQUIRED	This policy indicates whether a password must be configured on the device. The following list shows the possible values: • 0 indicates that a password is required. • A value other than 0 indicates that a password is not required. The Default value is zero (0). The associated registry key does not exist by default. The Required role to modify this policy is SECROLE_MANAGER or SECROLE_ENTERPRISE.
4132	Network PIN Prompt Policy SECPOLICY_WAP_NETWORK_PIN_PROMPT	This setting is used when the over the air (OTA) OMA Client Provisioning message is signed with only a network personal identification number (PIN). This setting indicates whether or not to

		prompt the user to accept device setting changes. The following list shows the possible values: • 0 indicates that the device prompts the user for confirmation to accept changes to device settings. • 1 indicates that the user is not prompted. The Default value is 1. The Required role to modify this policy is SECROLE_MANAGER.
4133	Desktop Unlock SECPOLICY_LASS_DESKTOP	This policy has been deprecated. Use SECPOLICY_LASS_DESKTOP_QUICK_CONNECT (4146) instead.
4134	Encrypt Removable Storage Policy SECPOLICY_MENCRYPT_REMOVABLE	This setting specifies if the user is allowed to change mobile encryption settings for the removable storage media. The default setting is 1. • 0 (POLICYVAL_MENCRYPT_REMOVABLE_NO_USER) indicates that the user is not allowed to change the encryption settings. • 1 (POLICYVAL_MENCRYPT_REMOVABLE_USER_ALLOW) indicates that the user can change the encryption settings. The required role to modify this policy is SECROLE_MANAGER or SECROLE_ENTERPRISE.
4135	Bluetooth Policy SECPOLICY_BLUETOOTH	This setting specifies if a Bluetooth enabled device allows other devices to perform a search on the device. • 0 (POLICYVAL_BLUETOOTH_VISIBLE_BLOCKED) blocks other devices from searching. • 1 (POLICYVAL_BLUETOOTH_VISIBLE_ALLOWED) allows other devices to search.

4136	HTML Message Policy SECPOLICY_HTML_MESSAGE	This setting specifies whether message transports will allow HTML messages. • 0 (POLICYVAL_HTML_MESSAGE_DISABLED) indicates that HTML messages are not allowed. • 1 (POLICYVAL_HTML_MESSAGE_ENABLED) indicates that HTML messages are allowed.
4137	SMIME Signing Policy SECPOLICY_SMIMESIGNING	This setting specifies whether the Inbox application will send all messaged signed. • 0 (POLICYVAL_SMIMESIGNING_FORCED) all messages must be signed. • 1 (POLICYVAL_SMIMESIGNING_OPTIONAL) signing messages is optional.
4138	SMIME Encryption Policy SECPOLICY_SMIMEENCRYPTION	This setting specifies whether the Inbox application will send all messages encrypted. • 0 (POLICYVAL_SMIMEENCRYPTION_FORCED) all messages must be encrypted. • 1 (POLICYVAL_SMIMEENCRYPTION_OPTIONAL) encrypting messages is optional.
4139	SMIME Signing Algorithm Policy SECPOLICY_SMIMESIGNINGALGORITHM	This setting specifies which algorithm to use to sign a message. • 0 (POLICYVAL_SMIMESIGNINGALGORITHM_DEFAULT) specifies the default algorithm. • 1 is an invalid value. Do not use this value. • 2 (POLICYVAL_SMIMESIGNINGALGORITHM_SHA_1) specifies SHA algorithm. • 3 (POLICYVAL_SMIMESIGNINGALGO

