

**MANUAL DE INSTALACIÓN Y
CONFIGURACIÓN COMPLETO DE
MIPAGO MÓVIL**

Mobile Desktop versión 1.6.
10 de Agosto 2012

Índice

1. Introducción.....	3
2. Lectura de código de barras	4
2.1. Configuración en Panasonic CF-U1	4
2.2. Configuración en Panasonic CF-H1	4
3. Bluetooth.....	6
4. IEEE 802.11b/g (WiFi).....	11
5. 3G/HSDPA	14
5.1. Configuración común.....	14
5.2. Configuración específica en Panasonic CF-U1.....	18
5.3. Configuración específica en Panasonic CF-H1.....	18
6. Modo quiosco	19

1. Introducción

El presente documento detalla las exigencias técnicas de la implementación actual de MiPago Móvil con el fin de integrarse con los diferentes dispositivos integrados en el ordenador portátil.

La aplicación ha sido construida con la versión 2.0 del framework de .NET y se ha diseñado específicamente para dispositivos UMPC, de reducidas dimensiones, que integran diferentes módulos hardware de comunicaciones y captura de datos: lector de código de barras, comunicaciones por bluetooth, IEEE 802.11b/g, módem 3G/HSDPA, etc.

Los únicos requerimientos técnicos de la aplicación son la compatibilidad con la versión 2.0 de .NET, que el mismo programa de instalación de MiPago se encarga de copiar, una conexión a Internet y acceso a una impresora para generar los justificantes de pago. El resto de dispositivos, como el lector de códigos de barras o de tarjetas de banda magnética, son aconsejables pero no imprescindibles; no obstante, los UMPC Panasonic de la gama Toughbook, junto a la impresora Zebra RW420, que han servido de plataforma de ejecución para el prototipo actual, facilitan enormemente la captura de información con la integración en su propia carcasa de todo los dispositivos necesarios.

Por tanto, el objetivo de este documento es recoger de la forma más completa posible las configuraciones adicionales en librerías del sistema, plataformas, configuración interna del sistema operativo, etc. que deben efectuarse para disfrutar de la integración plena entre la aplicación y los dispositivos adicionales proporcionados por el propio UMPC.

2. Lectura de código de barras

En este apartado se detalla la configuración necesaria de los lectores de códigos de barras en los modelos Toughbook de Panasonic empleados en el prototipo.

2.1. Configuración en Panasonic CF-U1

La gestión del hardware lector es controlada por un programa residente, ubicado en %ProgramFiles%\Panasonic\BCR1D_Emu\BCR1D_EMU.EXE, que la aplicación se encarga de asegurar que se encuentre en ejecución y emplea para activar o desactivar el módulo. Para su correcta gestión es necesario efectuar la siguiente configuración:

1. Actualizar el driver del dispositivo para que el módulo se encuentre siempre activado, sin solicitar autorización previa al usuario. En realidad, el driver propiamente dicho es el programa anterior (BCR1D_Emu.exe), que debe sustituirse por la última versión.
2. Seleccionar, si fuese necesario, la opción "Allways on" a través del menú contextual ofrecido por el icono de código de barras de la barra de tareas.
3. Introducir en el registro de Windows la siguiente clave:

```
[HKEY_CURRENT_USER\Software\Panasonic\BCR2D_EMU]
```

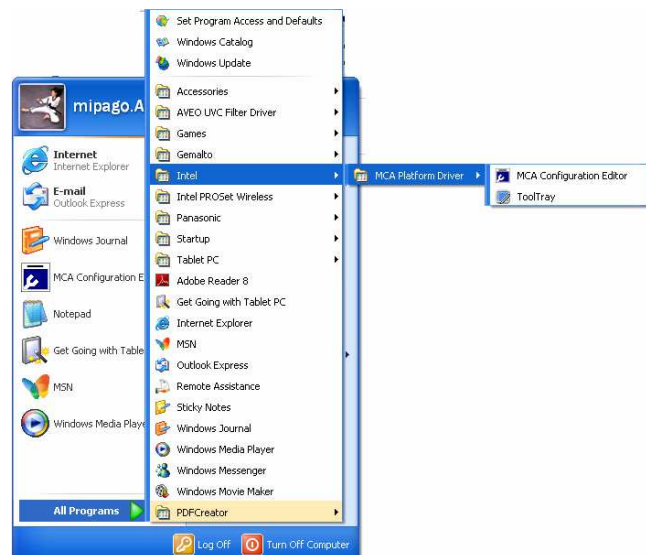
```
"AlwaysConnectStatus"=dword:00000001
```

4. Introducir en el registro de Windows la siguiente clave:
5. Asegurarse que se la opción para añadir la pulsación de ENTER al código capturado esté seleccionada.

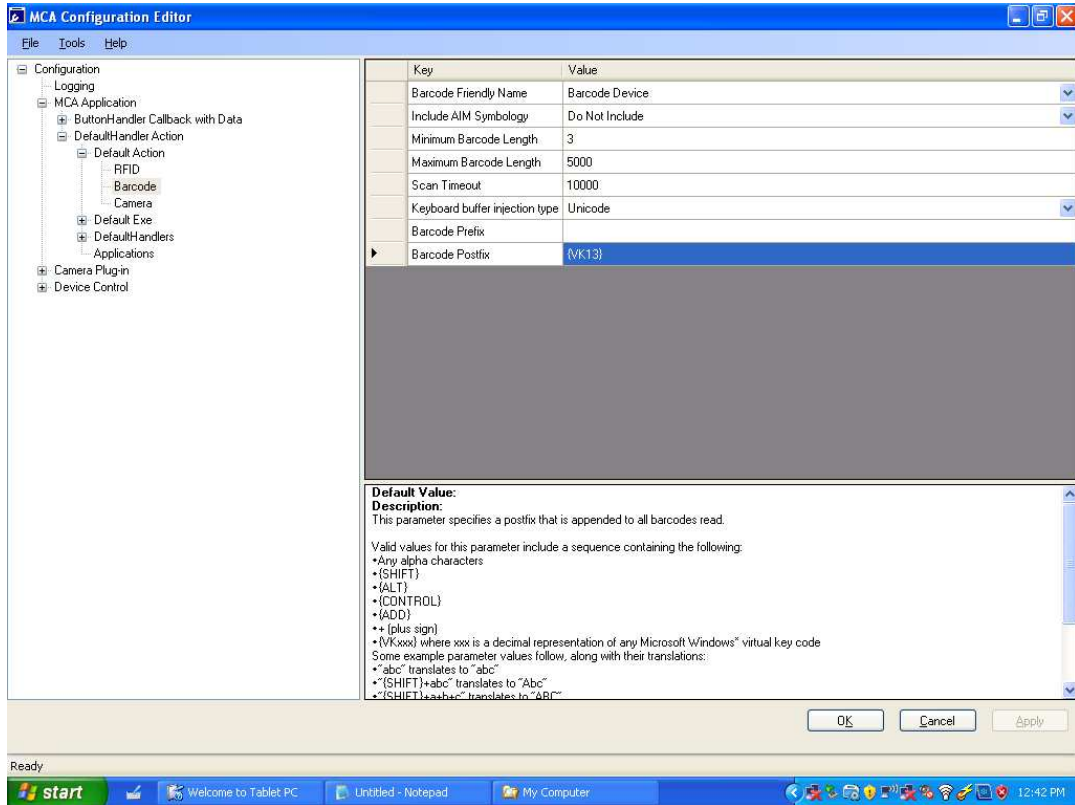
2.2. Configuración en Panasonic CF-H1

Este modelo está basado en la plataforma Intel® Mobile Clinical Assistant (MCA). Por tanto, existen diversas características del hardware que pueden gestionarse a través del editor de configuración de MCA:

1. Abrir el editor de configuración, **MCA Configuration Editor**, como se aprecia en la imagen.
2. Localizar las opciones de configuración del lector de código de barras en "Configuration > MCA Application > DefaultHandlerAction > Barcode". Debe editarse la opción "Barcode Postfix" para añadir las pulsaciones de teclado adicionales. Como se explica en el documento de soporte "CF-H1



Support_20090717.pdf” y en la propia ayuda del editor, los valores introducidos como prefijos o sufijos se codifican según las pulsaciones de teclado virtual de Microsoft (más información en <http://msdn.microsoft.com/en-us/library/ms645540%28VS.85%29.aspx>). En este caso, para añadir la pulsación de ENTER, deberíamos añadir la tecla 13, es decir, {VK13}:



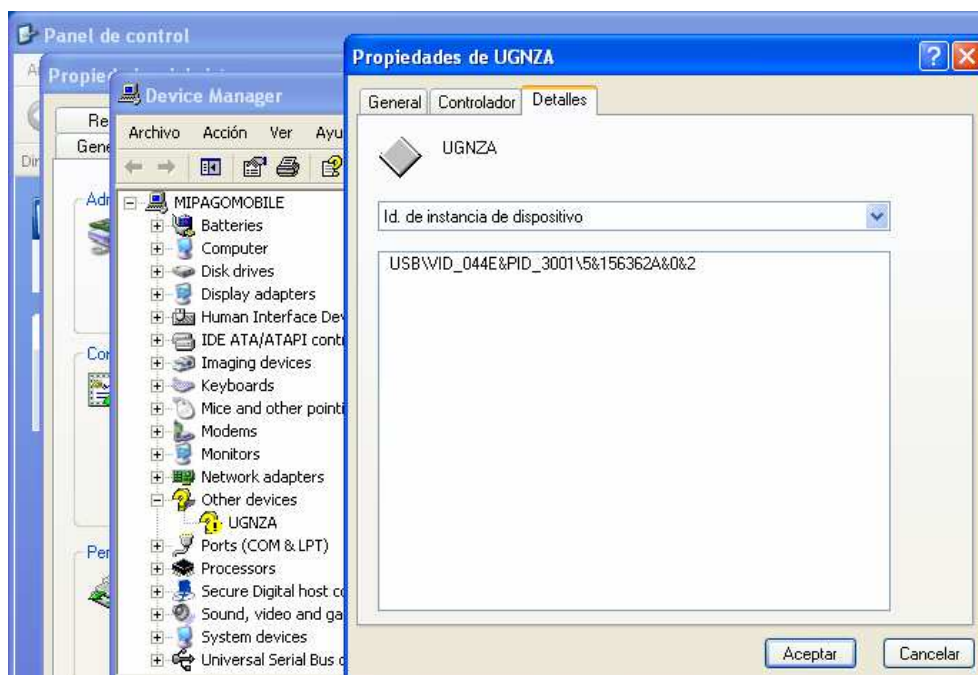
3. Bluetooth

La aplicación es capaz de gestionar la comunicación bluetooth desde dos puntos de vista: la activación y desactivación del hardware y el descubrimiento de servicios y vinculación de dispositivos.

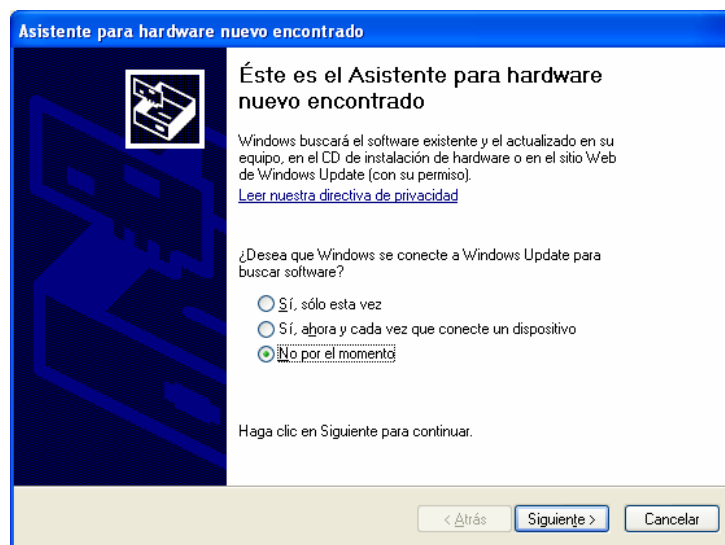
La versión actual mantiene una conexión abierta con la impresora Zebra RW-420, a través de un puerto serie COM virtual, ofrecido como servicio cliente por el propio dispositivo Panasonic; a través de esta comunicación se envían comandos CPCL a la impresora y se recoge la lectura de la banda magnética de las tarjetas. Por otra parte, el driver de impresión también tiene asociado un puerto COM para enviar a imprimir las solicitudes enviadas a la cola de impresión.