		RITHM_MD5) specifies MD5 algorithm.
4140	SMIME Encryption Algorithm Policy SECPOLICY_SMIMEENCRIPTIONALGORITHM	This setting specifies which algorithm to use to encrypt a message. 0 (POLICYVAL_SMIMEENCRIPTIONALGORITHM_DEFAULT) specifies the default algorithm. 1 is an invalid value. Do not use this value. 2 (POLICYVAL_SMIMEENCRIPTIONALGORITHM_3DES) specifies triple DES algorithm. 3 (POLICYVAL_SMIMEENCRIPTIONALGORITHM_DES)) specifies DES algorithm. 4 (POLICYVAL_SMIMEENCRIPTIONALGORITHM_RC2_128)) specifies RC2 128-bit algorithm. 5 (POLICYVAL_SMIMEENCRIPTIONALGORITHM_RC2_64)) specifies RC2 64-bit algorithm. 6 (POLICYVAL_SMIMEENCRIPTIONALGORITHM_RC2_40) specifies RC2 40-bit algorithm.
4141	OMA CP Network PIN Policy SECPOLICY_OMACPNETWPINMSG	This setting determines whether the OMA network PIN signed message will be accepted to be processed. The message that is accepted to be processed is still subject to network PIN signing authentication. If the authentication fails, the message will be dropped. The default is SECCROLE_PPG_AUTH SECCROLE_PPG_TRUSTED SECCROLE_OPERATOR_TPS. You can also use the following security roles: - SECCROLE_KNOWN_PPG - SECCROLE_TRUSTED_PPG - SECCROLE_ANY_PUSH_SOURCE

		You cannot use any other role than those specified above, otherwise the request will fail. The required role to modify this policy is SECROLE_MANAGER. Note: You cannot use 4141 and 4107 in the same provisioning document. The old security policy 4107 is deprecated.
4142	OMA CP User PIN Policy SECPOLICY_OMACPUSER PINMSG	This setting determines whether the OMA user PIN or MAC signed message will be accepted to be processed. The message that is accepted to be processed is still subject to user PIN or MAC signing authentication. If the authentication fails, the message will be dropped. The default is SECROLE_PPG_AUTH SECROLE_PPG_TRUSTED SECROLE_OPERATOR_TPS You can also use the following security roles: • SECROLE_TRUSTED_PPG • SECROLE_ANY_PUSH_SOURCE • SECROLE_KNOWN_PPG You cannot use any other role than those specified above, otherwise the request will fail. The required role to modify this policy is SECROLE_MANAGER. Note: You cannot use 4142 and 4107 in the same provisioning document. The old security policy 4107 is deprecated.
4143	OMA CP User Network PIN Policy SECPOLICY_OMACPUSER NETWPINMSG	This setting determines whether the OMA user network PIN signed message will be accepted to be processed. The message that is accepted to be processed is still subject to the user network PIN signing authentication. If the authentication fails, the message will be dropped. The default is SECROLE_PPG_AUTH SECROLE_PPG_TRUSTED SECROLE_OPERATOR_TPS.

		You can also use the following security roles: • SECROLE_KNOWN_PPG • SECROLE_TRUSTED_PPG • SECROLE_ANY_PUSH_SOURCE You cannot use any other role than those specified above, otherwise the request will fail. The required role to modify this policy is SECROLE_MANAGER. Note: You cannot use 4143 and 4107 in the same provisioning document. The old security policy 4107 is deprecated.
4144	Message Encryption Negotiation Policy SECPOLICY_SMIMEENCRIPTIONNEGOTIATION	This setting specifies whether the Inbox application can negotiate the encryption algorithm in case a recipient's certificate does not support the specified encryption algorithm. • 0 (POLICYVAL_SMIMEENCRIPTIONNEGOTIATION_NONE) does not allow negotiation. • 1 (POLICYVAL_SMIMEENCRIPTIONNEGOTIATION_ALLOWSTRONG) allows negotiation to a strong algorithm. • 2 (POLICYVAL_SMIMEENCRIPTIONNEGOTIATION_ALLOWALL) allows negotiation to any algorithm.
4145	SharePoint Access Policy SECPOLICY_SHAREPOINTUNCProtocolACCESS	This setting enables or disables Outlook Mobile SharePoint or UNC access through ActiveSync protocol to get documents. • 0 (POLICYVAL_SHAREPOINTUNCProtocolACCESS_DISALLOW) does not allow SharePoint or UNC file access. • 1 (POLICYVAL_SHAREPOINTUNCProtocolACCESS_ALLOW) allows Outlook Mobile to get documents on a corporate SharePoint site or UNC.
4146	Desktop Quick Connect	This setting specifies how device authentication is

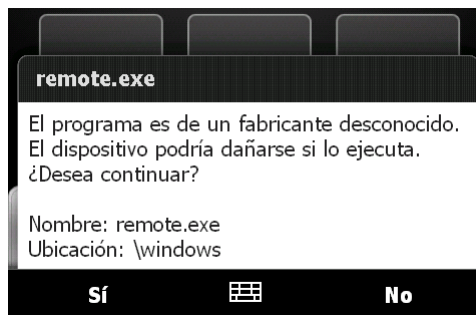
	Authentication Policy SECPOLICY_LASS_DESKTOP_QUICK_CONNECT	handled when connecting to the desktop.. • 0 (POLICYVAL_LASS_DESKTOP_QUICK_CONNECT_DISALLOWED) user must authenticate on the device upon connection, if the device lock is active. • 1 (POLICYVAL_LASS_DESKTOP_QUICK_CONNECT_ALLOWED) if user chooses quick connect, the desktop uniquely identifies the device and allows device to connect without requiring the user to manually unlock their device.
--	---	--

Más información, y en concreto los valores de los roles a aplicar como máscara en algunas de las políticas de seguridad, disponible en: <http://www.xs4all.nl/~itsme/projects/xda/smartphone-policies.html>.

8 APÉNDICE B: MYMOBILER

968. MyMobiler [Ref.- 41] es una aplicación de escritorio para Windows que permite visualizar la pantalla del dispositivo móvil desde un ordenador, siendo posible disponer de control completo del terminal desde el ordenador.
969. Adicionalmente al control del dispositivo móvil, MyMobiler también permite hacer uso del portapapeles entre el ordenador y el dispositivo móvil, capturar la pantalla del dispositivo móvil, grabar videos de las acciones que tienen lugar en el dispositivo móvil, intercambiar ficheros entre ambos equipos mediante las capacidades de arrastrar y soltar de Windows, gestionar los ficheros del dispositivo móvil a través de “Mobile Explorer”, o ejecutar comandos en el dispositivo móvil.
970. Debido a sus múltiples capacidades para la gestión del dispositivo móvil, se recomienda su utilización para la generación de documentación de seguridad, como por ejemplo, la presente guía.
971. MyMobiler puede hacer uso de una conexión ActiveSync entre el ordenador y el dispositivo móvil, y emplea conectividad TCP/IP para llevar a cabo sus acciones. La red empleada por la aplicación es la red privada 169.254.2.0/24 correspondiente a ActiveSync, y el puerto TCP empleado por defecto por la aplicación es el 1004.
972. En caso de no disponer de ActiveSync, MyMobiler puede establecer las conexiones entre el ordenador y el dispositivo móvil a través de cualquier red TCP/IP, como por ejemplo, una red inalámbrica Wi-Fi. En este escenario se recomienda establecer una contraseña en MyMobiler para la autenticación entre el ordenador y el dispositivo móvil.
973. La instalación de MyMobiler solicita autorización al usuario del dispositivo móvil para la ejecución de “remote.exe” a través del siguiente mensaje:

“El programa es de un fabricante desconocido. El dispositivo podría dañarse si lo ejecuta. ¿Desea continuar?”. Nombre: remote.exe; Ubicación: \windows”.



974. Este mensaje se muestra únicamente la primera vez que se accede a MyMobiler, proceso durante el cual se instala y copia la aplicación en “\Windows\remote.exe” dentro del dispositivo móvil (junto a un enlace en la lista de programas disponibles, “\Windows\Menú Inicio\Programas\My Mobiler.lnk”), siendo posible establecer la conexión directamente entre el ordenador y el dispositivo móvil en posteriores ocasiones sin que el usuario sea consultado de nuevo (ver descripción en el punto “163”).