Los dispositivos bluetooth de los Toughbook vienen acompañados de la pila bluetooth de Toshiba, una de las mejores y más utilizadas en el mercado. No obstante, la librería gratuita 32feet.NET no soporta esta pila, siendo necesario instalar la pila estándar de Microsoft para acceder al hardware bluetooth. A continuación, se detallan el proceso necesario:

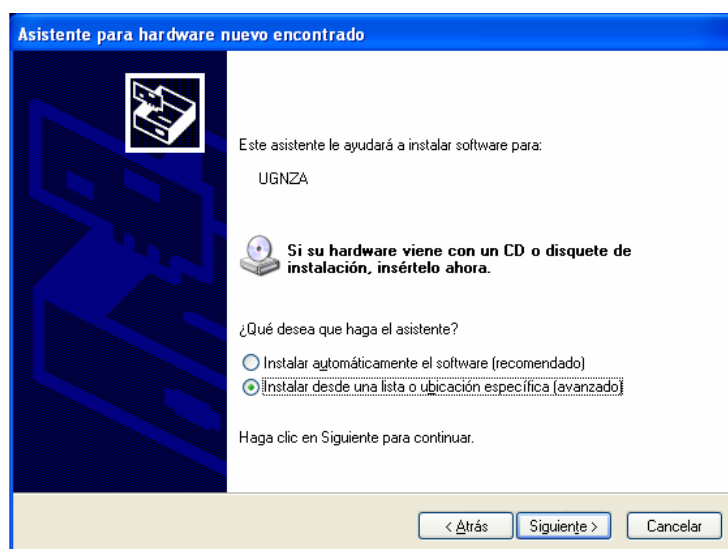
1. Desinstalar la pila bluetooth de Toshiba desde "Agregar o quitar programas".
2. Reiniciar el ordenador para que el sistema operativo detecte automáticamente el hardware bluetooth.
3. El hardware debería se detectado pero no se deberían haber encontrado los controladores apropiados. Ir al "Administrador de dispositivos" y copiar el identificador del hardware sin identificar ("Id. de instancia de dispositivo"):



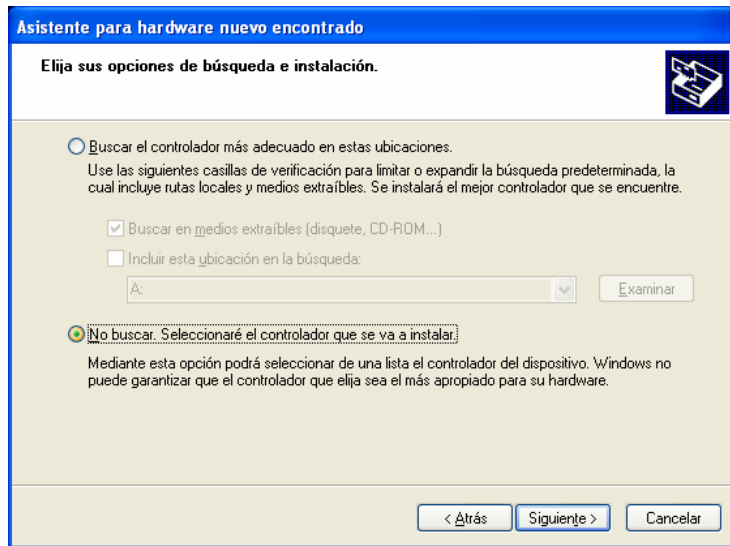
4. Localizar el fichero %WinDir%\inf\bth.inf (normalmente en C:\WINDOWS\inf\bth.inf). El fichero bth.inf contiene la información necesaria para instalar los dispositivos bluetooth compatibles con la pila de Microsoft.
5. Buscar por el término "Toshiba" para localizar otras entradas del fabricante y añadir según los anteriores un nuevo "TOSHIBA Bluetooth Adapter" utilizando el identificativo del hardware copiado anteriormente. Guardar el fichero bth.inf. En la siguiente captura se muestra el aspecto que podría tener el fichero después de la modificación:
6. Eliminar el dispositivo hardware del "Administrador de dispositivos" y se emplea la opción "Agregar hardware" o se intenta actualizar directamente el controlador del hardware desconocido:



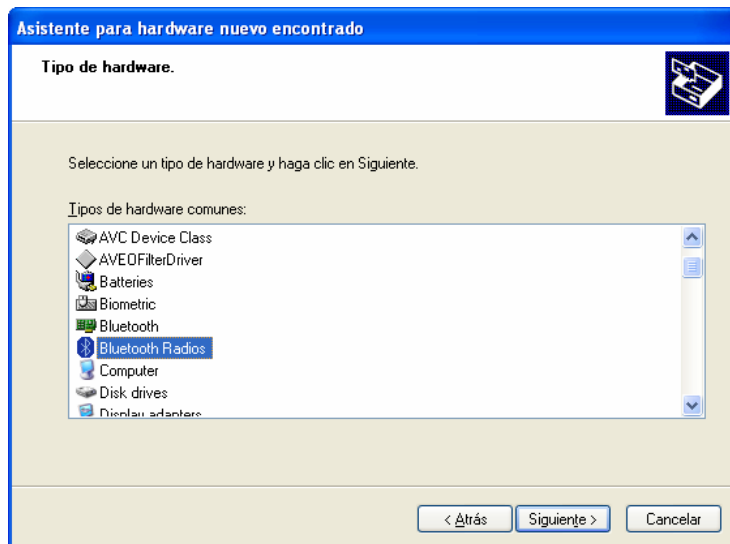
7. Seleccionar la opción de instalar el controlador desde una ubicación específica:



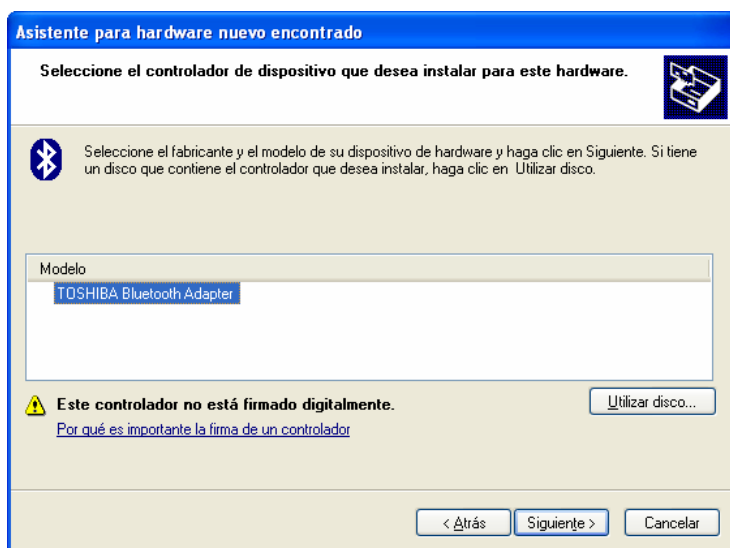
8. Seleccionar directamente el controlador que se va a instalar:



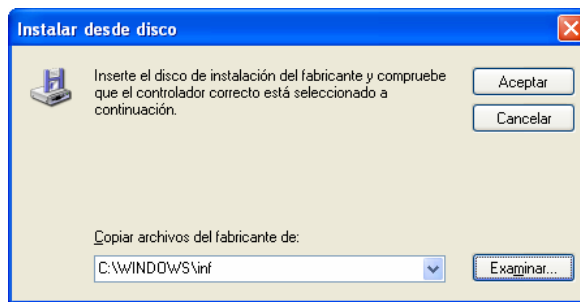
9. Seleccionar el tipo de hardware "Bluetooth Radios":