9 REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:

Referencia	Título, autor y ubicación
[Ref.- 1]	“Guía CCN-STIC-450: Seguridad de dispositivos móviles”. CCN-CERT. 2010. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 2]	Updating your phone to Windows Mobile 6.5. Microsoft. URL: http://www.microsoft.com/windowsmobile/en-us/meet/wm65-upgrade.msp
[Ref.- 3]	Mobile phone match-up: How do the latest Windows Mobile 6.5 features compare to those of older versions?. Microsoft. URL: http://www.microsoft.com/windowsmobile/en-us/meet/version-compare.msp
[Ref.- 4]	Windows Marketplace for Mobile. Microsoft. URL: http://marketplace.windowsphone.com
[Ref.- 5]	Microsoft My Phone. URL: http://myphone.microsoft.com
[Ref.- 6]	HTC asistencia (España). URL: http://www.htc.com/es/support.aspx
[Ref.- 7]	HTC asistencia (España): HTC HD2. URL: http://www.htc.com/es/supportdownloadlist.aspx?p_id=297&act=sd&cat=all
[Ref.- 8]	Microsoft ActiveSync v4.5. URL: http://www.microsoft.com/windowsmobile/activesync/activesync45.msp
[Ref.- 9]	Centro de Dispositivos de Windows Mobile (Windows Mobile Device Center). Microsoft. URL: http://www.microsoft.com/windowsmobile/devicecenter.msp
[Ref.- 10]	Device Security Manager PowerToy for Windows Mobile 5.0. Microsoft. URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=7e92628c-d587-47e0-908b-09fee6ea517a&DisplayLang=en
[Ref.- 11]	Security Configuration Manager PowerToy for Windows Mobile. 2010. MSDN. Microsoft. URL: http://msdn.microsoft.com/en-us/library/bb158490.aspx
[Ref.- 12]	Standard Security Configurations. 2010. MSDN. Microsoft. URL: http://msdn.microsoft.com/en-us/library/bb158508.aspx
[Ref.- 13]	Windows Marketplace for Mobile & Mobile2Market Program. Microsoft. URL: http://msdn.microsoft.com/en-us/windowsmobile/dd569132.aspx
[Ref.- 14]	Windows Mobile 5.0 Application Security. Jason Fuller. Microsoft. Mayo 2005. URL: http://msdn.microsoft.com/en-us/library/ms839681
[Ref.- 15]	Security Policy Settings. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb416355.aspx
[Ref.- 16]	Windows Mobile Security Model. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb416353.aspx
[Ref.- 17]	Privileged APIs. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/aa919335.aspx
[Ref.- 18]	“Mobile Application Security”. Himanshu Dwivedi, Chris Clark, David Thiel. McGraw-Hill. ISBN: 0071633561. 2010. URL: http://www.mhprofessional.com/product.php?isbn=0071633561
[Ref.- 19]	“Certificate Management in Windows Mobile Devices”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb416317.aspx
[Ref.- 20]	“What's new in Windows Mobile 6.5.3”. Mary Jo Foley. ZDNet. Febrero 2010. URL: http://www.zdnet.com/blog/microsoft/whats-new-in-windows-mobile-653/5111
[Ref.- 21]	Security Roles. MSDN. Microsoft. 2010. URL: 1. http://msdn.microsoft.com/en-us/library/bb416273.aspx
[Ref.- 22]	Descargas de móviles. Windows Mobile. Microsoft. URL: http://www.microsoft.com/windowsmobile/es-es/downloads/default.msp