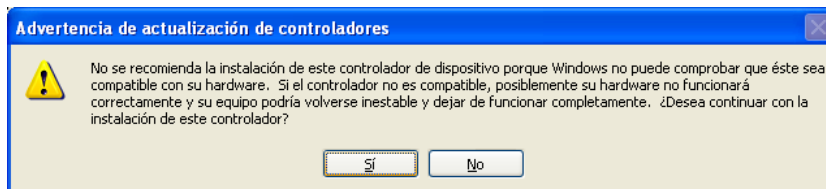
10. Continuar con el proceso seleccionado "Utilizar disco...":



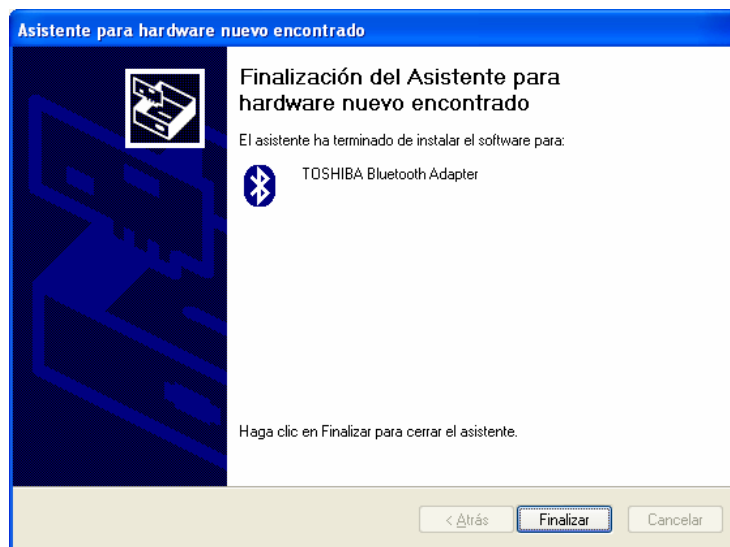
11. Seleccionar la ubicación del controlador bth.inf en %WinDir%\inf\
(normalmente en C:\WINDOWS\inf\):



12. Obviar los mensajes de advertencia y confirmar la instalación del controlador seleccionando "Sí":



13. Finalizar el proceso:



En la configuración de la aplicación es necesario indicar la dirección MAC de la impresora, así como el PIN que permite autenticar la conexión y establecer el vínculo. La propia aplicación se encarga de rastrear periódicamente los dispositivos bluetooth dentro de su radio de alcance, detectar los servicios ofrecidos, y en caso de no encontrarlo, volver a instalar el servicio puerto serie COM virtual.

La instalación de la pila Microsoft trae consigo ciertas limitaciones, como la imposibilidad de crear diversos puertos series virtuales sobre un mismo servicio. Como se ha comentado anteriormente, la aplicación exige una doble comunicación por puerto serie: para el control de la propia impresora y para que el driver de Zebra responda a las peticiones de la cola de impresión. Por ello, siempre que la aplicación precise imprimir es necesario cerrar la comunicación con el puerto serie del servicio bluetooth y reanudarlo una vez liberado por el driver de impresión.

Por otro lado, la aplicación también precisa un mayor control del hardware bluetooth del UMPC con el fin de activarlo y desactivarlo cuando resulte necesario o bajo petición para resolver posibles errores en la comunicación. Esta funcionalidad se

obtiene a partir del programa residente%ProgramFiles%\Panasonic\WSwitch\WSwitch.exe, que permite activar y desactivar los diferentes módulos de comunicación del UMPC.

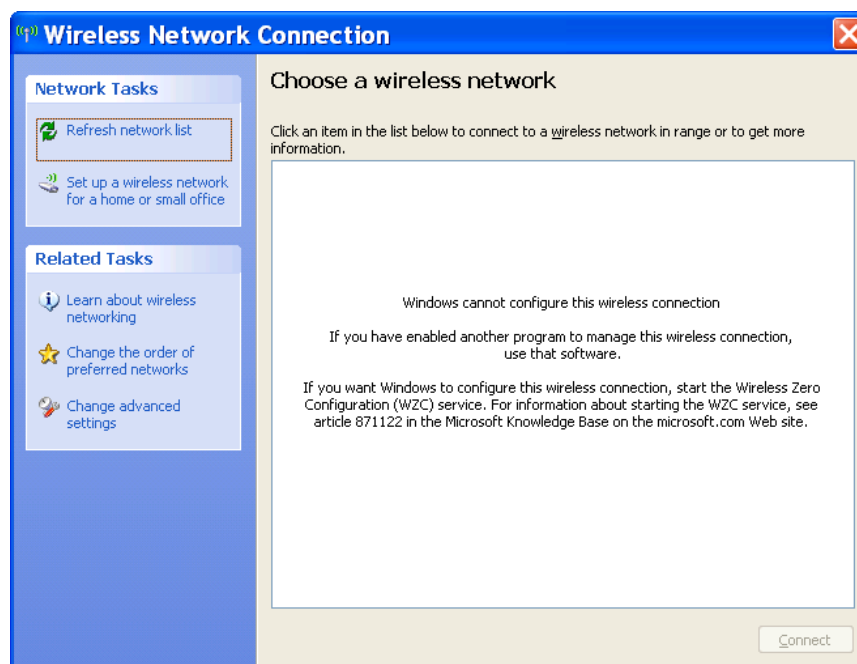
4. IEEE 802.11b/g (WiFi)

La aplicación gestiona la conexión inalámbrica IEEE 802.11b/g utilizando el API nativa WiFi de Windows, que se invoca desde el código gestionado de .NET a través del API de interoperabilidad.

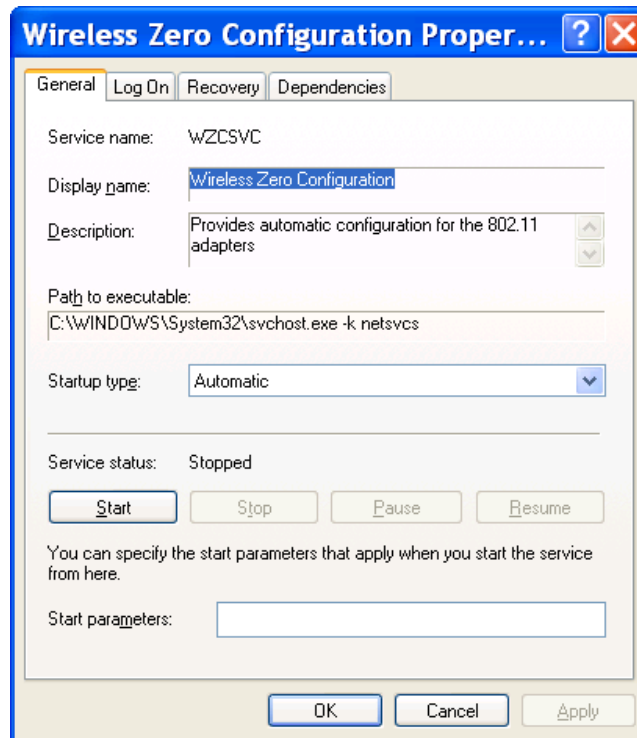
Por otra parte, el API nativa WiFi sólo puede utilizarse con el servicio de Windows **Wireless Zero Configuration** activo, que se encargará de gestionar la conectividad en vez de la aplicación específica del fabricante, como el gestor Wireless de Intel que acompaña a los ordenadores de la gama Toughbook.

A continuación, se detallan los pasos necesarios para posibilitar la gestión de la conexión IEEE 802.11b/g:

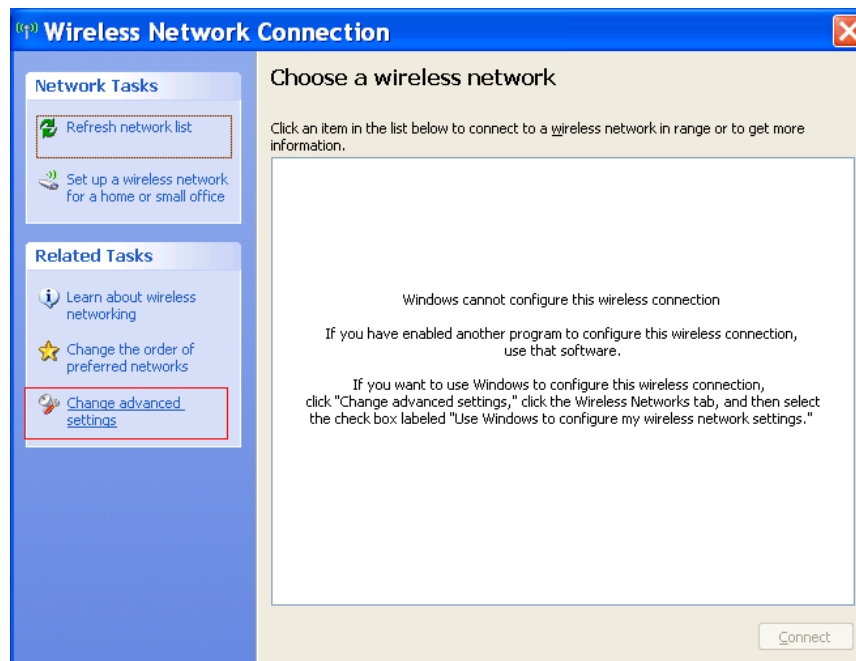
1. (Opcional si el sistema incluye la actualización). El API nativa WiFi puede instalarse en versiones genuinas de Windows XP Service Pack 2 y posteriores (para más información consultar <http://support.microsoft.com/kb/918997>). La librería puede descargarse desde aquí: <http://www.microsoft.com/downloads/details.aspx?displaylang=es&FamilyID=52a43bab-dc4e-413f-ac71-158efd1ada50>
2. Seleccionar "Ver redes inalámbricas disponibles" desde la conexión de red inalámbrica. Si existe algún programa gestor específico de esta conexión aparecerá una ventana similar a la siguiente:



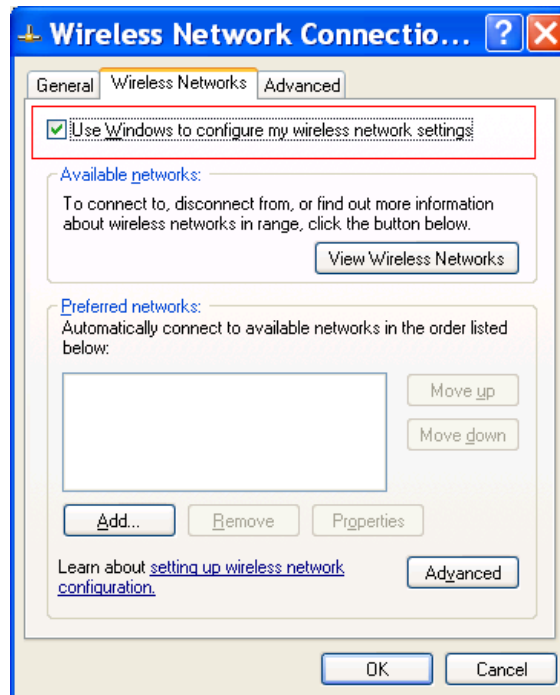
3. Arrancar el servicio WZC (Wireless Zero Configuration) de Windows desde la consola de servicios (services.msc). El servicio deberá activarse para todos los usuarios que vayan a hacer uso de la aplicación:



4. En la ventana anterior, de gestión de conexión a redes inalámbricas, acceder a la configuración avanzada, seleccionando "Change advanced settings"/"Cambiar configuración avanzada":



5. Seleccionar "Use Windows to configure my wireless network settings"/"Usar Windows para establecer mi configuración de red inalámbrica", para establecer el servicio WZC como responsable único de esta comunicación:



5. 3G/HSDPA

La gestión de la conexión Wireless WAN a través de un módem compatible con las redes 3G, HSDPA, GRPS, etc. se efectúa a través del programa Mwconn.

Mwconn es una potente utilidad gratuita, creada por Markus B. Weber, para gestionar la conexión a redes móviles. La aplicación es compatible con ciertas tarjetas internas y módems, encargándose tanto de inicializar el hardware como de controlar los procesos de conexión y desconexión, medir la velocidad de conexión, analizar las redes de comunicaciones, enviar y recibir SMS, etc.

La aplicación utiliza Mwconn con el propósito de activar el hardware interno de comunicaciones de la gama Toughbook y controlar la conexión y desconexión a las redes de telefonía móvil.

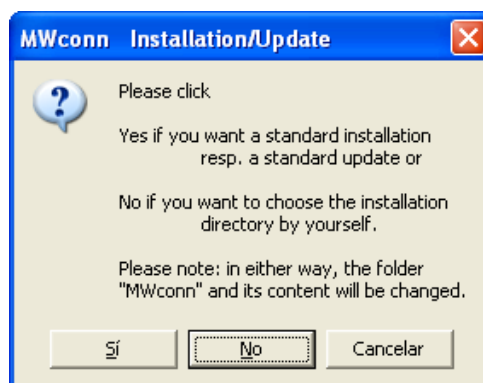
5.1. Configuración común

La configuración en ambos dispositivos es muy similar, a pesar de las diferencias en el hardware destinado a las comunicaciones: en el Panasonic CF-U1 el módem interno ha sido fabricado por Novatel Wireless, Inc., mientras que en el Panasonic CF-H1 procede del fabricante Qualcomm, Inc.