Referencia	Título, autor y ubicación
[Ref.- 23]	“Actualización del horario de verano en teléfonos con Windows Mobile” (Update your Windows phone for Daylight Saving Time). Windows Mobile. Microsoft. 2009. URL: http://www.microsoft.com/windowsmobile/es-es/downloads/microsoft/daylight-savings-update.msp (marzo de 2008) URL: http://www.microsoft.com/windowsmobile/en-us/downloads/microsoft/daylight-savings-update.msp (agosto de 2009)
[Ref.- 24]	“WebOS: Examples of SMS delivered injection flaws”. Intrepidus Group. April, 2010. URL: http://intrepidusgroup.com/insight/2010/04/webos-examples-of-sms-delivered-injection-flaws/ URL: http://intrepidusgroup.com/insight/webos/
[Ref.- 25]	“XSS and Content Injection in HTC Windows Mobile SMS Preview PopUp”. Michael Mueller. Abril, 2010. URL: http://www.securityfocus.com/archive/1/510897/30/0/threaded
[Ref.- 26]	ROM Upgrade for HTC HD2. HTC. 2010-01-22. (ROM version: 1.66.707.1) URL: http://www.htc.com/sea/SupportDownload.aspx?p_id=297&cat=2&dl_id=854
[Ref.- 27]	PHM Registry Editor. Philippe Majerus. (No disponible actualmente; Julio 2010) URL: http://www.phm.lu/downloads/download.aspx?{940B734A-C437-41C7-ADED-2A4418802FD3}
[Ref.- 28]	CeRegEditor. mdSoft. URL: http://ceregeditor.mdsoft.pl
[Ref.- 29]	“Guidelines for Creating Strong Passwords”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb416446.aspx
[Ref.- 30]	“Windows Mobile 6 Storage Card Encryption FAQ”. Scott Yost. Windows Mobile Team Blog. MSDN. 2007. URL: http://blogs.msdn.com/b/windowsmobile/archive/2007/03/26/windows-mobile-6-storage-card-encryption-faq.aspx
[Ref.- 31]	“New and Notable Features of Windows Mobile 6.5 and Microsoft Exchange Server 2010”. Microsoft Technet. 2010. URL: http://technet.microsoft.com/en-us/library/ff459601.aspx
[Ref.- 32]	Device Encryption. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb964600.aspx
[Ref.- 33]	DojoCrypt. Andreas Helland. 2008. URL: http://mobilitydojo.net/2008/09/16/windows-mobile-61-how-do-i-encrypt-my-device/ URL: http://mobilitydojo.net/2008/11/19/update-dojocrypt-goes-10/
[Ref.- 34]	“Features of Exchange Server 2007”. (Videos: Mobile Device Management in Exchange Server 2007 (y SP1)). Microsoft. URL: http://www.microsoft.com/exchange/2010/en/us/exchange-2007-features.aspx?pf=true
[Ref.- 35]	“Perform a Remote Wipe on a Mobile Phone” (MS Exchange 2010). Microsoft Technet. 2009. URL: http://technet.microsoft.com/en-us/library/aa998614.aspx
[Ref.- 36]	“New Client Access Features in Exchange 2007 SP1”. Microsoft Technet. 2008. URL: http://technet.microsoft.com/en-us/library/bb684907%28EXCHG.80%29.aspx
[Ref.- 37]	“View or Configure Exchange ActiveSync Mailbox Policy Properties” (Microsoft Exchange 2010). Microsoft Technet. 2010. URL: http://technet.microsoft.com/en-us/library/bb123994.aspx
[Ref.- 38]	(System Center) Mobile Device Manager 2008. Microsoft. URL: http://www.microsoft.com/windowsmobile/es-xl/business/solutions/enterprise/mobile-device-manager.msp
[Ref.- 39]	Exchange 2010. Microsoft. URL: http://www.microsoft.com/spain/exchange/default.msp
[Ref.- 40]	LASS Registry Settings. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/aa919751.aspx
[Ref.- 41]	MyMobiler. MTUX. 2010. URL: http://www.mymobiler.com
[Ref.- 42]	Remote Registry Editor. MSDN. Microsoft. URL: http://msdn.microsoft.com/en-us/library/ms894590.aspx