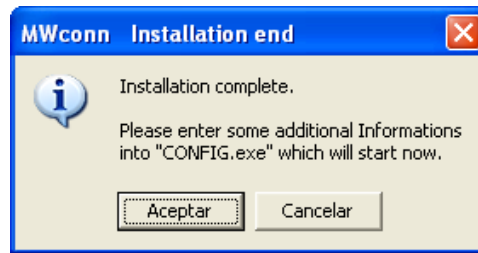
En la configuración por defecto, en el directorio de instalación de la aplicación, se crea el subdirectorio **mwconn** con los ficheros necesarios para instalar la utilidad Mwconn, así como los manuales de la misma.

El proceso común de instalación incluye los siguientes pasos:

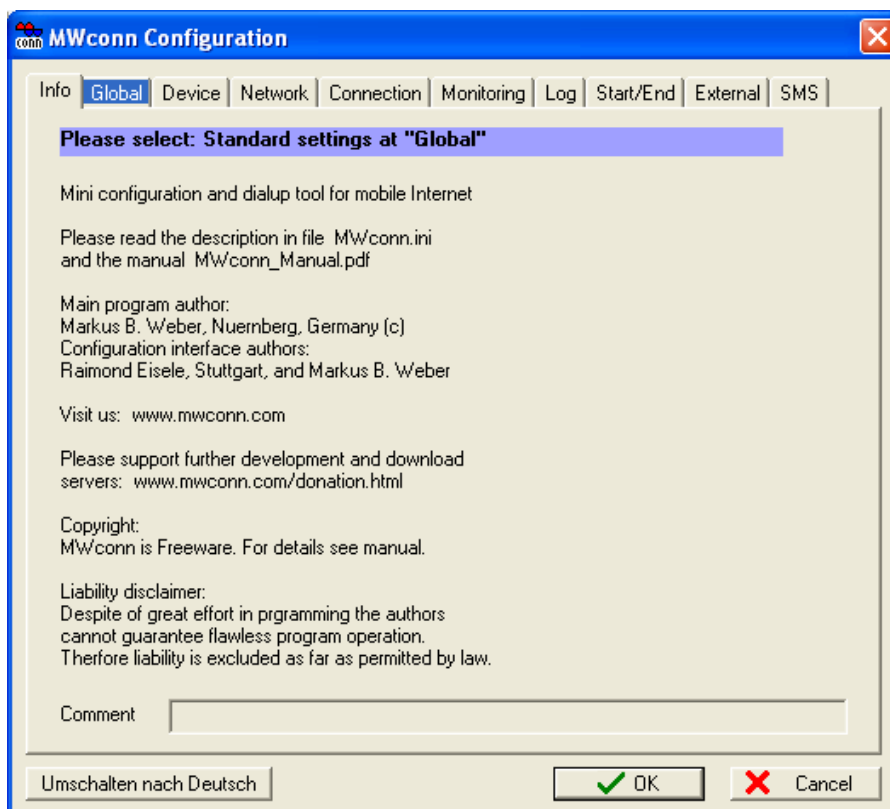
1. Ejecutar Mwconn.exe desde el directorio de instalación. Después de las pantallas de selección de idioma y presentación se mostrará el cuadro de diálogo de abajo:



2. Seleccionar "No", para la instalación personalizada, e indicar como directorio de instalación el de ubicación de Mwconn.exe. Una vez concluida la instalación se mostrará la siguiente ventana:



3. Seleccionar "Aceptar" para ejecutar el programa de configuración (CONFIG.exe), que se crea en el mismo directorio destino:

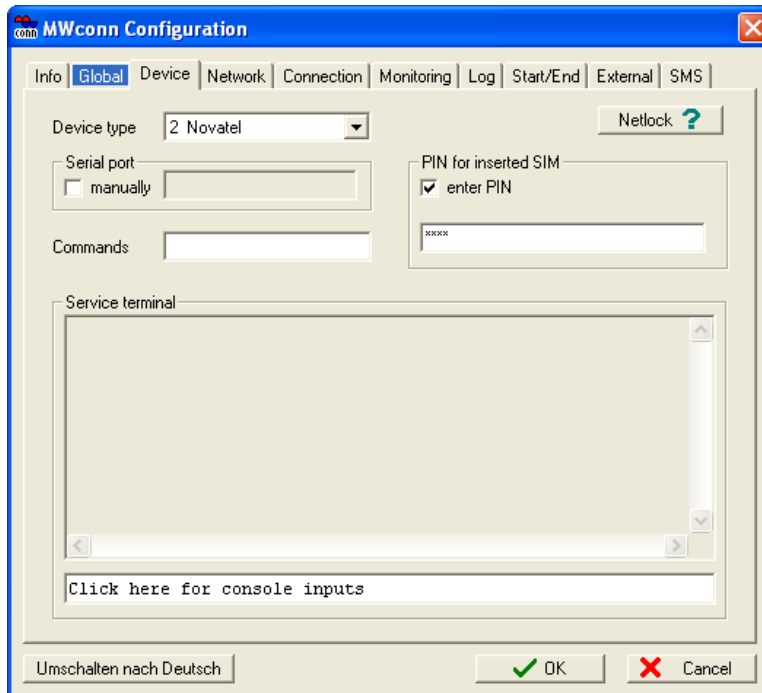


Con este programa se establecen los parámetros de funcionamiento de la red móvil. La configuración mínima requiere cumplimentar cierta información en las pestañas "Device" y "Network".

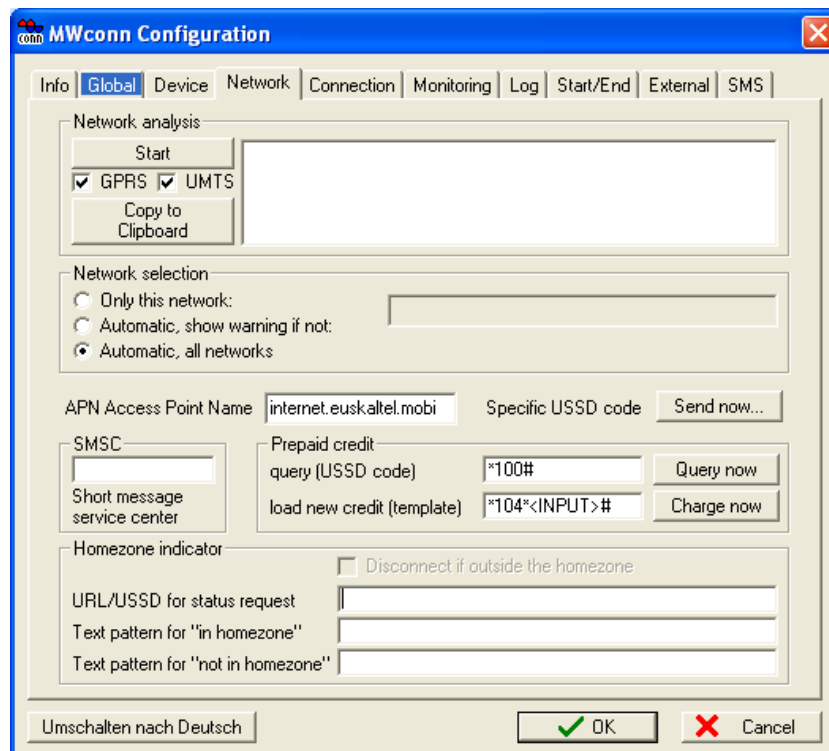
4. En la pestaña "Device" seleccionar el tipo de hardware del módem 3G interno: "Novatel" para el CF-U1 y "Qualcomm" para el CF-H1. No resulta imprescindible, pero también es posible indicar el puerto serie al que está conectado el módem en el campo de texto "Serial port" (seleccionado previamente "manually"), lo que puede acelerar el proceso de conexión.