Referencia	Título, autor y ubicación
[Ref.- 43]	Signing and Checking Code with Authenticode. MSDN. Microsoft. URL: http://msdn.microsoft.com/en-us/library/ms537364%28VS.85%29.aspx
[Ref.- 44]	Additional Security Settings. MSDN. Microsoft. 2010. URL: http://technet.microsoft.com/en-us/library/cc182302.aspx
[Ref.- 45]	“SCMDM 2008 SP1 PIN Reset or Password Recovery Feature”. mnielsen. Enterprise Mobile. URL: http://blog.enterprisemobile.com/2009/01/scmdm-2008-sp1-pin-reset-or-password-recovery-feature/
[Ref.- 46]	“Managing your Active Sync Device from Outlook Web Access in Exchange 2007 SP1”. James Chen. The Microsoft Exchange Team Blog. URL: http://msexchangeteam.com/archive/2007/05/30/439568.aspx
[Ref.- 47]	“Update for HTC HD2 – New SMS Function Update” (en). HTC. URL: http://www.htc.com/www/SupportDownload.aspx?p_id=297&cat=0&dl_id=812
[Ref.- 48]	“Actualización para el HTC HD2 – Actualización de nueva función SMS” (es). HTC. URL: http://www.htc.com/es/SupportDownload.aspx?p_id=297&cat=0&dl_id=812
[Ref.- 49]	“Guía CCN-STIC-406; Seguridad en redes inalámbricas”. CCN-CERT. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 50]	“Description of the Wireless Client Update for Windows XP with Service Pack 2”. Microsoft. 2010. URL: http://support.microsoft.com/kb/917021
[Ref.- 51]	“Guía CCN-STIC-418; Seguridad en Bluetooth”. CCN-CERT. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 52]	“Modelo de seguridad de Bluetooth en Windows Mobile”. Alberto Moreno Tablado. Seguridad Mobile. 2009. URL: http://www.seguridadmobile.com/windows-mobile/seguridad-windows-mobile/seguridad-bluetooth.html
[Ref.- 53]	“Wi-Fi Registry Settings”. Windows Mobile 6.MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/ee495876.aspx
[Ref.- 54]	“Connection Manager Security”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb416530.aspx (security) URL: http://msdn.microsoft.com/en-us/library/bb416566.aspx (security levels)
[Ref.- 55]	“Connection Manager ActiveSync Desktop Pass-through (DTPT)”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/ee497235.aspx
[Ref.- 56]	“Introduction to Connection Manager”. Adam Dyba. MSDN Blogs. 2006. URL: http://blogs.msdn.com/b/cenet/archive/2006/06/06/620360.aspx
[Ref.- 57]	“Learn How to Find GPS Location on Any SmartPhone, and Then Make it Relevant”. Acoustic. 2009. URL: http://www.codeproject.com/KB/windows/DeepCast.aspx
[Ref.- 58]	“Services.exe Registry Settings”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/aa926416.aspx
[Ref.- 59]	“Authentication Services Registry Settings”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/aa922895.aspx
[Ref.- 60]	“TCP/IPv6 Configurable Registry Settings”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/aa915728.aspx URL: http://msdn.microsoft.com/en-us/library/aa916327.aspx
[Ref.- 61]	“TCP/IPv4 and TCP/IPv6 Common Registry Settings”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/aa915651.aspx
[Ref.- 62]	“Assigning an IPv4 Address to a Device”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/aa924135.aspx
[Ref.- 63]	“TCP/IPv4 Configurable Registry Settings”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/aa922356.aspx URL: http://msdn.microsoft.com/en-us/library/aa922329.aspx
[Ref.- 64]	“Connection Sharing Registry Settings”. MSDN. Microsoft. URL: http://msdn.microsoft.com/en-us/library/ms881495.aspx
[Ref.- 65]	“Why did we remove Bluetooth DUN?”. Windows Mobile Team Blog. 2007. URL: http://blogs.msdn.com/b/windowsmobile/archive/2007/04/17/why-did-we-remove-bluetooth-dun.aspx

Referencia	Título, autor y ubicación
[Ref.- 66]	“Automatic Client Configuration for IPv4”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/aa915613.aspx
[Ref.- 67]	“Configurar su cuenta Outlook del trabajo”. HTC. 2010. URL: http://www.htc.com/es/howto.aspx?p_id=297&id=179 URL: http://www.htc.com/es/howto.aspx?p_id=297&id=191
[Ref.- 68]	“Desktop Configuration Tool”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb737308.aspx URL: http://msdn.microsoft.com/en-us/library/bb737244.aspx
[Ref.- 69]	“Enabling Remote API (RAPI) Bootstrapping”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb737384.aspx
[Ref.- 70]	“OMA Client Provisioning”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb737289.aspx URL: http://msdn.microsoft.com/en-us/library/bb737572.aspx URL: http://msdn.microsoft.com/en-us/library/bb738068.aspx
[Ref.- 71]	“How to Change Security Policies”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb737407.aspx
[Ref.- 72]	“Microsoft Exchange Server ActiveSync Certificate-Based Authentication Tool”. (RapiConfig.exe). Microsoft. URL: http://www.microsoft.com/downloads/details.aspx?FamilyId=82510E18-7965-4883-A8C3-F73F1F4733AC&displaylang=en URL: http://technet.microsoft.com/en-us/library/bb508836%28EXCHG.65%29.aspx
[Ref.- 73]	“Conexiones de red: ¿Internet o Trabajo?”. igalan. 2008. URL: http://www.todopocketpc.com/wiki/Conexiones%20de%20red%20Internet%20o%20trabajo.ashx
[Ref.- 74]	“Connection Manager FAQ”. Chris De Herrera. Version 1.03 Revised 3/19/2009. URL: http://www.pocketpcfaq.com/faqs/connectionmanager.htm
[Ref.- 75]	“Installing certificates on Windows Mobile 6”. Jacco de Leeuw.2007. URL: http://www.jacco2.dds.nl/networking/windowsmobile-certinstall.html URL: http://www.jacco2.dds.nl/networking/p12imprt.html
[Ref.- 76]	“Secure e-mail with Windows Mobile 6”. Jacco de Leeuw.2008. URL: http://www.jacco2.dds.nl/networking/windowsmobile-smime.html
[Ref.- 77]	“Wi-Fi Configuration Service Provider”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/bb737539%28v=MSDN.10%29.aspx
[Ref.- 78]	“WMDC/ActiveSync Pass Through Features”. Windows Mobile Team Blog. 2006. URL: http://blogs.msdn.com/b/windowsmobile/archive/2006/11/20/wmdc-activesync-pass-through-feature.aspx
[Ref.- 79]	“Understanding Exchange ActiveSync Mailbox Policies”. Exchange Server 2010. 2010. URL: http://technet.microsoft.com/en-us/library/bb123484.aspx
[Ref.- 80]	“Security Considerations on the Exchange Server”. Microsoft TechNet. 2010. URL: http://technet.microsoft.com/en-us/library/cc182279.aspx
[Ref.- 81]	“Improve Security with Windows Mobile 6”. Matt Fontaine. Microsoft TechNet. 2008. URL: http://technet.microsoft.com/en-us/magazine/2007.07.mobile.aspx
[Ref.- 82]	“Security Considerations for Windows Mobile Messaging in the Enterprise”. Microsoft. 2007. URL: http://download.microsoft.com/download/c/b/d/cbdc18d1-1a01-4736-a557-08474ec73443/Windows_Mobile_Security_Considerations.doc
[Ref.- 83]	“Internet Explorer security zones registry entries for advanced users”. Microsoft. 2010. URL: http://support.microsoft.com/kb/182569
[Ref.- 84]	“Tutorial about Detecting User Agent Types and Client Device Capabilities”. Developer’s Home. URL: http://www.developershome.com/wap/detection/

Referencia	Título, autor y ubicación
[Ref.- 85]	“Guía CCN-STIC-502: Seguridad para aplicaciones cliente Windows. Navegador y correo electrónico”. CCN-CERT. 2010. “Guía CCN-STIC-502B: Seguridad para navegador y correo electrónico en Windows Vista”. CCN-CERT. 2010. “Guía CCN-STIC-519A: Seguridad para aplicaciones cliente Windows XP. Navegador y correo electrónico”. CCN-CERT. 2010. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 86]	“Developing Web Applications for Internet Explorer Mobile 6 on Windows Mobile 6.5”. MSDN. Microsoft. 2010. URL: http://msdn.microsoft.com/en-us/library/dd938878.aspx
[Ref.- 87]	“Version comparison”. FlashLite. Adobe. URL: http://www.adobe.com/uk/products/flashlite/version/
[Ref.- 88]	“How To: Add Windows Mobile 6 and Windows Mobile 6.1 Browser Definitions to ASP.NET”. Jim Wilson, JW Hedgehog, Inc. Microsoft. 2008. URL: http://msdn.microsoft.com/en-us/library/cc546461.aspx
[Ref.- 89]	“Security changes in Flash Player 8”. Deneb Meketa. Adobe Developer Connection. URL: http://www.adobe.com/devnet/flash/articles/fplayer8_security.html
[Ref.- 90]	“Adobe Announces Availability of Flash Player 10.1 for Mobile”. Adobe. Junio 2010. URL: http://www.adobe.com/aboutadobe/pressroom/pressreleases/201006/06222010FlashPlayerAvailability.html
[Ref.- 91]	“Supported Devices”. Flash Lite. Adobe. URL: http://www.adobe.com/mobile/supported_devices/
[Ref.- 92]	Adobe Reader LE. Adobe. URL: http://www.adobe.com/products/readerle/
[Ref.- 93]	“Cómo obtener Office Mobile 6.1”. Microsoft. URL: http://www.microsoft.com/windowsmobile/es-es/downloads/microsoft/buy-office-mobile.msp#x URL: http://www.microsoft.com/windowsmobile/es-es/downloads/microsoft/office-mobile-upgrade.msp#x?productid=830
[Ref.- 94]	“Microsoft Office Mobile 2010 (version 6.5)”. Microsoft Marketplace. URL: http://marketplace.windowsphone.com/details.aspx?appId=3c5f7fc0-313e-4518-8786-e13ca4873815
[Ref.- 95]	“.NET Compact Framework Service Pack 1 Redistributable”. Microsoft. 2006. URL: http://www.microsoft.com/downloads/details.aspx?familyid=0c1b0a88-59e2-4eba-a70e-4cd851c5fcc4&displaylang=en
[Ref.- 96]	“.NET Compact Framework Service Pack 2 Redistributable”. Microsoft. 2007. URL: http://www.microsoft.com/downloads/details.aspx?familyid=aea55f2f-07b5-4a8c-8a44-b4e1b196d5c0&displaylang=en
[Ref.- 97]	“.NET Compact Framework 3.5 Redistributable”. Microsoft. 2008. URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=e3821449-3c6b-42f1-9fd9-0041345b3385&displaylang=en
[Ref.- 98]	“HOWTO: Determining the .NET Compact Framework Version”. Neil Cowburn. 2007. URL: http://blog.opennetcf.com/ncowburn/2007/08/22/HOWTODeterminingTheNETCompactFrameworkVersion.aspx
[Ref.- 99]	“Power Toys for .NET Compact Framework 3.5”. Microsoft. 2007. URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=c8174c14-a27d-4148-bf01-86c2e0953eab&displaylang=en
[Ref.- 100]	“Manual Verification of SSL/TLS Certificate Trust Chains using Openssl (Part 1/2)”. Raul Siles. Taddong’s Security Blog. 2010. URL: http://blog.taddong.com/2010/04/manual-verification-of-ssl-tls.html
[Ref.- 101]	“How the Direct Push Technology Works”. Microsoft Technet. 2010. URL: http://technet.microsoft.com/en-us/library/cc182244.aspx
[Ref.- 102]	“Configuring Microsoft Exchange Direct Push technology”. Brien M. Posey. SearchExchange.com. 2007. (4 partes) URL: http://searchexchange.techtarget.com/generic/0,295582,sid43_gci1268251,00.html

Referencia	Título, autor y ubicación
[Ref.- 103]	“Implementing S/MIME for Windows Mobile”. Microsoft. 2007. URL: http://download.microsoft.com/download/1/a/9/1a9019c5-4fdb-4fab-a6f3-29e649558a93/Windows%20Mobile%20S/MIME%20Implementation%20Guide.pdf
[Ref.- 104]	“Provisioning for Windows Mobile-Based Devices”. MSDN. Microsoft. URL: http://msdn.microsoft.com/es-es/library/ms894922.aspx
[Ref.- 105]	“Making an AlwaysOn Data Connection”. MSDN. Microsoft. URL: http://msdn.microsoft.com/en-us/library/bb416388.aspx
[Ref.- 106]	“[TAD-2010-002] Vulnerability in the chatty Wi-Fi interface of Windows Mobile 6.5 & 6.1”. Raul Siles. Taddong. Septiembre 2010. URL: http://blog.taddong.com/2010/09/vulnerability-in-chatty-wi-fi-interface.html
[Ref.- 107]	“[TAD-2010-003] Vulnerability in the indiscreet Wi-Fi interface of Windows Mobile 6.5”. Raul Siles. Taddong. Septiembre 2010. URL: http://blog.taddong.com/2010/09/vulnerability-in-indiscreet-wi-fi.html
[Ref.- 108]	“Hacking Exposed Wireless”. 2 nd Edition. Johnny Cache, Joshua Wright, y Vincent Liu. 2010. Mc Graw Hill. ISBN: 978-0-07-166662-6. URL: http://www.hackingexposedwireless.com
[Ref.- 109]	“Microsoft Windows Mobile Overly Long Bluetooth Device Name Denial of Service Vulnerability”. Julien Bedard. Septiembre 2008. URL: http://www.securityfocus.com/bid/31420/
[Ref.- 110]	“[TAD-2011-001] Vulnerability in HTC Peep: Twitter Credentials Disclosure”. Raul Siles. Taddong. February 2011. URL: http://blog.taddong.com/2011/02/vulnerability-in-htc-peep-twitter.html