En la sección "PIN for inserted SIM" introducir el PIN asociado a la tarjeta SIM actual, marcando previamente la casilla "enter PIN".

El aspecto final de la sección debería parecerse al mostrado en la siguiente ventana:



5. En la pestaña "Network" indicar los parámetros de conexión a la red de telefonía móvil, básicamente, el APN (Nombre del Punto de Acceso) en el campo "APN Access Point Name":



6. Pulsar sobre el botón "OK" en la parte inferior derecha de la ventana para cerrar el programa de configuración, que mostrará el siguiente cuadro de diálogo:



7. Seleccionar "Sí" para que el propio programa de configuración se encargue de crear una conexión llamada "Internet", imprescindible para la completa funcionalidad de Mwconn.
8. Por último, si el acceso al APN del proveedor de telefonía móvil requiere autenticación mediante usuario y contraseña editar el fichero de configuración de Mwconn para especificarlos. El fichero "Mwconn.ini", situado en el mismo directorio de instalación de la utilidad, es un fichero de configuración de texto tradicional, que puede abrirse con cualquier editor de textos como el mismo "Bloc de notas" de Windows. Buscar la sección "PASS" y añadir el usuario y contraseña con el siguiente formato "PASS=[#usuario#];[#contraseña#]", donde "[#usuario#]" y "[#contraseña#]" se corresponden respectivamente con el usuario y contraseña de identificación en el APN de la red móvil. Aunque estos parámetros se indiquen en texto plano, la aplicación se encargará de cifrarlos en la próxima ejecución:

```
Archivo Edición Formato Ver Ayuda
01 AAA000000000-000000000000-1000000000000000000000
02 (Please do not change line 01.)
03
04 --> If necessary, complete lines PIN and APN (see below)!
05 MWconn 5.5
06
07 LAN=English
08 COM=
09 DEV=
10 DEVI=
11 PIN=
12 NET=
13 APN=
14 PPQ=*100#
15 PPC=*104*<INPUT>#
16 CONA=SE
17 CON=Internet
18 PASS=[#usuario#];[#contraseña#]
19 DAY=
20 RND=1;1
21 MAXV=0;0;0
22 MAXT=0;0;0
23 HOMU=
24 HOMI=
25 HOMO=
26 ERR=NOC0 FRZ15 CRC50 TME10 ALG10 FRM10 BUF10 L4
27 PING=
28 SDLY=0
29 ENDM=0
30 ENDC=
31 END=0
```

5.2. Configuración específica en Panasonic CF-U1

El programa de instalación copia los ficheros necesarios para que funcione Mwconn en todos los modelos. Por ello, en el modelo Panasonic CF-U1 es necesario borrar dos ficheros que no son necesarios (sólo se emplean en los modelos equipados con módem de Qualcomm) que pueden ralentizar e incluso impedir el normal funcionamiento de la aplicación:

- MWconnQC.dll
- QCWWAN.dll

5.3. Configuración específica en Panasonic CF-H1

En este modelo no es necesario efectuar ninguna configuración adicional. Sólo en caso de no constar que MWconn no funciona correctamente, debe revisarse que en el directorio de instalación de Mwconn existan los siguientes ficheros:

- MWconnQC.dll
- QCWWAN.dll

En caso de no encontrarse o de haberlos borrado accidentalmente será necesario copiarlos de otro dispositivo o reinstalar la aplicación de pago móvil, repitiendo la configuración anterior.

6. Modo quiosco

El término de modo quiosco se refiere a aquella configuración del propio dispositivo de pago lo más restrictiva posible, en la que el usuario, por muy poco experimentado o malintencionado que sea, sólo tiene la posibilidad de hacer aquello que la aplicación le permita expresamente. Este tipo de configuraciones suele utilizarse con frecuencia en los ordenadores accesibles al público en general en diversos puntos de información, casi siempre se encuentran arrancados o sólo se encargan de visualizar datos en paneles informativos. Cualquier cambio de configuración, el uso de las combinaciones de teclado, el acceso al administrador de tareas o las opciones de apagado y cierre de sesión deben encontrarse perfectamente controladas.

En nuestro caso, el dispositivo de pago móvil cuenta con una configuración mínima de dos cuentas de usuario del sistema operativo. Uno de los usuarios debe ser el administrador de la aplicación y del dispositivo, mientras que el otro usuario es el que se empleará para acceder al modo quiosco propiamente dicho, desde el que deberá ejecutarse la aplicación. Si es necesario efectuar cualquier configuración, será el usuario administrador el que modifique los parámetros del sistema o de la aplicación y devuelva el control al usuario final.

La forma más sencilla de establecer las directivas de seguridad y diversas configuraciones para el usuario del modo quiosco es utilizar la herramienta Windows SteadyState, que simplifica enormemente este proceso en los sistemas operativos Windows XP y Windows Vista. Puede descargarse desde aquí, una vez superada la validación del sistema:

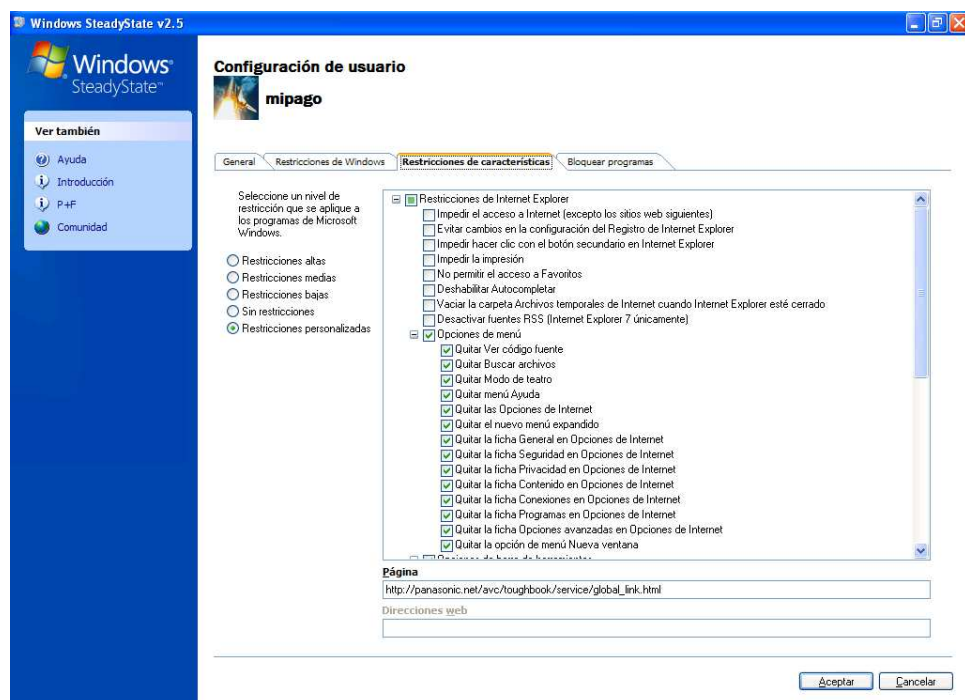
<http://www.microsoft.com/downloads/details.aspx?FamilyId=D077A52D-93E9-4B02-BD95-9D770CCDB431&displaylang=es>

A continuación, se detallan los pasos necesarios para crear el usuario del modo quiosco:

1. Crear el usuario como limitado (grupo "Usuarios" o "Users"), pero añadirlo temporalmente, para facilitar algunas configuraciones, al grupo de administración ("Administradores" o "Administrators").
2. Iniciar la sesión con el usuario anterior.
 1. Aprovechar a instalar, aunque se haya hecho para otros usuarios, el driver de la impresora Zebra, configurando adecuadamente el puerto serie empleado. Así mismo, deben considerarse los siguientes parámetros:
 - Configurar el tamaño por defecto del papel según los requerimientos de la aplicación (Ej: 4" X 6"/10,16 cm x 15,24 cm).
 - Establecer "Dispense Mode" en "None".
 - Establecer "Media Tracking" en "Continuous".
 - Establecer la impresora Zebra como impresora por defecto del usuario.
 2. Configurar el servicio de Windows para la gestión de la conexión WiFi (Wireless Zero Configuration), según se ha descrito en el apartado 4, centrándose exclusivamente en el servicio gestor de la conexión.
 3. Configurar el escritorio y la barra de tareas para eliminar aquellos accesos

no deseados. Por ejemplo, eliminar los accesos a Internet y al correo electrónico.

4. Configurar el lector de código de barras según se ha descrito en el apartado 2, centrándose exclusivamente en la parte relativa al registro de Windows, ya que estos parámetros son dependientes del usuario al residir en HKEY_CURRENT_USER.
 5. Ejecutar y probar la aplicación, incluyendo los procesos de lectura de códigos de barras, banda magnética, gestión de la conexión bluetooth, wireless o 3G, impresión en modo on-line y diferido, etc.
3. Cerrar la sesión del usuario del modo quiosco e iniciarla con el usuario administrador.
 4. Quitar al usuario anterior del grupo de administradores.
 5. Ejecutar Windows SteadyState para facilitar la configuración del usuario anterior. A continuación, aplicar todas las restricciones en lo referente a permisos del sistema operativo y el acceso a unidades de disco excepto lo que se indique aquí expresamente:
 1. Aplicar todas las restricciones de la pestaña "Restricciones de Windows" excepto las referentes al menú de inicio clásico (desmarcar "Allow only the classic Start Menu") y a suprimir el botón de apagar (desmarcar "Remove the Shut Down button"). Seleccionar todas las unidades de disco para bloquear su acceso.
 2. En la pestaña "Restricciones de características" seleccionar todas las opciones referentes a "Opciones de menú" pero desmarcar las primeras opciones de Internet Explorer, para que la aplicación pueda descargarse las imágenes correspondientes en la elaboración de los informes:



3. Adicionalmente, puede optarse por bloquear explícitamente ciertos programas en la pestaña "Bloquear programas".

6. Acceder al registro de Windows (regedit.exe) para configurar el acceso del usuario a ciertas claves globales del ordenador (HKEY_LOCAL_MACHINE). Otorgar permisos de lectura y escritura a las siguientes claves:
 - HKLM_SOFTWARE>Panasonic>WSwitch
7. Conceder permisos de lectura y escritura, recursivamente, a todos los directorios ubicados dentro de la ruta de instalación de la aplicación, para posibilitar la escritura de logs, ficheros temporales, etc.
8. Eliminar el acceso a la opción "Todos los programas/All Programs" del menú de inicio. Para ello, ejecutar el editor de las directivas de grupo (gpedit.msc) y seguir las instrucciones descritas en <http://support.microsoft.com/kb/293655/es>:
 1. Ejecutar la consola de las directivas de grupo (gpedit.msc) y activar la restricción "Administrative Templates > Start Menu and Taskbar > Remove All Programs list from the Start Menu".
 2. Cerrar la sesión del usuario administrador y acceder con el usuario limitado. Comprobar que la opción de "Todos los programas/All Programs" ha desaparecido. Cerrar la sesión y volver a acceder como administrador.
 3. Hacer una copia de seguridad del fichero "%Systemroot%\System32\GroupPolicy\User\Registry.pol".
 4. Acceder nuevamente a la consola de las directivas de grupo y desactivar la directiva anterior. Cerrar esta consola de administración.
 5. Comprobar que la opción de "Todos los programas/All Programs" aparece en el usuario administrador. Volver a restaurar el fichero Registry.pol a partir de la copia de seguridad anterior.
9. Añadir un script de arranque al usuario del modo quiosco, copiando un acceso directo al script "p12Script\launch.vbs" en la carpeta "Inicio/Startup" del perfil correspondiente. El script anterior lanza a ejecutar la aplicación y cierra la sesión cuando el usuario sale de la misma. Es fundamental que el acceso directo al script no modifique la carpeta de trabajo de la aplicación, que siempre debe coincidir con el directorio de instalación.
- 10.
11. Adicionalmente, puede ser necesario cambiar las opciones de seguridad local, para permitir que aparezca el botón de apagado en la ventana de login y apagar el equipo sin necesidad de haber iniciado la sesión:
 1. Ejecutar la consola de las políticas de seguridad locales (secpol.msc).
 2. Expandir la sección "Local Policies" y seleccionar "Security Options"
 3. En el panel derecho, localizar la entrada "Shutdown: Allow system to be shut down without having to log on" y habilitarla, como se muestra en la siguiente captura:

