ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

ÍNDICE DE DIAGRAMAS

No existe contenido en esta sección.

Esta página se deja deliberadamente en blanco.

ÍNDICE DE CÓDIGO

No existe contenido en esta sección.

Esta página se deja deliberadamente en blanco.

RESUMEN

El presente trabajo pretende ser guía de referencia y aportar soluciones a problemáticas que se presentan al diseñar una solución móvil profesional basada en terminales portátiles. Se aborda toda la normativa y estándares que afectan a este tipo de dispositivos y se exponen las diferentes tecnologías presentes en los mismos.

En diferentes apartados, se identifican los requerimientos, se definen criterios de diseño para la solución global, ayudando a seleccionar los componentes hardware / software. Se expone la forma de implementar las comunicaciones de datos entre los dispositivos y los servicios centrales de la empresa de forma eficiente.

Palabras Clave: mobile computers, windows ce, rugged handhelds, windows mobile, terminales portátiles

SUMMARY

The present work tries to serve as a reference guide and provide solutions to problems that arise while designing a professional mobile solution based on handheld devices. All the standards and regulations affecting this kind of devices are covered, detailing different technologies available in these equipments.

In different sections, we identify the requirements and define the criteria for designing the global solution, helping to choose the hardware and software components. It is also shown the way to implement the data communications between mobile devices and the central corporate services in a secure and efficient manner.

Keywords: mobile computers, windows ce, rugged handhelds, windows mobile, terminales portátiles

RESUMEN EXTENDIDO

El presente trabajo se ha centrado en la gama de terminales portátiles que puede llevar un usuario como equipo de mano, y no se ha contemplado otros equipos embarcables o acoplables a vehículos, carretillas u otros entornos. Digamos que las soluciones móviles objetivo del estudio del presente trabajo son aquellas cuyo usuario final dispone de un terminal portátil en su mano, ya sea de forma permanente o esporádica.

La exposición de temas parte del mismo punto inicial que se encontraría el diseñador de una solución móvil para un entorno profesional y, se avanza a lo largo de las etapas necesarias hasta llegar al despliegue final de la solución. Se pasa por todos esos puntos relevantes en el mismo orden que se los encontraría el diseñador de la solución, empezando por la recogida de requerimientos y selección de los terminales portátiles y finalizando con las pruebas piloto y el despliegue a gran escala de la solución.

Como guía de referencia, este trabajo pretende dar un enfoque eminentemente realista, intentando mostrar los conceptos que dan lugar a decisiones importantes en el diseño de la solución y dejando de lado detalles específicos de programación o configuración software.

En ningún momento se intenta enseñar en profundidad todos y cada uno de los pasos necesarios en un proyecto de este tipo, sino más bien se intenta centrar en aquellos aspectos que son diferentes de un proyecto convencional no basado en terminales portátiles.

A lo largo de todo el trabajo se hace referencia a gran cantidad de estándares o directivas, los cuales cada uno de ellos ya sería motivo de todo un trabajo monográfico al respecto. Ahí es donde se muestra un resumen muy seleccionado de aquellos apartados de las normativas o estándares que son especialmente relevantes para el diseño de la solución y que el diseñador de la solución móvil deberá tener en cuenta.

En muchos apartados se intenta que el lector pueda llegar a conclusiones rápidas sin tener que estudiar y dominar todos los pormenores, análisis técnicos y experiencias previas que dan lugar a esas decisiones de diseño, y que en algunos casos, podría salir del alcance del presente trabajo y ser un trabajo diferente en sí mismo.

Un ejemplo claro de este tipo de enfoque es el apartado de seguridad en las comunicaciones. En ese apartado se ha intentado resumir las tecnologías de control de acceso y autenticación disponibles actualmente y, en base a unos criterios de exclusión y selección, se presenta un conjunto reducido de alternativas para la solución móvil en nuestro entorno de red inalámbrico. Así pues, el lector no tendrá que navegar sobre multitud de estándares, entender decenas de posibilidades y algoritmos, o evaluar todas las problemáticas para elegir su alternativa idónea. Simplemente se exponen de forma resumida y razonada los motivos que llevan a esa elección para que el lector entienda las razones subyacentes a la hora de tomar esa decisión de diseño en la arquitectura de su solución móvil profesional basada en terminales portátiles.

Como las soluciones móviles basadas en terminales portátiles que son el objeto de estudio del presente trabajo estarán destinadas en muchos casos a entornos especiales, como pueden ser

aplicaciones industriales, aplicaciones en ambientes sucios, con exposición a golpes y agua, e incluso atmósferas explosivas, se han tratado todos esos temas de forma concisa, poniendo el foco en aquellos detalles que atañen al diseñador de la solución.

Como en otras áreas cubiertas en el trabajo, estos entornos especiales están regulados por multitud de normativas y estándares, a los cuales se hará referencia, pero simplemente para exponer aquello que se considera necesario y relevante, ya que entrar en el estudio detallado de cada estándar o normativa estaría fuera del alcance del presente libro y se desviaría de los propósitos de este trabajo. Aún así, se hace un resumen interesante y concreto de aquellos aspectos de esas normativas que sí son relevantes y se deberán tener en cuenta en el diseño de la solución.

Otro área importante que se cubre es aquella concerniente a las diferentes tecnologías que pueden estar presentes en un terminal portátil y que pueden ser de utilidad en el diseño de la solución. Igual que en otros apartados, cualquier tecnología expuesta podría ser objeto de un extenso trabajo monográfico que estaría fuera del alcance de este libro. Por el contrario, lo que se ha pretendido es mostrar que tecnologías pueden estar presentes en nuestros terminales portátiles y de que forma se pueden emplear en el diseño de una solución, sin entrar en profundos detalles técnicos de programación o configuración. Se ha intentado sin embargo, resumir en cierta medida las características principales de tecnologías como los lectores de códigos de barras, tarjetas inteligentes, bandas magnéticas y otros, ya que no se encuentran presentes en otro tipo de equipamientos informáticos de uso general como por ejemplo un ordenador portátil.

En algunos apartados se aportan tablas o listas de selección que ayudarán a elegir un determinado terminal portátil en base a unos criterios de selección determinados como puede ser la protección ante impactos y vibraciones, la disponibilidad de una determinada tecnología, o el cumplimiento de una determinada directiva o estándar.

En definitiva, el presente trabajo, pretende ser de ayuda para quienes se enfrenten a sus primeros proyectos con terminales portátiles y sean responsables del diseño global de la solución.

MEMORIA

1.- INTRODUCCIÓN

El presente trabajo pretende ser un estudio detallado sobre las diferentes tecnologías utilizadas en la elaboración de soluciones móviles profesionales involucrando terminales portátiles y, al mismo tiempo, aportar las claves técnicas para su empleo eficaz y exitoso en el diseño, desarrollo e implementación de una solución completa en áreas como logística, transporte, fuerzas de venta, e industria, entre otras.

Es prácticamente inexistente la literatura específica para el diseño de este tipo de soluciones, que abarque todas las tecnologías y herramientas que son necesarias para el diseño, desarrollo e implementación de principio a fin. Existen libros dedicados, por ejemplo, a Windows Mobile como sistema operativo para dispositivos portátiles, libros que se centran en comunicaciones Wi-Fi, GPS y otras tecnologías, pero no existe una referencia completa que las aglutine y las enfoque en el diseño y desarrollo completo de este tipo de soluciones específicas para un entorno profesional y que además abarque las problemáticas que se presentan en el diseño, desarrollo e implementación con este tipo de dispositivos en dichos entornos.

El estudio a realizar podrá servir de guía de referencia para cualquier ingeniero o diseñador de sistemas informáticos que desee diseñar e implementar una solución completa para un entorno profesional (no para usuarios domésticos que utilizan smartphones) utilizando terminales portátiles. Un ejemplo claro de una de estas soluciones, podría ser la automatización de una fuerza de reparto en una empresa de transportes o mensajería. En este tipo de soluciones, se vuelve necesario controlar todo el proceso de gestión de paquetes, implementar la trazabilidad mediante códigos de barras, etiquetas electrónicas o cualquier otro medio, gestionar las comunicaciones de datos, ya sea en lotes o en tiempo real, controlar la posición y/o ubicación del usuario, gestionar las rutas, y otros aspectos.

Dado que muchas de estas soluciones deben ser implementadas en entornos exigentes, se tendrán en cuenta los criterios para seleccionar equipos que cumplan estas exigencias, es decir, entornos en los que los dispositivos estarán sometidos a condiciones de iluminación deficiente o excesiva, temperaturas de trabajo extremas, polvo o humedad excesivos., incluso lluvia o salpicaduras de agua. Todos estos aspectos, aparte del uso intensivo por parte del usuario final, deben ser contemplados en una solución profesional mediante dispositivos portátiles, y que sin embargo, es obviada en las soluciones destinadas al usuario de otros dispositivos como los smartphones.

2.- DISEÑO DE LA SOLUCIÓN

Es conveniente seguir unas determinadas pautas a la hora de diseñar, desarrollar y poner en marcha una solución basada en terminales portátiles. Las características de los entornos en los que van a trabajar los terminales portátiles, el hecho de que sean dispositivos y las características del usuario con el que van a tener que interaccionar (a menudo sin conocimientos informáticos y en actividades poco amigables), hacen que se tengan que añadir elementos de control y verificación adicionales a lo largo del proyecto.

En la gráfica siguiente se puede apreciar como serían las diferentes fases de una solución basada en terminales portátiles hasta el momento final de su implantación definitiva.

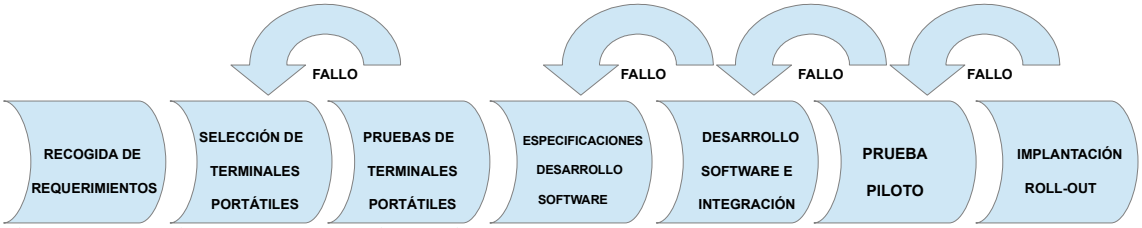

Ilustración 1: Etapas de un proyecto con terminales portátiles

Se debería resaltar tres fases especialmente importantes y que se diferencian de un proyecto informático convencional:

- Selección de Terminales Portátiles
- Pruebas de Terminales Portátiles
- Prueba Piloto

3.- RECOGIDA DE REQUERIMIENTOS

Esta fase es muy similar a la de cualquier otro proyecto informático, aunque con ciertas peculiaridades que deberán ser tenidas en cuenta.

- Condiciones Ambientales
    - Además de todos los requerimientos funcionales propios de una solución informática, se deberá recabar toda la información posible sobre las condiciones ambientales del entorno en el que va a ser implantada la solución final con terminales portátiles.
- Condiciones de uso
    - A diferencia de cualquier proyecto informático en el que considerasen usuarios con un determinado nivel mínimo exigible de conocimientos informáticos y un cierto trato apropiado a los equipos, en este tipo de soluciones, alguna o todas estas premisas pueden no cumplirse.

3.1.- Condiciones ambientales

Aquellas condiciones a las que se podrán exponer los terminales portátiles en su entorno de aplicación. Dentro de este apartado se deberá recabar la siguiente información:

- Temperatura máxima y mínima de operación
- Humedad relativa máxima y mínima
- Presencia o no de agua
- Presencia o no de partículas sólidas en suspensión
- Posibilidad de descargas electrostáticas
- Posibilidad de shock térmico

En el supuesto caso de que algunos de estos datos no fuesen facilitados, habría que tomar medidas in-situ en el lugar objetivo de nuestra solución. Por poner un ejemplo, si no se está seguro de las temperaturas máximas y mínimas a las que se tendrá que someter los equipos, y no existiesen registros de esas temperaturas, habría que hacer mediciones en el entorno durante todo el periodo de la jornada de trabajo habitual a la que se vería expuesto uno de los equipos. Por ejemplo de una planta metalúrgica a diferentes horas y en diferentes zonas de operación.

3.2.- Condiciones de uso

Aquí se deberá recoger todos los datos que dependen de la interacción con el usuario final y que serían los siguientes:

- Requerimientos ergonómicos
- Posibilidad de impactos, caídas y vibraciones

4.- SELECCIÓN DE TERMINALES PORTÁTILES

En el apartado anterior se deberían haber recogido los requerimientos ambientales y de uso de la solución, los cuales serán vitales en el apartado de selección de terminales portátiles.

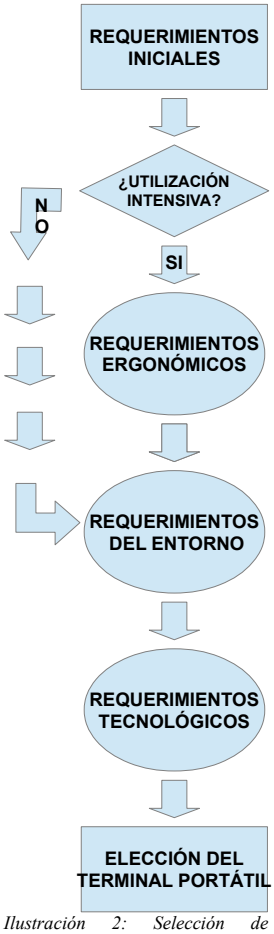

Ilustración 2: Selección de Terminales Portátiles

Como se puede ver en la imagen, se tendrán unos requerimientos iniciales para nuestra solución móvil, los cuales servirán de base para el proceso de selección de los terminales a emplear en la solución.

El primer punto que se deberá determinar es si nuestra solución es de utilización intensiva y, si por lo tanto, se tienen requerimientos especiales en materia de ergonomía.

Esto es así, porque una aplicación que esté pensada para hacer captura intensiva de datos con un terminal portátil siendo sujetado durante horas por el usuario, requerirá un estudio ergonómico.

De este estudio, se obtendrán dos elementos claves para la selección del terminal portátil:

- Factor de forma (Tableta, handheld, pistola, ...)
- Peso máximo del terminal
- Período máximo de utilización ininterrumpida
- Períodos de descanso recomendados

A partir de aquí, se aplicarán los requerimientos del entorno y tecnológicos para seleccionar los terminales portátiles que podrían ser aplicables en nuestra solución móvil.

De esta selección final de equipos se tendrán que elegir los más idóneos en base a otros criterios específicos de la solución y, que posteriormente se verificarán con una etapa de pruebas específicas para dichos terminales.

4.1.- Selección de Terminales Portátiles por criterios ergonómicos

Cuando se trata con actividades de uso intensivo de terminales portátiles, uno de los puntos fundamentales en el diseño de la solución mediante estos dispositivos es la identificación del factor ergonómico idóneo que requerirá el usuario final.

Ilustración 3: Ergonomía: Terminal Portátil con empuñadura y disparador

← La ilustración (3)[1] muestra un terminal portátil tipo pistola

A menudo se ven usuarios que, con un terminal portátil en su mano (por ejemplo en un supermercado), sujetan un dispositivo tipo tableta mientras efectúan labores repetitivas sobre el mismo durante periodos prolongados y, este sería un ejemplo de solución móvil mal diseñada desde el punto de vista ergonómico.

Pongamos por ejemplo el caso anterior, el empleado de supermercado que tiene que hacer control de stock y existencias en los lineales del mismo. En este caso, la función del empleado se reduce a, identificar el producto (mediante código de barras o tag identificativo) e introducir la cantidad del mismo.

Que duda cabe de que se trata de una labor altamente repetitiva y, que efectuada durante largos períodos de tiempo, puede provocar problemas físicos al usuario que tiene que estar sosteniendo durante horas en la mano un dispositivo tipo tableta en una posición anti-natural. No hay que olvidar que, ergonómicamente hablando, la posición de mínima tensión en los músculos y tensores de la muñeca y el antebrazo es con las palmas de la mano orientadas una hacia la otra, en perpendicular al suelo, y ligeramente orientadas hacia el interior del cuerpo y, que sujetar un dispositivo en la palma de la mano en posición de la misma horizontal al suelo, no es la posición natural y generará tensiones en los ligamentos, músculos y articulaciones.

Ilustración 4: Ergonomía: Terminal portátil tipo tableta

La ilustración (4) muestra un terminal portátil tipo tableta[2] →

Es bien conocido el efecto perjudicial sobre la salud de los operarios que realizan labores repetitivas, provocado por trabajar con herramientas y accesorios inadecuados o con criterios ergonómicos erróneos.

El lector se puede referir por ejemplo al artículo publicado por el nº 21de Septiembre de 1997 de la Revista de la OIT, "Prevención de las lesiones y enfermedades profesionales a través de la ergonomía". También en las instituciones españolas existe documentación y estudios al respecto. Como referencia se podría tomar la información suministrada por el Instituto Nacional de Seguridad e Higiene en el Trabajo [CINSHT0]en su

1 ilustración del terminal portátil CK71 de Intermec. Obtenida de la web del fabricante
2 ilustración del terminal portátil MC65 de Motorola. Obtenida de la web del fabricante

"Enciclopedia de Salud y Seguridad en el Trabajo", son especialmente relevantes el capítulo 6 [CINSHT6], "El Cuerpo Humano: Sistema Musculoesquelético" y el capítulo 29 [CINSHT29], "Herramientas y Enfoques: Ergonomía".

En el caso del ejemplo expuesto, el dispositivo idóneo para este empleado sería un dispositivo dotado de una empuñadura de sujección (tipo pistola) como el que se muestra en la figura anterior que permita sostener el mismo de forma que la palma de la mano esté lo más verticalmente posible.

Afortunadamente, la mayoría de fabricantes ya han tenido en cuenta esto en sus principales dispositivos, de manera que disponen de un accesorio, tipo empuñadura (*Handle*) , que permite utilizar el terminal de esa forma para aplicaciones repetitivas con captura de datos. De hecho, esa empuñadura, suele ir dotada de un gatillo disparador (*Trigger)* para activar cómodamente el lector de códigos de barras u otro dispositivo automático de captura incorporado en el equipo, pudiendo ser utilizado para orientarlo al más puro estilo pistola al objetivo, ya sea este un código de barras 1D o 2D.

Por lo tanto, uno de los primeros estudios que se deberán llevar a cabo para poder seleccionar un terminal portátil idóneo, es el tipo de actividad que se va a desarrollar y el mejor enfoque ergonómico para el usuario objetivo de dicha solución móvil.

Existe múltiple literatura al respecto disponible a través de organismos intenacionales, así como empresas especializadas en llevar a cabo estos estudios de ergonomía que pueden ser necesarias en caso de tener que realizar un estudio de este tipo para nuestro proyecto.

El lector puede obtener más información de las siguientes instituciones:

- Asociación Española de Ergonomía (AEE) [CESPERGO]
- International Ergonomics Association (IEA) [CINTERGO]

4.2.- Selección de Terminales Portátiles según el entorno de aplicación

En este apartado se verá como se puede seleccionar un terminal portátil para una aplicación concreta en función de los requerimientos del entorno de aplicación y el uso final del equipo en el mismo.

Para poder tomar con garantías estas decisiones de requerimientos en los equipos, se deberán analizar y entender, las diferentes especificaciones que maneja la industria y que pueden cumplir los terminales portátiles disponibles en el mercado. Entre todas las especificaciones, se abordarán especialmente las relativas al sellado frente a sólidos, líquidos y gaseosos, (protección IP), las relativas a la resistencia a golpes, y las relativas a las temperaturas de operación y almacenamiento.

Se verán cuales son los criterios a emplear en la selección de un dispositivo según las exigencias del entorno de trabajo real y como eso implica unas exigencias en el grado de protección de los equipos.

4.2.1.- Iluminación deficiente o excesiva

Una de las situaciones más comunes que se pueden encontrar en un entorno cambiante como es el de los terminales portátiles es la exposición a situaciones de poca luz o luz excesiva. Esto puede suceder cuando un usuario pasa de un espacio interior a un lugar al aire libre soleado.

4.2.1.1.- Tipos de pantalla

A continuación se numeran los diferentes tipos de pantalla que se pueden encontrar en el mercado.

4.2.1.1.1.- Reflexiva

La pantalla refleja parte de la luz que incide sobre ella. No apta para ambientes con poca luz ya que depende de la luz ambiente.

4.2.1.1.2.- Transmisiva

La pantalla transmite luz al exterior. Puede además estar apoyada por una retroiluminación LED para realzar el brillo en condiciones de mucha luz.

4.2.1.1.3.- Transflexiva

Es una combinación de las dos anteriores, es el tipo más versátil y permite trabajar en prácticamente cualquier condición de luz. Al igual que en el caso anterior, pueden estar apoyadas por una retroiluminación tipo LED.

Una fuente de información on-line para entender las tecnologías subyacentes podrían ser las notas de Kyocera sobre su tecnología de fabricación de displays:

- Información sobre pantallas reflexivas de Kyocera: [KYOCE1]
- Información sobre pantallas transmisivas de Kyocera: [KYOCE2]

- Información sobre pantallas transflexivas de Kyocera: [KYOCE3]
- Información sobre paneles digitalizadores resistivos de Kyocera: [KYOCE4]

4.2.1.2.- La pantalla en los terminales portátiles

En lo concerniente a las pantallas que se emplean en los terminales portátiles presentes en el mercado, principalmente se utilizan del tipo transflexivo (una mezcla entre reflexivo y transmisivo), que permiten trabajar mejor en situaciones de iluminación cambiante. Pueden trabajar bien con mucha luz como las reflexivas, pero también en situaciones de poca luz a diferencia de esas, y adicionalmente, pueden incorporar algún tipo de retroiluminación (*Back-Light*) de tipo LED. En algunos modelos se incorpora un sensor de luz ambiente que ayuda al software del terminal a determinar si será necesario el encendido de la retroiluminación y en que nivel de intensidad. Este sería el tipo de pantalla más idónea para una solución móvil.

El mayor inconveniente de las pantallas transflexivas es su coste y el consumo en retroiluminación, por eso en aplicaciones de tipo gran consumo se están empleando pantallas TFT o LED apoyadas por retroiluminación potente de bajo consumo como en el caso del iPhone de Apple y otros muchos modelos de electrónica de consumo.

Se podría decir que en la electrónica de gran consumo las pantallas transmisivas apoyadas por una potente retroiluminación LED están dominando el mercado, aunque en los entornos industriales también se encuentran pantallas trasnmisivas, una pantalla transflexiva con un digitalizador resistivo aún sigue siendo la mejor opción para entornos exigentes y condiciones de entorno agresivo.

4.2.1.3.- Luminancia

Existe un término ampliamente utilizado cuando se trata con pantallas de terminales portátiles y que se denomina *Luminancia*.

Se puede definir la *Luminancia* como la densidad superficial de la intensidad luminosa que se emite en una dirección dada. Este valor vendrá dado en Cd / m^2, aunque también se emplea el término NIT proveniente del campo de la óptica y la fotometría.

Por lo tanto: 1 NIT = 1 Cd / m^2

En el caso de un display, se expresa la luminancia medida para la dirección de emisión perpendicular al plano formado por la superficie de la pantalla del terminal portátil.

Idealmente, para aplicaciones en las que el usuario va a trabajar con gran incidencia de luz solar sobre el display, se elegirán pantallas transflexivas, con potente retroiluminación LED (backlight) con al menos 500 NIT de luminancia.

En caso de que en la ficha del producto no aparezca reflejado este dato, este existe y se deberá pedir al fabricante del dispositivo las especificaciones completas de su pantalla y digitalizador (normalmente fabricado por una compañía distinta)

4.2.2.- Shock Electrostático (ESD)

La ESDA (*Electrostatic Discharge Association*) [CESDA] define la descarga electrostática de la siguiente forma:

"Se define electricidad estática como una diferencia de potencial causada por una desbalance de carga de electrones en la superficie de un material. Este desequilibrio de electrones produce un campo eléctrico que puede ser medido y que puede influenciar otros objetos a distancia. Una descarga electrostática se define como la transferencia de cargas entre cuerpos con diferentes potenciales eléctricos".

En otras palabras: Cuando se tienen dos superficies con diferentes potenciales eléctricos, existe un campo eléctrico que puede originar una descarga electrostática para igualar los potenciales si el medio entre ambas superficies permite el paso de cargas eléctricas. Un dieléctrico puede llegar a permitir la transferencia de cargas cuando la diferencia de potencial se vuelve tan elevada que consigue arrancar electrones del mismo (*Potencial de Ruptura*).

Los terminales portátiles son equipos que a menudo trabajarán en zonas industriales, en presencia de fenómenos químicos y máquinas / herramientas en movimiento, expuestos a campos eléctricos y electromagnéticos, que pueden originar ciertas diferencias de potencial con respecto a las superficies del terminal portátil y que, eventualmente pueden dar lugar a descargas electrostáticas.

Es fundamental verificar la magnitud y el tipo de las descargas electrostáticas que el terminal portátil puede soportar para asegurar que funcionará sin problemas en el entorno objetivo.

Normalmente los fabricantes de terminales portátiles suministran unas especificaciones de diferencia de potencial máxima permitida para descarga electrostática soportada por el dispositivo (ESD) medida en kV. Este valor es facilitado para tres situaciones, descarga directa, descarga indirecta y descarga por el aire.

4.2.2.1.- Descarga directa

Se trata de la diferencia de potencial máxima que puede existir entre la superficie del terminal y otro objeto en contacto para que no se produzca una descarga electrostática (ESD) perjudicial para el equipo.

4.2.2.2.- Descarga indirecta

La descarga indirecta mide la diferencia de potencial máxima que puede existir entre la superficie del terminal portátil y otro objeto, teniendo intercalado otro material entre ambos para que no se produzca una descarga electrostática (ESD) perjudicial para el equipo. Este parámetro es poco común en las especificaciones de los terminales portátiles.

4.2.2.3.- Descarga por el aire

Indica la diferencia de potencial máxima que puede existir entre una superficie y el terminal portátil cuando ambos elementos están separados por el aire de forma que no se produzca una descarga electrostática (ESD) perjudicial para el equipo.

Ejemplo:

Un fabricante suministra una especificación para uno de sus modelos con los siguientes valores:

- ESD directo: ± 8kV
- ESD aire: ± 15kV

Como se puede observar, el equipo soporta más diferencia de potencial si existe un medio dieléctrico o poco conductor intercalado (aire), lo cual es lógico.

4.2.3.- Shock Térmico

Se define como shock térmico aquella variación brusca de la temperatura del aire alrededor del dispositivo aunque esta se produzca dentro de su rango de temperaturas de funcionamiento.

Una posible referencia para definir el shock térmico podría ser la empleada en el estándar militar USA MIL-STD-810G [US810G]. En este estándar de tipo militar se define el *Shock Térmico* como *"Cualquier variación brusca de temperatura de al menos 10ºC (18º F) en el intervalo de tiempo de 1 minuto"*.

Así pues, un equipo capaz de operar sin problemas en el rango de temperaturas comprendido entre -20 ºC y +50º centígrados, puede no ser capaz de soportar un shock térmico de 20º en 30 sg y, en consecuencia, puede fallar al pasar bruscamente de una temperatura de -10 º C a una temperatura ambiente de 10º C, estando ambas temperaturas dentro de su rango de temperaturas de operación, y esto podría fácilmente suceder al salir de una cámara refrigerada y pasar a un entorno más cálido.

En general, salvo que el fabricante indique claramente en sus especificaciones que el equipo está preparado para soportar shock térmico y los rangos de temperatura entre los que se puede producir, se deberá evitar el shock térmico en los terminales portátiles. En aquellos entornos en los que su operativa de trabajo implique la exposición al shock térmico, se deberán elegir terminales especialmente probados y certificados para soportarlo.

4.2.4.- Rango de temperaturas de operación

Se define el rango de temperaturas de operación, como aquellos valores de temperatura entre los cuales el fabricante del dispositivo certifica que el mismo funcionará sin problema alguno. Generalmente, estos datos están siempre presentes en las especificaciones técnicas de un terminal portátil. Así pues, puede ser común un rango de temperaturas de operación de -10º C (14ºF) a 50ºC (122 ºF), aunque existen diferencias sustanciales entre las especificaciones de los equipos, incluso dentro de los de un mismo fabricante. De esta forma, un dispositivo que debe operar en el desierto y soportar temperaturas de operación entre -10ºC y 50ºC sería conveniente que tuviese un rango de temperaturas de operación en sus especificaciones de -20ºC a 60ºC que sería un valor que especifica un fabricante real en uno de sus modelos.

4.2.5.- Rango de temperaturas de almacenamiento

Generalmente suele ser un rango más amplio que el de temperaturas de operación. El fabricante en sus especificaciones indica que valores de temperatura mínimos y máximos se deberán respetar a la hora de almacenar o depositar nuestros equipos durante un determinado periodo de tiempo sin que sufran daño alguno por los efectos de la temperatura ambiente sobre los mismos.

Tomando el ejemplo del equipo anterior cuyo rango de temperaturas de operación estaba entre -20ºC y 60ºC, el fabricante de dicho equipo especifica un rango de temperaturas de almacenamiento de -30 a 70ºC.

4.2.6.- Rango de temperaturas de carga

Aunque generalmente no se suelen especificar y se asume que es el mismo que el de temperaturas de operación, es posible que algunos equipos no operen eficientemente al ser cargadas sus baterías recargables a una temperatura ambiente determinada con algunos cargadores o cunas de alimentación. En algunos casos, el fabricante advierte de esta circunstancia especificando un rango de temperaturas de carga inferior al de temperaturas de operación.

4.2.7.- Humedad Relativa

Se define Humedad Relativa como el cociente entre cantidad de vapor de agua presente en el aire y cantidad de vapor de agua (saturación) que produciría la condensación expresado como porcentaje.

Una explicación interesante on-line sobre este concepto se encuentra en un documento [UGEHUM] del Departamento de Físicas y Astronomía de la Universidad de Georgia.

$$Humedad\ Relativa(\%) = \frac{Densidad\ vapor\ de\ agua\ en\ aire\ (gr/m^3)}{Densidad\ vapor\ de\ agua\ saturación\ (gr/m^3)}\ x\ 100$$

Otra posible definición sería la que emplea el estándar militar USA [US810G] que se basa en las presiones atmosféricas del aire.

$$Humedad\ Relativa(\%) = \frac{Presión\ atmosférica\ de\ vapor\ de\ agua\ en\ aire\ (mmHg)}{Presión\ atmosférica\ de\ saturación\ de\ vapor\ de\ agua\ en\ aire\ (mmHg)}\ x\ 100$$

De cualquier forma que se exprese, conceptualmente indica el margen de vapor de agua que se puede tener en el aire antes de que se produzca la condensación manteniendo la temperatura constante.

En los terminales portátiles se verá que humedad relativa pueden soportar operando correctamente. Generalmente se suministrará un rango de humedad relativa, como por ejemplo (de 0 a 95% sin condensación).

Se deberá verificar que los equipos pueden soportar la humedad relativa del entorno donde se vayan a utilizar los terminales portátiles. Por ejemplo en una selva tropical donde las humedades relativas pueden ser fácilmente del 98%, un equipo cuyas especificaciones son de 0 a 95% podría no ser apropiado.

4.2.8.- Ambientes explosivos e incendiarios

Es posible que nuestros equipos deban operar en atmósferas potencialmente explosivas, en cuyo caso, se deberá conocer las clasificaciones de los equipos y de las diferentes zonas de riesgo según las normativas de cada país. El presente trabajo se centrará en las normativas norteamericanas (USA y Canadá) y europeas.

4.2.8.1.- Organismos de certificación internacionales

Un organismo certificador a nivel internacional es el IECEX dependiente del IEC [IECEX].

A nivel internacional, el IEC ha generado estándares para regular las características que deben tener aquellos equipos que vayan a operar en atmósferas potencialmente explosivas:

- IEC 60079-0 Equipamiento: Requerimientos generales [IS60790]
- IEC 60079-10-1 Atmósferas Explosivas – Clasificación de Áreas: Atmósferas explosivas

de gas [IS0079101]

- IEC 60079-10-2 Atmósferas Explosivas – Clasificación de Áreas: Atmósferas explosivas de polvo combustible [IS0079102]
- IEC 60079-11 Atmósferas Explosivas – Protección de los equipos por protección intrínsec "i" [IS6007911]
- IEC 60079-25 Atmósferas Explosivas – Protección de equipos eléctricos intrínsecamente seguros [IS007925]

4.2.8.2.- Normativa Europea ATEX

En el caso de la Unión Europea, la regulación sobre la protección de los equipos eléctricos y electrónicos que deban funcionar en atmósferas potencialmente explosivas viene dada por las siguientes directivas:

- Directiva 1999/94/CE del Parlamento Europeo y del Consejo de 16 de diciembre de 1999

  Relativa a las disposiciones mínimas para la mejora de la protección de la salud y la seguridad de los trabajadores expuestos a los riesgos derivados de atmósferas explosivas.

- Directiva 94/9/CE del Parlamento Europeo y del Consejo de 23 de marzo de 1994 [IS949CE]

  Relativa a la aproximación de las legislaciones de los Estados miembros sobre los aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas.

Es la última de estas directivas la que afecta en concreto a la clasificación de los tipos de protección que deben aportar los equipamientos (en nuestro caso terminales portátiles) para trabajar en atmósferas explosivas.

Existen unas directrices para su aplicación en el documento “ATEX Guidelines” de la Comisión Europea de Industria y Empresa [ISATEX1].

Hay que contemplar los siguientes grupos y categorías para el marcado y certificación de aparatos que deban operar en atmósferas explosivas:

4.2.8.2.1.- Grupo I – Categoría M1

Estos equipos se caracterizan por estar destinados para su uso en trabajos de minería tanto subterráneos como en sus instalaciones al aire libre en la que exista peligro debido al grisú y/o polvos explosivos.

Los aparatos de esta categoría deben permanecer operativos en presencia de atmósferas explosivas, aún en caso de avería infrecuente.

4.2.8.2.2.- Grupo I - Categoría M2

Al igual que en la categoría anterior, estos equipos se caracterizan por estar destinados para su uso en trabajos de minería tanto subterráneos como en sus instalaciones al aire libre en la que exista peligro debido al grisú y/o polvos explosivos.

En caso de que haya signos de una atmósfera potencialmente explosiva, deberá poderse cortar la alimentación energética de estos aparatos.

Los medios de protección relativos a los aparatos de esta categoría asegurarán el nivel de protección requerido durante su funcionamiento normal, incluso en condiciones de explotación más rigurosas, en particular las resultantes de una utilización intensa del aparato y de condiciones ambientales cambiantes.

4.2.8.2.3.- Grupo II – Categoría 1

Los aparatos de esta categoría están previstos para utilizarse en un medio ambiente en el que se produzcan de forma constante, duradera o frecuente atmósferas explosivas debidas a mezclas de aire con gases, vapores, nieblas o mezclas polvo-aire.

4.2.8.2.4.- Grupo II - Categoría 2

Los aparatos de esta categoría están destinados a utilizarse en un ambiente en el que sea probable la formación de atmósferas explosivas debidas a gases, vapores, nieblas o polvo en suspensión.

Los medios de protección relativos a los aparatos de esta categoría asegurarán el nivel de protección requerido, aún en caso de avería frecuente o de fallos del funcionamiento de los aparatos que deban tenerse habitualmente en cuenta.

4.2.8.2.5.- Grupo II - Categoría 3

Los aparatos de esta categoría están destinados a utilizarse en un ambiente en el que sea poco probable la formación de atmósferas explosivas debidas a gases, vapores, nieblas o polvo en suspensión y en que, con arreglo a toda probabilidad, su formación sea infrecuente y su presencia sea de corta duración. Los aparatos de esta categoría asegurarán el nivel de protección requerido durante su funcionamiento normal.

4.2.8.2.6.- Marcado CE para Atmósferas Explosivas

Ilustración 6: Marcado CE Atmósferas Explosivas

En el marcado del aparato, además de aparecer marca CE de la ilustración (5), y otros datos obligatorios, aparecerá el marcado específico de protección contra las explosiones de la ilustración (6), seguido del símbolo del grupo de aparatos y de la categoría. Para el grupo de aparatos II, además aparecerá la letra G (referente a atmósferas explosivas debidas a gases, vapores o nieblas), y/o la letra D referente a atmósferas explosivas debidas a la presencia de polvo.

Ilustración 5: Marcado Conformidad CE

4.2.8.2.7.- Grupos de gases

- Grupo I: Minería (Metano/Grisú)
- Grupo II: A (Metano industrial, propano, petroleo y la mayor parte de gases industriales)
- Grupo II: B (Etileno y otros gases industriales)
- Grupo II: C (Hidrógeno, acetileno, ….)

La lista de gases está ordenada de menos a más volátil.

4.2.8.3.- Intrínsecamente seguro / (IS) Intrinsically Safe)

El término *Intrinsically Safe, IS* o *Intrinsic Safe*, según donde aparezca publicado, hace referencia al más alto grado de protección que puede aportar un equipo para funcionamiento en atmósferas explosivas según las normativas norteamericanas (ANSI / UL 913).

Los equipos marcados como *(IS) o Intrinsically Safe* pueden operar en las siguientes clasificaciones de entornos para atmósferas explosivas en USA y Canada:

Class I – Division 1 – Grupos (los que se especifiquen) Tn (la que especifique)

Class II – Division 1 – Grupos (los que se especifiquen) Tn (la que especifique)

Class III – Division 1 – Grupos (los que se especifiquen) Tn (la que especifique)

Class I – Zone 0 – Grupos (los que se especifiquen) Tn (la que especifique)

Siempre y cuando cumpla con los requisitos de temperatura de operación y en cuanto a las temperaturas de ignición del polvo y partículas en suspensión.

Los grupos, podrían ser por ejemplo A, B, C, D (gases) o E, F, G (polvo y partículas) y la temperatura podría ser T4 (135ºC). Un código de temperatura T6 (85ºC) indicaría un equipo más seguro en las mismas condiciones.

Se define como un equipo intrínsecamente seguro aquel que es incapaz de generar una chispa o el calor suficiente para provocar una ignición en una atmósfera explosiva, independientemente de que tipo de atmósfera explosiva se trate: gases inflamables, vapores, combustibles, polvo, o partículas y fibras en suspensión en el aire.

4.2.8.4.- No incendiario / (NI) Non-Incendive

Es el segundo grado de protección más alto que puede tener un equipo después de Intrinsically Safe (IS) en atmósferas explosivas.

El término *Non Incendive o (NI)*, hace referencia a un equipo incapaz de provocar una chispa o temperatura suficiente para provocar una ignición en atmósferas explosivas clasificadas como según las normativas norteamericanas (ANSI / UL 913) en uno o varios de los siguientes entornos:

Class I – Division 2 – Grupos (los que se especifiquen) Tn (la que especifique)

Class II – Division 2 – Grupos (los que se especifiquen) Tn (la que especifique)

Class III – Division 2 – Grupos (los que se especifiquen) Tn (la que especifique).

Siempre y cuando cumpla con los requisitos de temperatura de operación y en cuanto a las temperaturas de ignición del polvo y partículas en suspensión.

Los grupos, podrían ser por ejemplo A, B, C, D (gastes) o E, F, G (polvo y partículas) y la temperatura podría ser T4 (135ºC). Un código de temperatura T6 (85ºC) indicaría un equipo más seguro en las mismas condiciones.

Se define como un equipo no incendiario aquel que es incapaz de generar una chispa o el calor suficiente para provocar una ignición en determinadas atmósferas explosivas, con una exposición limitada y según las especificaciones del fabricante.

4.2.9.- Exposición a partículas sólidas y agua

En multitud de aplicaciones el dispositivo portátil podrá estar expuesto, de forma puntual o permanente, a salpicaduras, polvo, derramamiento de líquidos, inmersiones accidentales, o cualquier combinación de estos eventos. Es por lo tanto fundamental que el dispositivo pueda soportar las condiciones de trabajo a las que va a ser sometido.

En este aspecto, existen normativas y estándares que permiten delimitar y clasificar estos riesgos y, por lo tanto, definir de forma clara y concisa las características que debe cumplir un equipo para trabajar en estos entornos exigentes.

El principal organismo encargado de elaborar este tipo de normas es la Comisión Internacional Electrotécnica (IEC).

4.2.9.1.- Nivel de protección IP requerido por el entorno de trabajo

El nivel de protección IP que hay que exigir a un equipo dependerá de la utilización del mismo en su entorno de trabajo real. Así pues, según el tipo de entorno y aplicación, existirá una determinada posibilidad de que el equipo en cuestión tenga que soportar agua o polvo. Una clasificación de estos entornos en función de la exposición al agua y a polvo podría ser la que se expone en los apartados siguientes.

Lo que más va a marcar el nivel de protección IP necesario en nuestro equipo será la exposición al agua, ya que el diseño y sellado de una carcasa frente al agua implica un alto grado de protección inherente ante el polvo, pero no al contrario. Por ejemplo, un equipo con nivel de protección IP4X puede proteger bien frente a sólidos y ser mediocre ante el agua. Sin embargo, un equipo con un buen nivel de protección frente al agua tiene obligatoriamente un buen nivel de protección ante el polvo también. No se encontrarán equipos IPX5 cuyo primer dígito de protección contra el polvo sea inferior a 5. De hecho, lo normal es que un equipo con nivel de protección 5 ante el agua aporte un sellado ante sólidos de nivel 6.

4.2.9.1.1.- Exposición ligera y ocasional al agua

Se trata de situaciones en las que los equipos en su entorno habitual de trabajo estarán en interiores o al aire libre, pero con exposición reducida a lluvia o salpicaduras de forma ocasional, limitada en el tiempo y en su posición habitual de trabajo.

Para este tipo de aplicaciones será suficiente un nivel de protección IPX4. El segundo dígito que indica el nivel de protección frente al ingreso de agua deberá ser 4 o superior. Como un equipo que se ha protegido frente al ingreso de agua, inherentemente, al diseñar la carcasa para ese propósito, también estará protegido ante la entrada de ciertos sólidos. Generalmente un equipo que ofrece nivel 4 de protección ante el ingreso de agua, también ofrece superior a 4 ante la entrada de sólidos. Un grado de protección IP54 sería el nivel mas extendido entre las especificaciones de los terminales portátiles disponibles en el mercado, aunque también se encontrarán equipos con el nivel de protección IP64.

4.2.9.1.2.- Exposición permanente al agua o a la intemperie

Se trata de terminales que van a tener que trabajar en exteriores muy lluviosos, expuestos permanentemente al agua o a la intemperie. En este tipo de entornos no es válido el nivel 4 porque no se podrá garantizar que el agua incida siempre en el rango de +60% / -60º con respecto a la vertical de la posición habitual de trabajo.

Para este tipo de aplicaciones serán necesarios terminales con sellado del tipo IPX5. Al igual que

se explicó en el caso anterior, un equipo que ofrece nivel 5 de protección ante líquidos, también aportará un nivel 5 o superior frente a sólidos. El nivel de protección más extendido que se encontrará en los equipos será el IP65.

4.2.9.1.3.- Exposición a chorros de agua a gran presión desde cualquier dirección

Se trata de un caso poco común, pero que requeriría un nivel de protección IP66 o superior.

4.2.9.1.4.- Gran exposición al agua e inmersión accidental

Serán entornos muy expuestos al agua o en los que se prevea que el equipo pueda sumergirse accidentalmente en agua.

En estos entornos hay que exigir que el equipo pueda sumergirse de forma temporal. Esta protección la aportaría el nivel IP67 ya que, obviamente, ningún equipo con protección frente al agua de nivel 7 tendrá una protección ante al polvo y sólidos inferior a 6.

4.2.9.1.5.- Inmersión permanente en agua

Equipos de utilización bajo el agua, o en los que se pueda contemplar la inmersión prolongada en agua.

Se deberá emplear el nivel de protección máxima, IP68.

También se prestará atención a la letra suplementaria con el valor M. Esta letra indicaría que se podría utilizar el equipo funcionalmente bajo el agua ya que estaría preparado para soportar la inmersión con sus partes móviles en movimiento (teclas, gatillo disparador, …). IP68M sería otra posible especificación para este tipo de equipos.

En este caso, el fabricante deberá especificar la presión que puede soportar el equipo, la profundidad de inmersión o ambos parámetros.

4.2.9.1.6.- Poco polvo o partículas sólidas con Ø ≥ 1 mm

Entornos poco polvorientos o con partículas de sólidos de diámetro superior a 1 mm

En estos entornos será suficiente un equipo con nivel de protección IP4X. Una especificación común en el mercado es IP42.

4.2.9.1.7.- Bastante polvo o partículas sólidas con Ø < 1 mm

Entornos polvorientos o con partículas de sólidos de diámetro inferior a 1 mm

Aquí se debe exigir que, si bien el equipo no esté totalmente sellado, si pueda soportar el ingreso de estas partículas de polvo en poca cantidad y sin afectar a su funcionamiento.

Un nivel de protección IP5X será valido para estos propósitos. Una especificación muy extendida para estos equipos en el mercado es el IP54. Esto será válido siempre y cuando el tipo y la composición químicas de los sólidos que ingresen en el interior del equipo no sean dañinos para sus componentes internos, por reacciones químicas con los mismos, en cuyo caso se deberá seleccionar el nivel de protección máximo IP6X.

4.2.9.1.8.- Mucho polvo con Ø < 1 mm o perjudicial para los equipos

Estos son entornos muy polvorientos, con partículas cuyo diámetro es inferior a 1 mm y que

pueden además, por su composición química, ser perjudiciales para los componentes internos del equipo y deteriorarlo.

Será necesario un nivel de protección IP6X y el equipo no deberá permitir de ninguna manera la entrada de polvo en el mismo (sellado). Posibles niveles de protección normalmente ofrecidos por los fabricantes de equipos son: IP64, IP65, IP66 e IP67.

4.2.9.1.9.- Selección del nivel mínimo de protección IP

Se ha elaborado la tabla (1) que permite seleccionar el nivel de protección IP mínimo que debe proveer un terminal portátil en función del entorno de trabajo al que se verá expuesto.

Agua → Sólidos	Sin lluvia ni exposición al agua	Lluvia o salpicaduras ocasionales	Mucha exposición al agua o a la intemperie	Chorros de agua a gran presión	Mucha exposición al agua e inmersión accidental	Actividades sub-acuáticas / Inmersiones prolongadas
Poco Polvorientos	IP4X	IP54	IP65	IP66	IP67	IP68
Polvorientos	IP5X	IP54	IP65	IP66	IP67	IP68
Muy polvorientos	IP6X	IP64	IP65	IP66	IP67	IP68

Tabla 1: Matriz de selección del nivel de protección IP mínimo

4.2.10.- Exposición a caídas, vibraciones y golpes

Un aspecto importante en la gran mayoría de aplicaciones profesionales es la capacidad de soportar golpes fortuitos o caídas por parte de los terminales portátiles. A diferencia de entornos de oficina, en los que los equipos se encuentran en un entorno controlado y en una posición más o menos estable, en las aplicaciones reales de los terminales portátiles, el usuario será en la mayoría de los casos un operario, se desplazará con una cierta asiduidad portando el equipo e, interaccionará con el mismo al realizar diversas labores físicas, dando lugar a que el equipo sufra caídas accidentales o reciba impactos de otros objetos.

Es vital para el éxito de nuestra aplicación efectuar un estudio pormenorizado del entorno real en el que van a trabajar los terminales portátiles, la probabilidad de impacto o caída y, en caso de producirse esta, desde que altura o con que frecuencia se va a producir.

La mayoría de los terminales portátiles para uso profesional pasan una serie de test de caída que garantizan que el equipo podrá soportar caídas en las condiciones determinadas en función del grado de protección garantizado por el fabricante. Será por lo tanto, labor del diseñador de la aplicación, definir qué requerimientos mínimos debe cumplir en sus especificaciones el terminal portátil elegido.

En general, habrá que considerar normativas o estándares de los dos organismos más reconocidos y utilizados a la hora de evaluar la protección ante caídas, golpes y vibraciones para certificar el nivel de protección de los terminales portátiles.

- Comisión Internacional Electrotécnica (IEC)
- Departamento de Defensa de los Estados Unidos de América.

Para entender las especificaciones de los fabricantes en lo concerniente a la protección contra golpes, se deberán entender dos conceptos muy utilizados y con una traducción a veces no evidente del inglés: *Drop* y *Tumble*.

Casi todas las especificaciones de dispositivos hablan de certificaciones o pruebas en esos dos apartados.

4.2.10.1.- Test de caída libre (Drop Test)

Sería la prueba más estricta de caída libre. Se coloca el terminal portátil a una altura determinada de prueba de la superficie sobre la que se pretende que impacte, y además, en una orientación determinada. Por ejemplo, con una de sus aristas apuntando al suelo en perpendicular, y en ese momento, se suelta y se evalúan los efectos de dicho impacto sobre el dispositivo. Se repite tantas veces y en tantas posiciones como defina el estándar de prueba que se quiera aplicar.

Normalmente un fabricante indicará la altura máxima de test que el terminal portátil ha pasado sin sufrir daños y, en caso de cumplir algún estándar o norma, cuáles cumple y en qué apartados.

Ejemplo: Drop Test: 1,22 m sobre hormigón, estándar militar USA MIL-STD-810G

4.2.10.2.- Test de caída repetida en movimiento (Tumble Test)

Se trata de una prueba menos exigente en cuanto a la altura, y más en cuanto a la repetición de los impactos y la aleatoriedad de los mismos. En este tipo de prueba se mide la capacidad que tiene el equipo de soportar repetidos golpes típicos de manipulación y caídas de baja altura con el dispositivo en movimiento que se puedan producir en su uso diario, golpes que si bien no se producen a una altura tan exigente como el de caída libre, si son más repetidos y más aleatorios en su punto de incidencia sobre la superficie del terminal portátil.

Digamos que, por ejemplo, cuando un usuario va andando con un terminal portátil en la mano, y tropieza, el terminal portátil girará en el aire y efectuará varios movimientos antes de caer en una superficie, que además puede no ser el suelo. Lo mismo sucede cuando al tropezar con un mueble un terminal portátil sale despedido y cae al suelo. Ese es el efecto que se busca con esta prueba. El equipo se lanza en movimiento (girando sobre sus ejes) desde una altura determinada para impactar sobre una superficie de prueba.

En este apartado un fabricante indicará la altura máxima de test que el terminal portátil ha pasado sin sufrir daños, y el número de pruebas que se han repetido y, en caso de cumplir algún estándar o norma, cuáles cumple y en qué apartados.

Ejemplo: Tumble Test: 1000@ 1 m, equivalente a 2000 según IEC 60068-2-32

4.2.10.3.- Entornos de funcionamiento

Para clasificar los terminales portátiles se utilizarán tres posibles tipos de entorno en los que se tendrán que desenvolver:

4.2.10.3.1.- Entorno medio

Aplicaciones en las que exista baja probabilidad de impacto y en caso de producirse este sea siempre desde menos de 1 m de altura.

En este entorno, los terminales portátiles son utilizados en interiores y existe posiblidad de caídas eventuales desde mesas de trabajo.

En este caso será suficiente que nuestro equipo cumpla con los estándares IEC.

Aplicaciones cuyos impactos por caída libre se producirán siempre desde la altura de utilización de un operario o inferior.

Este es el caso que queda plenamente cubierto por el estándar militar USA MIL-STD-810G.

4.2.10.3.2.- Entorno duro

Aquí se debería elegir equipos con el mayor nivel de protección posible ante impacto ya que es muy probable por el uso que va a dar el operario al equipo que se produzca el impacto por caída y, en caso de producirse esta, seguramente sea a más altura de la de utilización del operador o, que aunque desde menor altura, los impactos sean más repetidos en el tiempo.

En este caso se elegirán equipos que excedan los requerimientos de 1,22 m del estándar militar USA MIL-STD-810G y, siempre que sea posible, que indiquen una protección de al menos 1000 impactos repetidos en movimento desde 1 m de altura (*Tumble*).

4.2.10.3.3.- Entorno muy duro

Aplicaciones con gran probabilidad de impacto o que deben soportar caídas desde una altura de 1,8 m o mayor. Se trata de operarios de gran movilidad, en actividades manuales intensivas, manipulando materiales, subidos en algún tipo de máquina o herramienta (grúas, toros mecánicos, escaleras, elevadores, estanterías, ...).

Se define como entornos muy duros aquellos en los que los equipos portátiles deban soportar caídas de altura igual o superior a 1,8 m

4.2.10.4.- Definiciones del fabricante en protección ante golpes, caídas y vibraciones

Los fabricantes utilizan la denominación *Rugged* o *Ultra Rugged*, y cuando utilizan estos términos, se refieren a terminales portátiles que cumplen con los siguientes requerimientos mínimos en su protección frente a impactos y caídas.

4.2.10.4.1.- Rugged

Caída Libre (Drop):	1,22 m (4 ft)

4.2.10.4.2.- Ultra Rugged

Caída Libre (Drop):	1,8 m (6 ft)
Impactos repetidos (Tumble):	2000 @ 1 m (3,3 ft)

Estos son indicaciones de las pruebas que debe efectuar el fabricante sobre el equipo en cuestión. Adicionalmente, el fabricante podrá incluir información sobre certificaciones o cumplimientos de estándares al respecto.

4.2.10.5.- Clasificación de terminales portátiles según su protección ante impactos y caídas

Entorno de Aplicación	Fabricante	Terminales Portátiles	Caídas Impactos	Estándares y Sellado
Muy duro	Intermec	CK71 / CK70 / CN70 / CN70e	2,4 m (8 ft) 2000 @ 1 m	IEC, MIL-STD-810G, IP67 (1,8 m drop MIL-STD-810G todas temperaturas)
Muy duro	Intermec	CN4 / CN4e	1,8 m (6 ft)	IEC, MIL-STD-810G, IP64
Muy duro	Intermec	CN3e	1,8 m (6 ft)	IEC, MIL-STD-810G, IP64
Muy duro	Intermec	CN3	1,8 m (6 ft)	IEC, MIL-STD-810G, IP54
Muy duro	Motorola	MC9500-K	1,8 m (6 ft) 2000 @ 1 m + Vibration[1]	IEC, MIL-STD-810G, IP67
Muy duro	Motorola	MC9190-G / MC55A0	1,8 m (6 ft) 2000 @ 1 m	IEC, MIL-STD-810G, IP64
Muy duro	Motorola	MC65	1,8 m (6 ft) 1000 @ 0,5 m + Vibration	IEC, MIL-STD-810G, IP64
Muy duro	Motorola	MC75 / MC55A0	1,8 m (6 ft) 1000 @ 0,5 m	IEC, MIL-STD-810G, IP64
Muy duro	Datalogic	KYMAN / FALCON X3	1,8 m (6 ft)	IP64
Muy duro	Honeywell	Dolphin 99EX / MX9 / MX9 HL / MX9 CS	1,8 m (6 ft)	IEC, IP67
Muy duro	Honeywell	Dolphin 99GX	1,8 m (6 ft)	IEC, IP64
Duro	Intermec	CK32IS	1,52 m (5 ft) + Vibration	IEC, MIL-STD-810G, MIL-PRF-28800F, IP67
Duro	Intermec	CK3B	1,5 m (5 ft)	IEC, MIL-STD-810G, IP54
Duro	Intermec	CN50	1,5 m (5 ft) 1000 @ 0,5 m	IEC, MIL-STD-810G, IP54

1 (+Vibration) Estos equipos han pasado pruebas de resistencia a vibraciones según las especificaciones del fabricante o del estándar correspondiente.

Entorno de Aplicación	Fabricante	Terminales Portátiles	Caídas Impactos	Estándares y Sellado
Duro	Datalogic	SKORPIO / SKORPIO X3 / ELF	1,5 m (5 ft)	IP54
Duro	Honeywell	MX7 / MX7 CS	1,5 m (6 ft)	IEC, MIL-STD-810F, IP65
Duro	Honeywell	TECTON / TECTON CS	1,5 m (6 ft)	IP65
Duro	Honeywell	Dolphin 7800	1,5 m (6 ft) 1600 @ 1 m	IEC, IP64
Duro	Honeywell	Dolphin 7800 HC	1,5 m (6 ft) 1600 @ 1 m	IEC, IP54
Duro	Honeywell	Dolphin 9700	1,5 m (6 ft) 2000 @ 0,5 m	IP64
Medio	Intermec	CS40	1,22 m (4 ft)	IEC, MIL-STD-810G, IP54
Medio	Motorola	MC3100	1,22 m (4 ft) 500 @ 0,5 m	IEC, MIL-STD-810G, IP54
Medio	Motorola	MC2100	1,22 m (4 ft) 500 @ 0,5 m + Vibration[1]	IEC, MIL-STD-810G, IP54
Medio	Motorola	ES400	1,22 m (4 ft) 150 @ 0,5 m + Vibration	IEC, MIL-STD-810G, IP42,MIL-STD-810G Vibration Method 514.5
Medio	Motorola	MC1000	1,22 m (4 ft) 500 @ 0,5 m	IEC, IP54
Medio	Datalogic	RHINO	1,22 m (4 ft) + Vibration	MIL-STD-810F, IP65
Medio	Datalogic	MEMOR	1,22 m (4 ft)	IP54

1 (+Vibration) Estos equipos han pasado pruebas de resistencia a vibraciones según las especificaciones del fabricante o del estándar correspondiente.

Entorno de Aplicación	Fabricante	Terminales Portátiles	Caídas Impactos	Estándares y Sellado
Medio	Honeywell	Dolphin 6100 / Dolphin 6500	1,22 m (4 ft) 1000 @ 1 m	IP54
Medio	Honeywell	MX8	1,22 m (4 ft) 500 @ 0,5 m	IP54
Medio	Honeywell	Optimus 5900 RFID	1,22 m (4 ft) 250 @ 1 m	IP54
Medio	Honeywell	MARATHON	1,22 m (4 ft)	IP65

Tabla 2: Clasificación de terminales portátiles por su protección ante impactos, caídas y vibración

4.2.10.6.- Estándares de protección ante vibraciones, impactos y caídas

En ese aspecto, los estándares más reconocidos y aplicados por los diferentes fabricantes para certificar sus equipos e indicar su grado de protección ante caídas, impactos y vibraciones son:

- Estándares ISO/IEC
  - IEC 60068-2-27 Caída libre (*Drop / Transit Drop*) [IS068227]
  - IEC 60068-2-32 Impactos repetidos en movimiento (*Tumble*)
    - Estándar reemplazado por IEC 60068-2-31 [IS068231]
  - IEC 60068-2-64 Vibraciones [IS068264]
- Estándar USA-MIL-STD-810G [US810G]:
  - METHOD 514: Vibraciones
  - METHOD 516: Impactos y caídas (*Drop & Tumble*)

4.3.- Selección de Terminales Portátiles según las tecnologías a emplear

En este apartado, será una extensión del anterior y en él se verán las diferentes tecnologías que existen en el mercado y que pueden estar presentes en estos dispositivos. Qué pantallas se pueden encontrar, sus características, qué interfaz de usuario para la entrada de datos y cómo hacer uso de él.

También se abordarán en este apartado tecnologías como la captura de códigos de barras 1D y 2D, lectura de tarjetas de banda magnética, tarjetas inteligentes, GPS, Wi-Fi, Bluetooth, cómo estás tecnologías están incorporadas en los dispositivos portátiles y de qué forma pueden ser empleadas.

El primer paso a dar a la hora de definir una solución móvil profesional es detallar qué tecnologías se va a necesitar que estén presentes en los dispositivos.

Así pues, si se pretende desarrollar una aplicación que captura fotos de documentos, pruebas de entrega, o detalles del estado de un artículo, para atención al cliente, será necesario un dispositivo con cámara integrada y una resolución de al menos 2 Mpixel.

Lo mismo habrá que tener en cuenta si se necesita leer códigos de barras de artículos con simbología EAN-13 en los lineales de un supermercado. En ese caso, se deberá disponer de un lector de códigos de barras 1D. Generalmente los lectores de códigos de barras 2D, también pueden leer códigos 1D, de modo que se asumirá que un dispositivo dotado de lector de códigos 2D también puede capturar códigos 1D.

4.3.1.- La base de datos de Terminales Portátiles

Para facilitar la labor de seleccionar terminales según unos requerimientos determinados, se ha elaborado una base de datos de OpenOffice 3.4.1 con todas las características que pueden tener los terminales portátiles para uso profesional.

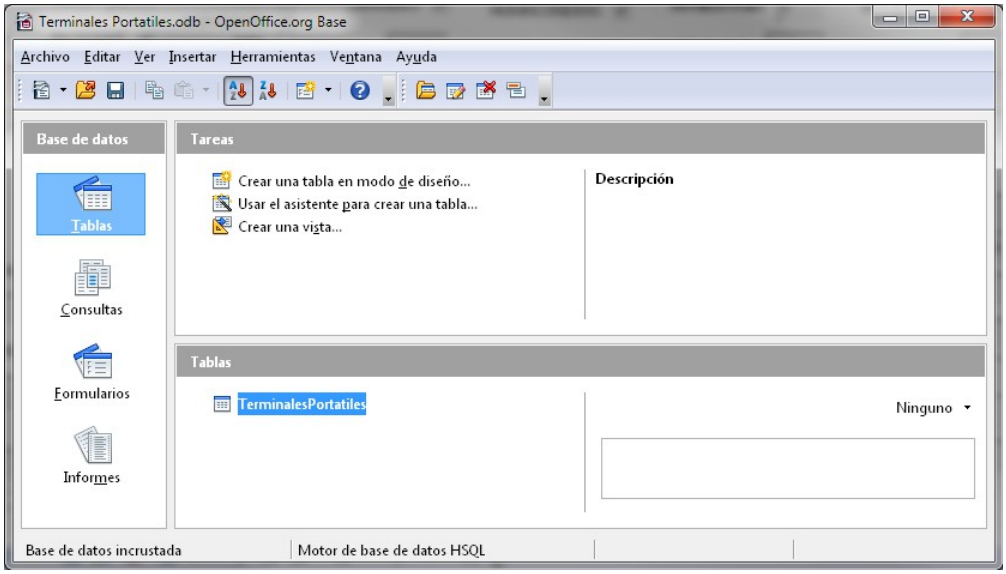

Ilustración 7: Pantalla Principal de OpenOffice con la base de datos

En la ilustración (7) se puede observar la pantalla principal del gestor de base de datos de OpenOffice con la base de datos de terminales portátiles (*TerminalesPortatiles.odb*).Dada la gran

cantidad de posibles dispositivos, se ha reducido la base de datos con algunos registros y, posteriormente, el usuario puede incorporar todos los dispositivos disponibles en el mercado para los fabricantes que quiera considerar en sus proyectos. El procedimiento es sencillo, bastará con abrir el formulario de edición de la base de datos (*TerminalesPortátiles.Frm*) y añadir, modificar, o eliminar registros. Se deja abierto a los criterios y necesidades del usuario.

4.3.1.1.- Creación, modificación y borrado de registros

El formulario *TerminalesPortatiles.Frm* ha sido diseñado tanto para añadir registros a la base de datos, como para modificar o borrar los ya existentes.

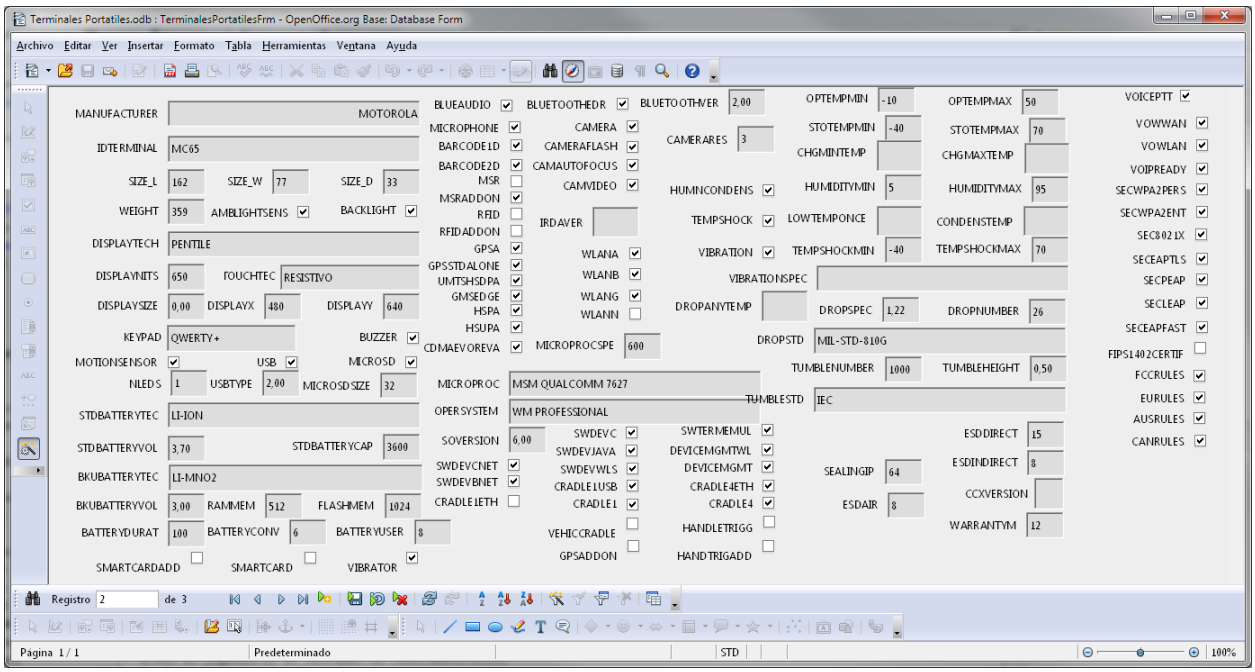

Ilustración 8: Formulario de creación, modificación y borrado de registros

Al abrir el formulario se interacciona con la pantalla que se muestra en la ilustración (8).

En la parte inferior, está la barra de navegación que permitirá avanzar y retroceder registros y, en caso necesario, guardar los cambios efectuados.

Para elaborar la base de datos y evitar posibles errores de transcripción se recomienda la utilización de las hojas de características y especificaciones originales de cada fabricante en inglés, de ahí que en la base de datos también se haya puesto los nombres de los campos en inglés.

4.3.1.2.- Creación de una consulta con el asistente

Se puede crear una consulta personalizada y guardarla para ejecutarla posteriormente cuantas veces sea necesario. En este ejemplo utilizará el asistente de OpenOffice.

En este caso, y para simplificarlo, se creará una consulta de ejemplo que se basará en lo siguiente:

Seleccionar todos los terminales portátiles de la base de datos que dispongan de código de barras 1D o 2D.

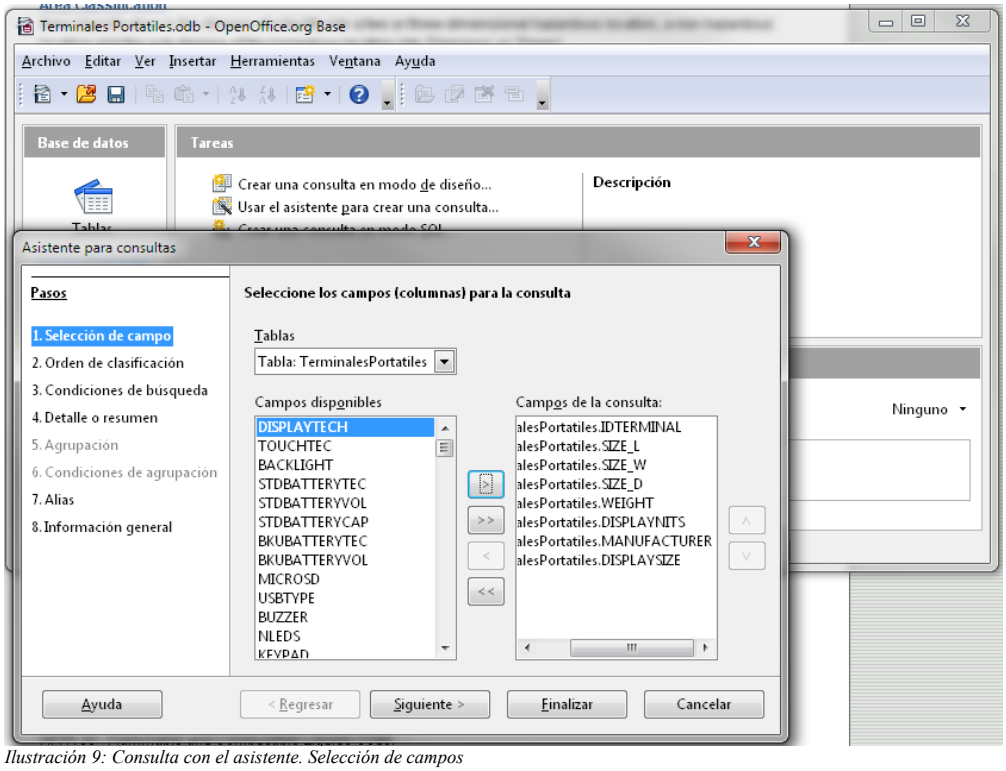

Ilustración 9: Consulta con el asistente. Selección de campos

También mostrar los siguientes campos de los registros seleccionados (ilustración :

- Fabricante
- Modelo del terminal
- Largo, Ancho, Algo y Peso del equipo
- Tamaño de la pantalla (en pulgadas) y NITS de luminancia

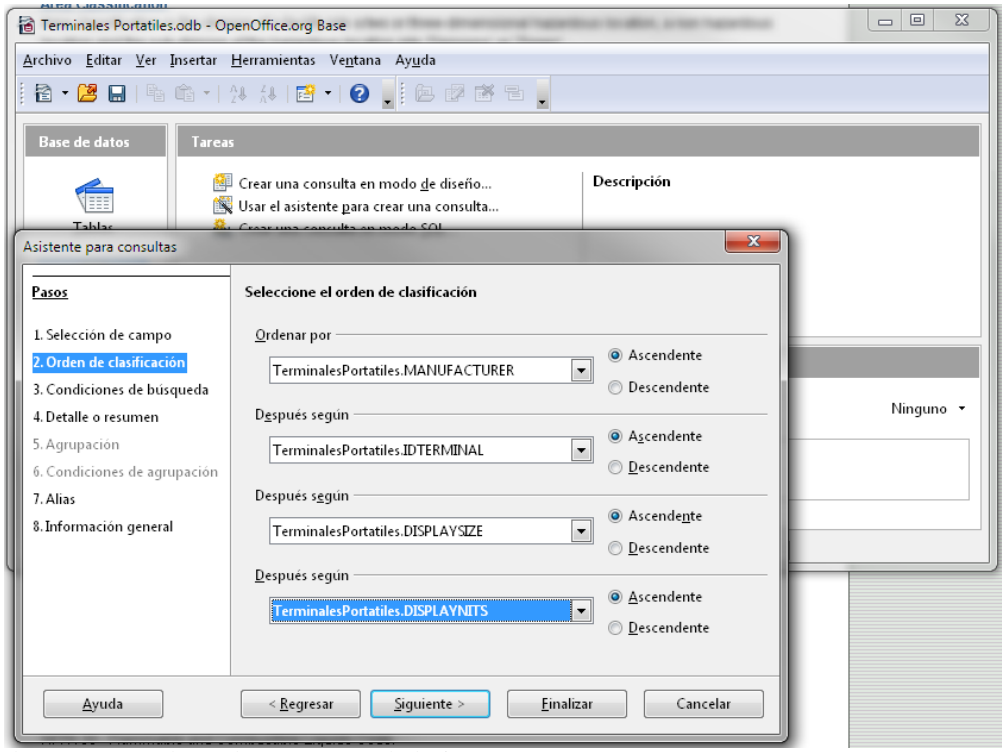

Ilustración 10: Consulta con el asistente. Criterio de clasificación

Además se pueden elegir los criterios de ordenación de los registros seleccionados. En este caso, se seleccionará: 1º por fabricante, 2º por modelo de terminal, 3º por tamaño de pantalla y 4º por luminosidad en NITS.

Ahora se indican los criterios de selección, que son que alguno de los indicadores de códigos de barras 1D o 2D esté activados.

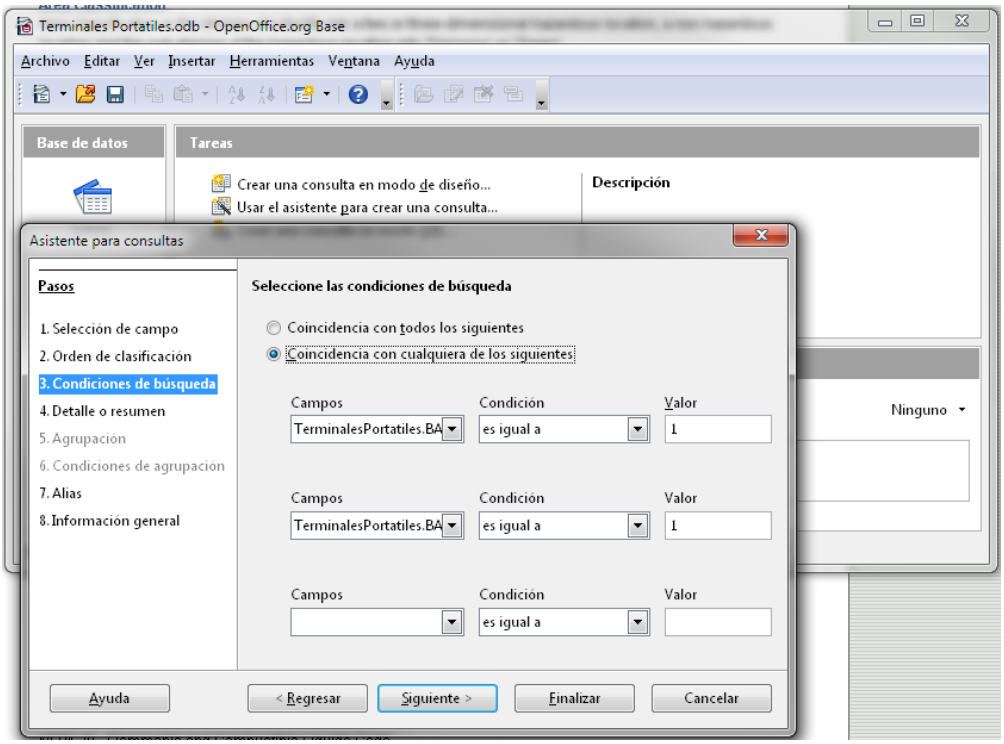

Ilustración 11: Consulta con el asistente. Condiciones de búsqueda

Y lo último que faltará configurar será las descripciones de los campos.

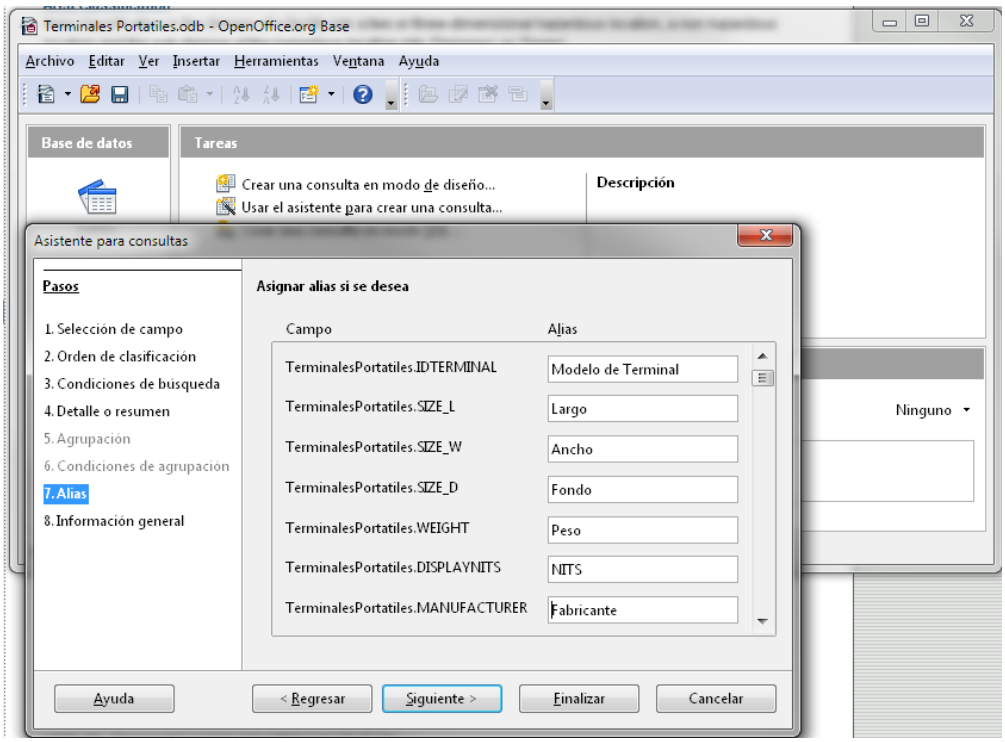

Ilustración 12: Consulta con el asistente. Alias de los campos

Al ejecutar nuestra consulta el resultado conseguido es el que se muestra.

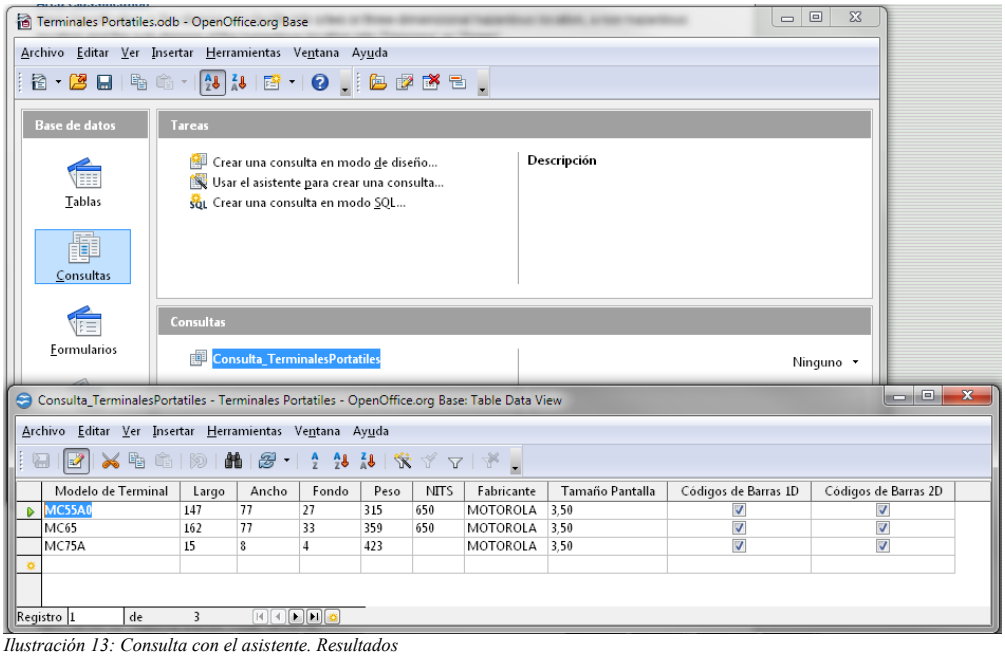

Ilustración 13: Consulta con el asistente. Resultados

Hay que tener en cuenta que el resultado mostrado no es más que un ejemplo y no es indicativo de la realidad del mercado, ya que en el momento de efectuar la consulta solamente había unos pocos registros en la base de dato, de entre los cuales 3 cumplían las condiciones establecidas.

5.- PRUEBAS DE TERMINALES PORTÁTILES

Una vez seleccionado el terminal o terminales portátiles que se van a utilizar para una solución móvil, se deberá añadir un paso adicional que no añadiría en otro proyecto que involucrase por ejemplo equipos de escritorio y servidores. Se deberá efectuar unas pruebas de funcionamiento del equipo en un entorno de trabajo real.

5.1.- Objetivo de las pruebas

El objetivo de la prueba es detectar debilidades del equipo en el entorno de aplicación real que van más allá de lo estipulado en sus especificaciones o simplemente se desconoce cual podrá ser su comportamiento.

5.2.- Ubicación de las pruebas

La prueba se llevará a cabo en la ubicación más desfavorable para los equipos, con las peores condiciones ambientales, en las tareas más duras, con el peor trato en caídas y golpes, etc...

5.3.- Preparación de hardware y software para las pruebas

Para llevar a cabo la prueba, se tendrá que dotar al terminal portátil de los accesorios y configuraciones que vaya a tener en la aplicación real (fundas, soportes, empuñaduras, baterías de reemplazo, protectores de pantalla, dispositivos add-on para captura de datos o integrados).

El equipo deberá tener el mismo sistema operativo, versión, parches y actualizaciones, así como todos los controladores y herramientas software que tendrá cuando funcione con los aplicativos de producción, aunque no exista el software de producción porque aún no esté desarrollado.

Si no se ha desarrollado el software de producción, se hará un pequeño aplicativo de prueba que se limite a repetir una serie de acciones relevantes para nuestra prueba.

5.4.- Definición de los métodos de prueba

En el entorno real, los eventos no suceden de una forma ordenada y, un determinado equipo que cumple unas determinadas condiciones controladas de laboratorio, puede no desenvolverse bien en nuestro entorno de aplicación real.

Se definirán las pruebas a efectuar en los equipos de forma que se adapten a la realidad del entorno más desfavorable en el que vayan a tener que operar. Es decir, se seleccionan en base a unos criterios que se eligen por separado (protección IP, resistencia a impactos, rangos de temperatura, etc..) que el fabricante certifica que cumple en laboratorio, pero que de ningún modo puede asegurar que en las condiciones más desfavorables de test se podrían soportar todos

ellos simultáneamente de forma repetida. Ese es el tipo de prueba que el diseñador de la solución deberá contemplar una vez seleccionados los terminales portátiles para la misma.

Ejemplo:

Se dispone de un equipo de un fabricante dotado de un lector de códigos de barras 1D y 2D, con una especificación IP65 de sellado y soportando una especificación de caídas de 1,8 m sobre hormigón específica del fabricante.

Preocupa el comportamiento del equipo ante caídas y exposiciones al agua intercaladas.

Cuando un equipo pasa los test de sellado o caídas, los pasa por separado, y nunca uno después del otro, sino que son equipos diferentes. Esto quiere decir que, el hecho de que un equipo tenga una especificación del fabricante de 1,8 m de caída sobre hormigón, no quiere decir que después de N caídas desde esa altura, se pueda volver a pasar las pruebas de sellado IP y dejar el equipo a la intemperie bajo la lluvia.

En el ejemplo que se detalla, se ha decidido someter al equipo al menos a 3 caídas desde 1,5 m (que se aproxima más a nuestra situación real), intercalando entre cada una sesiones de trabajo de al menos dos horas y una exposición al agua de lluvia de al menos 20 minutos.

Esta operativa se repetirá durante al menos 5 días, y reportará un total de 15 impactos y el mismo número de exposiciones al agua.

También preocupa la autonomía real que pueda dar el equipo seleccionado en nuestro caso concreto y, del mismo modo, las especificaciones del fabricante hablan de una autonomía de funcionamiento con un perfil de usuario tipo de 8 horas, que puede no ser relevante para nuestras pautas de funcionamiento con el equipo. En realidad, al diseñador de la solución le interesa saber cuál es la autonomía que el equipo va a dar con nuestras pautas de funcionamiento.

La aplicación de prueba será diseñada de modo que lea códigos de barras de unas cartulinas de prueba y simule la cadencia máxima del usuario, con periodos de descanso y transmisiones de datos a ráfagas a través de la red inalámbrica.

Si el equipo no cumple con lo esperado, hay dos opciones posibles:

- Volver al proceso de selección de terminales y elegir otro equipo al que ´se hará pasar igualmente por el proceso de prueba
- Establecer parámetros de funcionamiento, cambiar algún componente del sistema o accesorio, imponer restricciones o adoptar medidas de protección adicionales.

En las pruebas de los terminales, se emplearán las condiciones más exigentes y hará que todas ellas concurran de forma simultánea en base a criterios realistas.

6.- ESPECIFICACIONES DE DESARROLLO E INTEGRACIÓN SOFTWARE

Es importante resaltar algunas consideraciones a tener en cuenta a la hora de redactar las especificaciones del desarrollo y posterior integración de todo el software presente en los dispositivos portátiles.

6.1.- Interfaz de usuario

A diferencia de otros entornos de aplicación, el usuario no siempre tendrá la formación adecuada ni conocimientos informáticos mínimos (un operario de fábrica), y por lo tanto, el interfaz de usuario debe ser lo más claro y conciso posible. Se evitarán términos excesivamente técnicos y flujos de operación complicados. No es adecuado hacer navegar al usuario por todo un compendio de menús y pantallas repletas de opciones.

El software de aplicación debe recoger del usuario aquellos datos imprescindibles para su operación en el momento correcto.

6.2.- Diseño de una interfaz gráfica de usuario

Si se elige una interfaz gráfica para la aplicación, basada en formularios y cuadros de diálogo, estos deberán tener opciones accesibles mediante la pulsación directa, sin la ayuda de ningún apuntador incluso con guantes de trabajo puestos.

Para cumplir con esta premisa, todos los objetos visibles en la pantalla y accesibles por el usuario tales como botones, listas desplegables, cajas de entrada de datos deberán tener el tamaño apropiado, que no debería ser inferior a una caja cuadrada de 10 mm x 10 mm. En caso de otras formas en los objetos representados en la pantalla del dispositivo, la menor de su medidas no debería ser inferior a 10 mm. Aquí se deberá olvidar aquello que se ve en aplicaciones genéricas para uso por el gran público en dispositivos con Android o iOS en donde se emplean principalmente pantallas con interfaz táctil capacitivo.

En nuestros entornos profesionales se emplean pantallas con interfaz táctil resistivo debido a su gran resistencia y a no depender del contacto directo con los dedos del usuario o del uso de un puntero activo. Esto es vital para aplicaciones donde el usuario está en entornos fríos o en labores que requieren el uso de guantes de trabajo permanentemente, lo cual obligaría al usuario a tener que ponerse y quitarse los guantes para manipular el terminal portátil o a depender de un puntero activo para usar la pantalla si esta tuviese el interfaz táctil de tipo capacitivo.

Allí donde se emplee una entrada de datos intensiva, como por ejemplo un formulario en el que haya que introducir dos datos numéricos, se intentará automatizar esta entrada de datos mediante el uso de códigos de barras, de modo que el usuario no tenga que introducir esos datos físicamente o, en caso de no ser posible, como por ejemplo si hay que introducir el número de artículos de una determinada categoría que hay en una estantería, introducirlos mediante un teclado numérico. No hay que olvidar que este tipo de labores repetitivas sobre el digitalizador

del dispositivo provocarán un gran desgaste en el mismo y, a la larga, grandes costes de mantenimiento en nuestra solución. Por el contrario, existen teclados diseñados para estos dispositivos que aportan una resistencia excepcional y una mejor confirmación al tacto de los datos introducidos. De hecho la gran mayoría de estos dispositivos disponen de un teclado numérico y con algunas teclas de función especiales.

6.3.- Flujograma de operación del aplicativo del terminal

La opción más conveniente sería diseñar el flujograma de operación de nuestro aplicativo basado en una máquina de estados con memoria del estado de la última operación efectuada. Esta sería la operativa más fácilmente entendible por un usuario sin ningún tipo de formación informática ni experiencia previa en el uso de dispositivos portátiles.

Se utilizará una aplicación de ejemplo desarrollada para el reparto de paquetería por una flota de operarios en una empresa de transportes. Esta aplicación ha sido diseñada siguiendo la filosofía de la máquina de estados.

La aplicación de ejemplo se llama *Palm Delivery Assistant (PDA)* y su flujograma se puede ver en la ilustración (14).

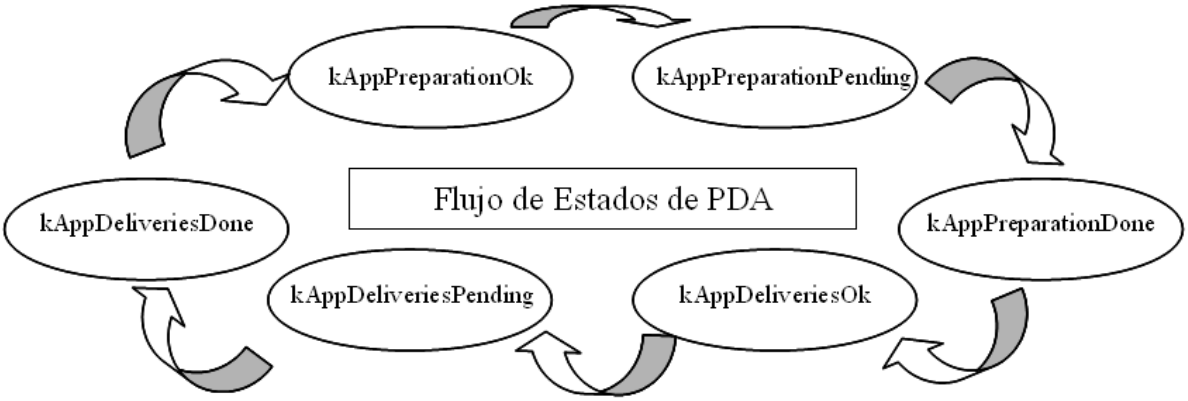

Ilustración 14: Flujograma de Aplicación de reparto de paquetería (PDA)

6.3.1.- El estado de la aplicación

A diferencia de lo que sucede con una aplicación ofimática estándar, en nuestro dispositivo portátil la aplicación podría quedar bloqueada en un punto y obligar al usuario al reinicio del dispositivo o incluso a perder los últimos datos introducidos que pueden no ser fácilmente recuperables. Imaginemos un entorno de alta rotación de vehículos, con gran exigencia de rapidez de transacción y una etiqueta de una caja de un vehículo que ya ha partido y, por lo tanto, no podemos leer de nuevo cuando la aplicación se queda bloqueada y se reinicia, perdiendo la última transacción en la que se estaba trabajando.

En la tabla (3) se muestra la definición de estados de la aplicación de ejemplo PDA.

Estado de la Aplicación	Valor	Descripción
kAppPreparationOk	1	Este será el estado con el que por defecto se inicie la aplicación por primera vez. Indica que la aplicación se encuentra en “Preparación para el reparto”.
kAppPreparationPending	2	La aplicación entrará en este estado justo antes de la sincronización de datos con el sistema. Este estado indicará a la máquina Host que tomará el control de la sincronización y que la aplicación estaba en preparación, que el usuario finalizó la preparación y que pretende enviar al sistema la preparación y recibir del mismo la información para el reparto
kAppPreparationDone	3	Este estado es establecido por el software de la máquina Host (PDAConduit) al finalizar la sincronización de datos de la preparación si dicha sincronización de datos ha sido llevada a cabo con éxito. En este estado PDA sabe que se ha sincronizado con éxito la preparación de datos y que la máquina Host ha cargado en dispositivo portátil la información para el reparto.
kAppDeliveriesOk	4	La aplicación PDA utiliza este estado en el dispositivo portátil para indicar que empieza la operativa de reparto. Antes de entrar en este estado requerirá una confirmación por parte del usuario.
kAppDeliveriesPending	5	La aplicación entrará en este estado justo antes de la sincronización de datos con el sistema. Este estado indicará a la máquina Host que tomará el control de la sincronización, que la aplicación estaba en reparto, que el usuario ha dado por finalizado la operación de reparto y que pretende enviar al sistema todos los datos resultado del reparto.
kAppDeliveriesDone	6	Este estado es establecido por el software de la máquina Host (PDAConduit) al finalizar la sincronización de datos del reparto si dicha sincronización de datos ha sido llevada a cabo con éxito. En este estado PDA sabe que se ha sincronizado con éxito los resultados del reparto y que por lo tanto puede pasar al siguiente estado de preparación.

Tabla 3: Estados de la aplicación de reparto de paquetería (PDA)

Será necesario tener en cuenta en todo momento el estado de la aplicación y recuperar el mismo en caso de desconexión por falta de alimentación (baterías agotadas), batería desprendida (tras un impacto) o por un fallo en un controlador de dispositivo o el sistema operativo que deje bloqueada la operación, o incluso debido a un fallo de la propia aplicación del terminal portátil. A poder ser, esto se realizará de forma transparente para el usuario, haciendo que cuando ponga las baterías o reinicie el dispositivo, la aplicación vuelva exactamente al punto en el que se encontraba antes del evento de bloqueo, y sin pérdida de datos.

En este punto, los fabricantes facilitan la labor al incorporar en los terminales portátiles memorias flash y una batería interna de respaldo que permite mantener los datos manejados en memoria mientras el usuario cambia la batería o reinicia el dispositivo. Aún así, se deberá ser especialmente cuidadoso con la gestión de la aplicación para sacar provecho de estas ventajas.

La pérdida del último punto de estado de la aplicación, debería ser un último recurso cuando la aplicación retorna de nuevo a un punto de bloqueo al recuperar el estado anterior. En ese caso, la salida a un punto neutro o pantalla principal de la aplicación debería producirse mediante una combinación especial de teclas o una opción de pantalla que requiera confirmación por parte del usuario.

7.- HERRAMIENTAS Y SISTEMAS DE DESARROLLO SOFTWARE

En este apartado se analizarán los principales sistemas de desarrollo software para dispositivos portátiles profesionales.

Antes de entrar en materia, será necesario ver cuales son las plataformas hardware y sistemas operativos que maneja la industria en este tipo de dispositivos.

Lejos quedan aquellos primeros dispositivos basados en MS-DOS y Windows 3.1 de sus inicios con grandes carencias de gestión de los recursos específicos del dispositivo móvil. Posteriormente, surgió una serie de dispositivos especialmente optimizados y derivados de la plataforma Palm OS, que durante un tiempo compartieron nicho de mercado con los sistemas basados en Windows CE, y que finalmente sucumbió a las plataformas de Microsoft con Windows Embedded en sus diferentes variantes para los entornos profesionales. Actualmente Windows Embedded es el sistema operativo incorporado en la inmensa mayoría de estos dispositivos.

- Microsoft® MS-DOS®
  - Microsoft® Windows® 3.1
  - Microsoft® Windows® Compact Embedded (Plataformas CE)
    - Microsoft® Windows® CE hasta versiones 2.xx
    - Microsoft® Windows® CE 3.0
      - **Microsoft® Windows® for Pocket PC 2002**
    - Microsoft® Windows® CE 4.0
      - Microsoft® Windows® CE .NET 4.2
        - **Microsoft® Windows® Mobile™ 2003 Software for Pocket PC (CE 4.2)**
      - Microsoft® Windows® CE .NET 4.21.111
        - **Microsoft® Windows® Mobile™ 2003SE Software for Pocket PC**
    - Microsoft® Windows® CE 5.0
      - **Microsoft® Windows® Mobile™ 5.0 Software for Pocket PC**
        - .NET Compact Framework 1.0 SP2
    - Microsoft® Windows® CE 6.0
      - **Microsoft® Windows® Mobile™ 6.0 / Windows Embedded Compact 6.0 R3**
        - Versiones Standard, Professional y Classic
      - **Microsoft® Windows® Mobile™ 6.1**

- **Microsoft® Windows® Mobile™ 6.5 (CE 6.5)**
  - **Windows® Embedded Handheld 6.5.3**
- **Microsoft® Windows® Embedded Compact 7 (CE 7.0)**
  - Expression Blend 3 + Silverlight + .NET

Ilustración 15: Evolución de Windows CE

En la ilustración (15) se puede apreciar la evolución de las plataformas "Embedded" generadas por Microsoft.

Cabe resaltar las principales evoluciones introducidas por Microsoft® en sus sistemas operativos *Embedded* como las siguientes:

- **Microsoft® Windows® CE 3.0**
  - Introducción del Sistema Operativo en Tiempo Real (Real-Time OS)
- **Microsoft® Windows® CE .NET 4.0 (CE 4.0)**
  - Introducción de emuladores para que el programador pudiese probar las aplicaciones en sus plataformas de desarrollo sin necesidad de cargarlas en los dispositivos
- **Microsoft® Windows® Mobile 5.0 for Pocket PC (CE 5.0)**
  - Primera plataforma abierta que permite a los fabricantes de dispositivos generar imágenes del sistema operativo modificadas y personalizadas sin asistencia de Microsoft
- **Microsoft® Windows® Embedded Compact 6.0 (CE 6.0)**
  - Introduce un nuevo kernel, redefinido para el nuevo sistema operativo, que permite la ejecución de más de 32K procesos con hasta 2GB de espacio de direccionamiento virtual para cada uno. También incluye un nuevo sistema de archivos que permite mayores medios de almacenamiento y el uso de ficheros de mayor tamaño

7.1.- SDK y herramientas de Microsoft para Windows Mobile y Windows CE

Para todas las plataformas Windows CE, las herramientas de desarrollo software son las proporcionadas por Microsoft, principalmente el compilador (Visual Basic, Visual C++, Visual C#....) y el SDK específico para la plataforma de Windows CE en cuestión.

Adicionalmente, los fabricantes de dispositivos aportan librerías y SDKs adicionales que permiten acceder a las funcionalidades extra de sus dispositivos, entre las cuales cabe destacar: gestión de red inalámbrica, gestión de red celular, utilización de lectores de códigos de barras (1D y 2D), bandas magnéticas, configuración y optimización de la alimentación del terminal portátil, así como sus recursos hardware y software.

El entorno de desarrollo necesario para la plataforma Microsoft® Visual Studio® 2005 o superior.

En la versión de Visual Studio 2008 ya vienen incluidos los SDKs necesarios para desarrollar aplicaciones para dispositivos genéricos basados en plataformas Pocket PC 2003, Windows CE, Windows Mobile 5.0 tanto para teléfonos como para dispositivos Pocket PC.

Desgraciadamente, la versión 2010 de Visual Studio no soporta ni incorpora los SDK para desarrollar sobre dispositivos basados en Windows CE del tipo handheld, unicamente sobre smartphones, con lo cual este libro ha tenido que ser escrito basado en la versión 2008 del entorno de desarrollo software. A fecha de escritura del presente libro, se desconoce si Microsoft ha resuelto esta inconsistencia en la nueva versión de Visual Studio 2012.

7.1.1.- ActiveSync o Windows Mobile Device Center

Asumiendo que se trabaja con dispositivos basados en Windows Mobile 2003 o superior, se deberá tener instalado *ActiveSync* en el equipo de desarrollo, pero si el equipo tiene Windows Vista / 7 y/o se utilizan dispositivos con Windows Mobile 6 o superior, en vez de *ActiveSync* se deberá disponer del *Centro de Dispositivos de Windows Mobile*. Será una máquina con una versión de Windows de 32 o 64 bits, y por lo tanto, deberá tener la correspondiente variante de *Windows Mobile Device Center*.

Ilustración 16: Windows Mobile Device Center

En la ilustración (16) que se muestra, se puede apreciar la pantalla de configuración de la conexión con un dispositivo móvil. Básicamente, será necesario indicar como se van a producir las conexiones de los dispositivos móviles que se conecten con nuestro equipo (Bluetooth o DMA), y si se está conectado a una red o directamente a Internet.

Una vez que se dispone de *Windows Mobile Device Center* y de la plataforma de desarrollo Visual Studio correctamente instalados en nuestro sistema, se podrá descargar aquellos SDK que no vengan ya con el entorno de Microsoft. En este caso, Visual Studio 2008 no trae por defecto los SDK para plataformas Windows Mobile 6.0 o superior, los cuales tendrán que ser descargados desde el sitio web de Microsoft e instalados en el equipo de desarrollo.

http://www.microsoft.com/es-es/download/default.aspx [CMCSFT1]

Los componentes y SDKs en el orden en el que se deberán instalar serán:

1. Windows Mobile 6.0 SDK (Software Development Kit) Standard
2. Windows Mobile 6.0 SDK Professional
3. Windows Mobile 6.1.4 Standard Emulator Images
4. Windows Mobile 6.1.4 Professional Emulator Images
5. Windows Mobile 6.5 DTK (Developer Tool Kit) Standard
6. Windows Mobile 6.5 DTK Professional
7. Windows Mobile 6.5.3 DTK Standard
8. Windows Mobile 6.5.3 DTK Professional
9. Windows Mobile 6.5.3 Standard Emulator Images
10. Windows Mobile 6.5.3 Professional Emulator Images

En nuestro panel de control deberían estar instalados los siguientes paquetes:

Windows Mobile 5.0 SDK R2 for Pocket PC	Microsoft Corporation	28/06/2012	128 MB	5.00.1700.5.14343.06
Windows Mobile 5.0 SDK R2 for Smartphone	Microsoft Corporation	28/06/2012	79,2 MB	5.00.1700.5.14343.06
Windows Mobile 6 Professional SDK	Microsoft Corporation	17/08/2012	909 MB	6.0.0.17740
Windows Mobile 6 Standard SDK	Microsoft Corporation	17/08/2012	474 MB	6.0.0.17740
Windows Mobile 6.1.4 Professional Emulator Images - USA	Microsoft Corporation	17/08/2012	775 MB	6.1.4.20757
Windows Mobile 6.1.4 Standard Emulator Images - USA	Microsoft Corporation	17/08/2012	581 MB	6.1.4.20757
Windows Mobile 6.5 Professional Developer Tool Kit - USA	Microsoft Corporation	17/08/2012	489 MB	6.5.0.21234
Windows Mobile 6.5 Standard Developer Tool Kit - USA	Microsoft Corporation	17/08/2012	195 MB	6.5.0.21234
Windows Mobile 6.5.3 Professional DTK	Microsoft Corporation	17/08/2012	858 MB	6.5.3.23090
Windows Mobile 6.5.3 Professional Emulator Images - ESP	Microsoft Corporation	17/08/2012	678 MB	6.5.3.23090
Windows Mobile 6.5.3 Standard DTK	Microsoft Corporation	17/08/2012	554 MB	6.5.3.23090
Windows Mobile 6.5.3 Standard Emulator Images - ESP	Microsoft Corporation	17/08/2012	385 MB	6.5.3.23090

Ilustración 17: SDKs de Windows Moblie 5.y 6.x en el Panel de Control

Una vez instalado todo el sistema de desarrollo software de Microsoft, solamente faltará instalar los SDKs y herramientas específicos del dispositivo que se vayam a programar y que serán provistas por el fabricante del dispositivo.

En el árbol de aplicaciones *"Inicio"* del menú de Windows de nuestra máquina de desarrollo, habrá dos directorios Windows Mobile 6 SDK y Windows Mobile 6.5.3 DTK con las subcarpetas correspondientes a cada uno de ellos.

Hay que resaltar que el DTK 6.5.3 es una actualización del SDK de Windows Mobile 6 y, aunque aparece separado, algunos elementos como las imágenes para el emulador del sistema 6.5.3 son instaladas dentro de la estructura de SDK en la carpeta *"Standalone Emulator Images"*.

Ahora que se dispone de todas las herramientas y SDK/DTK instalados, es posible abrir un proyecto existente o crear un nuevo proyecto dentro de Visual Studio específico para plataformas móviles.

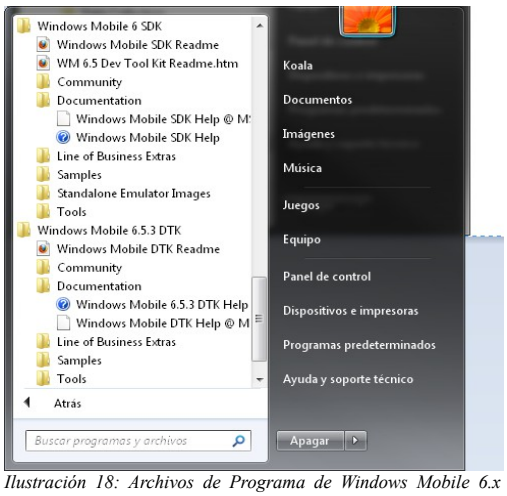

Ilustración 18: Archivos de Programa de Windows Mobile 6.x SDK y DTK

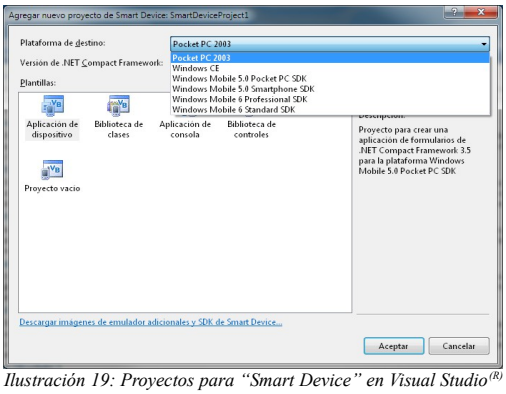

Ilustración 19: Proyectos para "Smart Device" en Visual Studio(R) 2008

Dentro de Visual Studio, este tipo de proyectos son proyectos para "*SmartDevice*", y dentro de ese apartado, se puede seleccionar el sistema operativo del dispositivo objetivo en el que se ejecutará la aplicación. En la ilustración (19) que se muestra se observa como el usuario puede elegir entre las diferentes plataformas CE, Pocket PC 2003 o superior. Hay que tener en cuenta que las aplicaciones para la plataforma Embedded Handheld 6.5.x están incluidas dentro del apartado Windows Mobile 6.

7.2.- Herramientas de desarrollo software de Intermec

Intermec provee varias herramientas y un conjunto de librerías para sus diferentes plataformas de dispositivo.

Estas herramientas y librerías son suministradas en forma de paquetes independientes, cada uno de ellos relacionado con diferentes funcionalidades y recursos específicos de sus dispositivos.

El conjunto de librerías y herramientas suministrado por Intermec se denomina *IDL (Intermec Developer Library) Resource Kits*.

Todos estos IDL Resource Kits están diseñados para ser utilizados con las herramientas de desarrollo software de Micrososft: eMbedded Visual C++ 4.0, Visual Studio 2005 y Visual Studio 2008.

Desafortunadamente, Visual Studio 2005 o 2008, que serían las opciones lógicas para un sistema de desarrollo software actual (Ya que 2010 no está ni se le espera .. con Windows Mobile) no soportan el desarrollo de aplicaciones para plataformas anteriores a *Windows Mobile 2003 for Pocket PC*.

La IDL de Intermec da soporte a toda su gama de dispositivos basados en las siguientes plataformas de sistema operativo:

- Windows Embedded Handheld 6.5
- Windows Mobile® 6.0 y 6.1
- Windows Mobile 5.0
- Windows Mobile 2003
- Windows CE 4.2 y 5.0
- Windows XP y XP Embedded

Sistema Operativo Plataformas CE	Equipos de Intermec (Mobile Computers)
Microsoft Windows Mobile for Pocket PC	730
Microsoft Windows CE .NET	CK30C
Microsoft Windows CE .NET 4.2	CK30A, CK30B, CK31 y CK31ex
Microsoft Windows Mobile 2003 for Pocket PC	741B, 751B, 761B y CN2B
Windows CE 5.0	CK61
Microsoft Windows Mobile 5.0	CK61, CN3, CN3e, CK32-IS
Microsoft Windows Mobile 6.1	CN3, CN3e, CN4, CN4e, CN50, CK3
Microsoft Windows Mobile 6.5	CS40, CN50
Microsoft Windows Embedded Handheld 6.5.3	CS40, CN50, CN70, CN70e, CK70, CK71

Tabla 4: Sistemas Operativos Windows CE en terminales de Intermec

Para instalar la IDL de Intermec es requisito previo tener instalado Visual Studio 2005 o 2008 y los SDK correspondientes a las plataformas CE a utilizar.

La IDL de Intermec está compuesta por los siguientes Resource Kits que se descargan por separado de la web del fabricante.

http://www.intermec.com/support/downloads/index.aspx [CINTERM1]

7.2.1.1.- IDL Resource Kit – Bluetooth™

Para gestionar las comunicaciones entre dispositivos móviles Intermec dotados de Bluetooth y dispositivos tales como periféricos u otras computadoras.

7.2.1.2.- IDL Resource Kit – Communications

Para configurar la funcionalidad de red 802.11, incluyendo las opciones de perfil de usuario y seguridad.

7.2.1.3.- IDL Resource Kit - Data Collection

Para hacer uso de las tecnologías de captura de datos incorporadas en los dispositivos, lectores de códigos de barras (1D y 2D), Imagers y lectores de banda magnética, así como la gestión y manipulación de los datos obtenidos de estos dispositivos.

7.2.1.4.- IDL Resource Kit – Device

Para configurar y gestionar parámetros específicos del hardware del dispositivo tales como audio del beeper, retroiluminación de la pantalla y mapeado del teclado.

7.2.1.5.- IDL Resource Kit - Device Management

Para configurar los dispositivos portátiles con capacidad de utilizar el sistema SmartSystems de Intermec desde la aplicación a través del API de SmartSystems™.

7.2.1.6.- IDL Resource Kit - Mobile Gadgets

Para añadir a la aplicación funcionalidades com la captura de firma electrónica o botones personalizados para aplicaciones móviles.

7.2.1.7.- IDL Resource Kit – Printing

Para configurar y comunicar con impresoras de Intermec y otras impresoras de tickets.

7.2.1.8.- IDL Resource Kit – RFID

Para gestionar y configurar los dispositivos móviles dotados de lector RFID además de leer y escribir RFID.

7.2.1.9.- IDL Resource Kit – Mutimedia

Permite gestionar y utilizar los elementos multimedia del dispositivo tales como la cámara de vídeo/fotográfica y las posibles salidas de sonido como altavoces.

7.2.1.10.- IDL Resource Kit – Location Services

Permite gestionar y utilizar los servicios de localización como el GPS en aquellos equipos que lo soporten.

7.2.1.11.- IDL Resource Kit - Antares Migration

Permite compilar una aplicación Trakker Antares® (u otra aplicación basada en caracteres) para su uso en los nuevos equipos de Intermec.

Si se instalasen todos los kits en el equipo de desarrollo, el nuestro panel de control aparecerían como se muestra en la ilustración (20).

Intermec Antares Migration Resource Kit v3.23.01.0001	Intermec	18/08/2012	17,6 MB	3.23.01.0001
Intermec Bluetooth Resource Kit v3.42.01.0001	Intermec	15/08/2012	27,6 MB	3.42.01.0001
Intermec Communications Resource Kit v3.41.01.0001	Intermec	15/08/2012	15,7 MB	3.41.01.0001
Intermec Data Collection Resource Kit v3.70.00.0183	Intermec	15/08/2012	47,6 MB	3.70.00.0183
Intermec Device Management Resource Kit v3.41.00.0086	Intermec	15/08/2012	22,9 MB	3.41.00.0086
Intermec Device Resource Kit v3.90.00.0176	Intermec	15/08/2012	21,4 MB	3.90.00.0176
Intermec IDL Multi Kit Installer	Intermec	18/08/2012	5,70 MB	1.01
Intermec Location Services Resource Kit v1.21.00.0218	Intermec	15/08/2012	10,6 MB	1.21.00.0218
Intermec Mobile Gadgets Resource Kit v3.32.01.0041	Intermec	15/08/2012	14,5 MB	3.32.01.0041
Intermec Multimedia Developer Resource Kit v1.32.00.0079	Intermec	18/08/2012	8,45 MB	1.32.00.0079
Intermec Printing Resource Kit v3.60.00.0103	Intermec	15/08/2012	14,0 MB	3.60.00.0103
Intermec RFID Resource Kit v3.41.00.0056	Intermec	15/08/2012	18,3 MB	3.41.00.0056

Ilustración 20: IDL Resource Kits en el Panel de Control de Windows

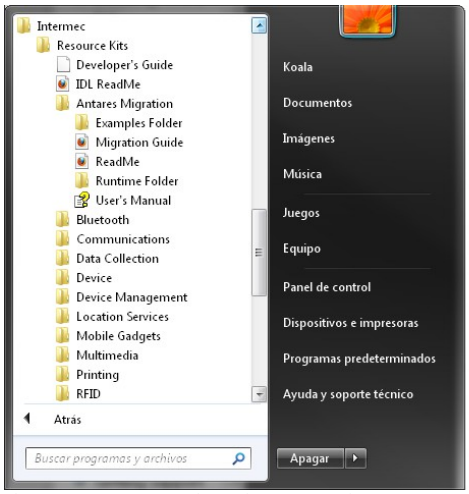

Ilustración 21: Menu Archivos de Programa de IDL Intermec

El desarrollador puede instalar únicamente aquellos kits que contengan la funcionalidad que va a utilizar en el dispositivo objetivo de su aplicación. Así pues, una aplicación que simplemente va a hacer uso del lector de códigos de barras de un dispositivo y configurar algunos aspectos específicos del hardware tales como la iluminación de la pantalla o el mapeado del teclado, simplemente necesitará instalar los IDL Resource Kits *"Device"* y *"Data Collection"*.

Desde el árbol de aplicaciones del menú de Windows de la máquina de desarrollo se podrá acceder a un directorio Intermec con las subcarpetas correspondientes a cada Resource Kit instalado de la IDL.

Cada Kit de la IDL viene con su manual de usuario, ejemplos en la carpeta *Examples Folder*, y los componentes run-time de las librerías para cada plataforma hardware específica dentro de *Runtime Folder.*

En nuestra computadora de desarrollo, cada Resource Kit de la IDL (salvo que se indique otra cosa en el programa de instalación) es instalado en un subdirectorio colgando de *C:\Program Files (x86)\Intermec\Developer Library.*

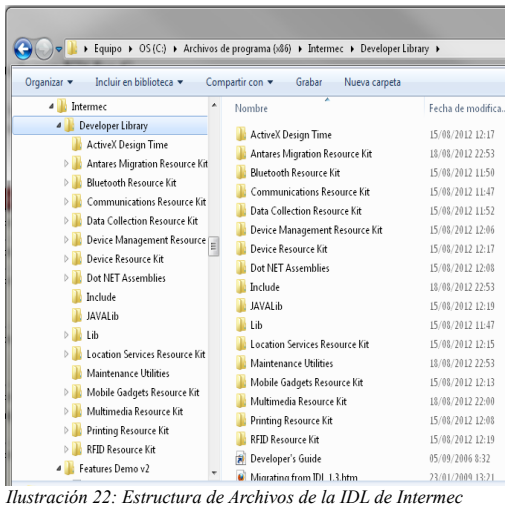

Ilustración 22: Estructura de Archivos de la IDL de Intermec

7.3.- Herramientas de desarrollo software de Motorola

Motorola provee de una serie de Kits de Desarrollo software para cada tipo de plataforma de desarrollo. Estos Kits de desarrollo específicos para sus dispositivos, son denominados EMDK (Enterprise Mobility Developer Kit) y existen tres EMDK diferentes para cada plataforma de desarrollo software (C, Java y .NET). Contienen todas las herramientas necesarias en cada plataforma de desarrollo para acceder a las funciones específicas de sus dispositivos tales como el audio, Bluetooth, display, WLAN, WWAN, captura de imagen, lectura de códigos de barras, administración del dispositivo y energía, entre otras.

Las EMDKs de Motorola dan soporte a toda su gama de dispositivos basados en las siguientes plataformas de sistema operativo:

Sistema Operativo Plataformas CE	Equipos de Motorola (Handheld Mobile Computers)
Windows CE 5.0	MC1000, MC17, MC3000, MC9000, MC9090
Windows CE 6.0	MC2100, MC3100, MC9100
Microsoft Windows Mobile 5.0	MC70, MC9000, MC9090, MC9090-RFID
Microsoft Windows Mobile 6.0/6.1	MC3000, MC3090Z, MC3100, MC55, MC70, MC75, MC9090, MC9090Z, MC9500
Microsoft Windows Mobile 6.5	ES400, MC3100, MC3190Z, MC55, MC55A, MC55N, MC65, MC75, MC9100, MC9500

Tabla 5: Sistemas Operativos Windows CE en terminales de Motorola

Los siguientes EMDKs pueden ser descargados de la web de Motorola Solutions:

http://support.symbol.com/support/product/softwaredownloads.do [MOTOSOL1]

7.3.1.- EMDK v2.5 for C

Contiene una serie de APIs contenidas en una librería de C, para su uso en las aplicaciones de dispositivo. Este EMDK ha sido especialmente concebido para su uso con Microsoft Visual Studio 2005 y 2008.

La instalación de este SDK en el equipo de desarrollo no requiere ninguna actuación más allá de seguir los pasos del instalador.

Para instalar este EMDK de Motorola es requisito previo tener instalado Visual Studio 2005 o 2008 y los SDK correspondientes a las plataformas CE a utilizar.

Hay una actualización "*Update 1"* para el "*EMDK v2.5 for C"* que deberá también ser descargado y con la que actualizará este EMDK.

7.3.2.- EMDK v2.5 for Java

Permite desarrollar aplicaciones en Java para los terminales portátiles.

Requiere tener previamente instalado el *Java Developer Kit (JDK)* correspondiente a la plataforma Win32 (32 bits). Se puede descargar desde la siguiente ubicación en la web de Oracle:

http://www.oracle.com/technetwork/java/javase/downloads/index.html [CORJAVA]

Si se decide desarrollar la aplicación con Java, no hay que olvidar que en los dispositivos objetivo de la aplicación deberá existir una JVM (Java Virtual Macnine). En la documentación de Motorola se habla de dos JVM aceptadas (testadas y probadas) para las aplicaciones Java en sus dispositivos. Se trata de:

- Eclipse 3.4 SDK (IDE) plataforma de desarrollo Java y WEME (IBM J9) JVM en los dispositivos portátiles
- NetBeans IDE 6.0 plataforma de desarrollo sofware con Java y NSIcom CrE-ME JVM en los terminales portátiles

Para más información sobre su instalación y configuración se puede ver el documento *"Eclipse and NetBeans Programmer's Guide"*.

7.3.3.- EMDK v2.5 for .NET Compact Framework 2.0 y 3.5

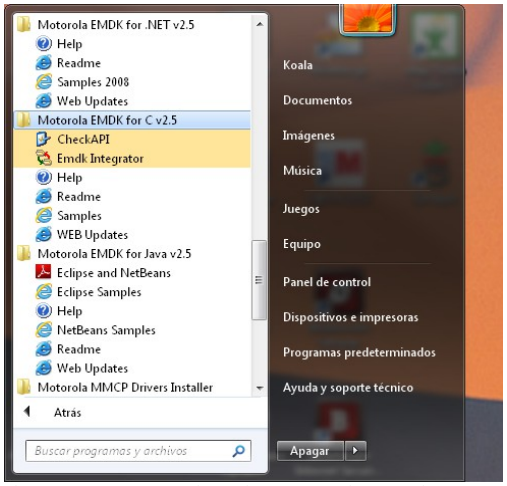

Ilustración 23: Menu Archivos de Programa de Motorola EMDKs

Permite desarrollar aplicaciones en Visual Basic .NET y Visual C# mediante Visual Studio 2005 o 2008.

Con Visual Studio se pueden generar aplicaciones basadas en CF 2.0 y con Visual Studio 2008 podrán ser generadas tanto para CF 2.0 como CF 3.5, seleccionable a la hora de crear el proyecto.

Para instalar este EMDK de Motorola es requisito previo tener instalado Visual Studio 2005 o 2008 y los SDK correspondientes a las plataformas CE a utilizar.

Hay una actualización "*Update 1*" para el "*EMDK v2.5 for .NET*" que deberá también ser descargado y con la que se procederá a actualizar este EMDK.

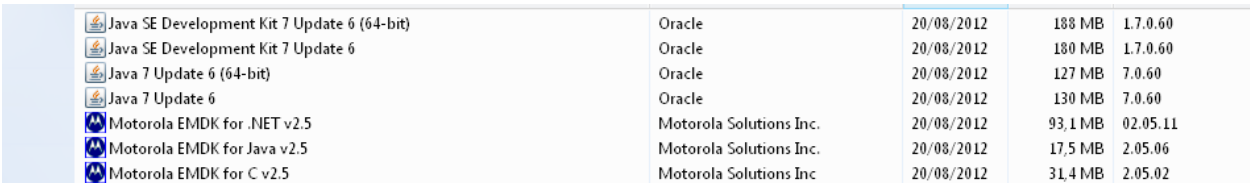

Ilustración 24: Motorola EMDKs en el Panel de Control

Una vez instalados los JDK y los EMDK de Motorola, en nuestro panel de control de Windows aparecerán instalados como se muestra en la siguiente ilustración (24).

Desde el árbol de aplicaciones "Inicio" del menú de Windows de nuestra máquina de desarrollo, se tendrá acceso a un directorio "*Motorola EMDK for ... "* con las subcarpetas correspondientes a cada EMDK instalado. En este caso, han sido instalados los tres kits de desarrollo.

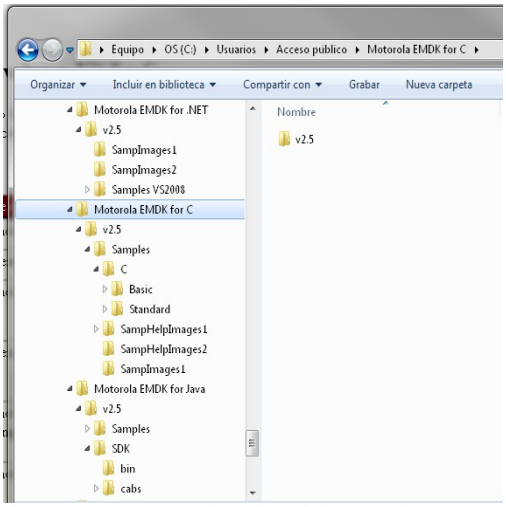

Ilustración 25: Estructura de Archivos de los Motorola EMDKs

Cada EMDK viene con su enlace a ayuda, ejemplos y actualizaciones. Estos EMDKs son instalados (si no se especifica otra cosa en el momento de la instalación), en subdirectorios colgando de *C:\Users\Public*.

En nuestro caso, al haber instalado los tres kits de desarrollo software, se tendrá en esa ubicación tres subdirectorios con el contenido de cada EMDK:

- Motorola EMDK for C,
- Motorola EMDK for .NET
- Motorola EMDK for Java

7.3.4.- Motorola System Configuration Manager (SCM)

SCM es un aplicación para el entorno desktop de desarrollo software que permite editar y generar archivos de configuración para los diferentes terminales portátiles de Morotola. Originalmente su nombre era el de la compañía absorbida posteriormente por Morotola y que era el fabricante original de todos estos dispositivos y tecnologías (Symbol Technologies Inc.). De hecho, las librerías, APIs, y otra documentación de desarrollo todavía hace referencia a los paquetes generados por Symbol.

7.4.- Wavelink Studio®

Wavelink Studio® [WLSTUD] es una herramienta multiplataforma de Wavelink Corporation orientada a la generación de soluciones en red con una arquitectura cliente-servidor basada en servidores de aplicaciones y clientes livianos (*Thin-Client),* con pocos requerimientos de capacidad de proceso y almacenamiento, que lanzarán y ejecutarán las aplicaciones en el servidor y tendrán un interfaz de usuario para representar los resultados de los aplicativos y recoger la interacción del usuario y los dispositivos de captura de datos del terminal.

Se ha desarrollado e implementado en Wavelink Studio® un protocolo de aplicación propio, diseñado especialmente para operar con redes inalámbricas y terminales portátiles, y permite que, utilizando un aplicativo cliente de Wavelink Studio®, los terminales puedan ejecutar aplicaciones en el servidor remoto, recoger datos, enviarlos y visualizar en pantalla sus resultados.

Ilustración 26: Sistemas Operativos de Servidor para Wavelink Studio®

Mediante Wavelink Studio® se pueden desarrollar aplicaciones utilizando JAVA y COM específicamente diseñadas para terminales portátiles con sistemas avanzados de captura de datos tales como, lectura de códigos de barras, tarjetas inteligentes y otros, utilizando las funcionalidades específicas de los dispositivos.

Wavelink Studio® existe para diferentes sistemas operativos para el servidor de aplicaciones:

- Microsoft® Windows®
- Unix
- Linux

Wavelink Studio® permite que estas aplicaciones se ejecuten independientemente del tipo de dispositivo sobre la gran mayoria de dispositivos presentes en el mercado.

Ilustración 27: Terminales portátiles soportados por Wavelink Studio®

Actualmente Wavelink Corporation reporta millones de licencias en el mercado, lo cual le convierte en una de las principales herramientas de desarrollo multiplataforma tipo *Thin-Client* para terminales portátiles.

Se puede acceder a la lista de dispositivos soportados en el siguiente enlace de la web de Wavelink [CWLSTERM]:

http://www.wavelink.com/p/mobile-device-application-development_supported-devices

Wavelink Studio® ha sido específicamente diseñado para soportar aplicaciones que requieren datos en tiempo real para operaciones en áreas como retail, gestión de almacén, control de inventario, automatización de fábricas, transporte y logística, aunque sin excluir otros entornos posibles de aplicación.

7.4.1.- Arquitectura de red de Wavelink Studio®

Wavelink Studio® utiliza una estructura de red tipo cliente-servidor basada en el modelo *Thin-Client* y, es en la parte cliente en la cual Wavelink utiliza un módulo de software específico para cada dispositivo que proporciona los controladores que acceden al hardware específico de cada dispositivo e interaccionan con el software cliente para proveer aquellas funcionalidades que son únicas y específicas del terminal portátil como puede ser el lector de códigos de barras, de tarjetas, el zumbador, el vibrador, la retroiluminación de la pantalla, la gestión de la energía, etc...

Una representación de bloques de la arquitectura de red de Wavelink es la que se puede ver en la ilustración (28) que se muestra a continuación.

Ilustración 28: Arquitectura de Red de Wavelink Studio®

Wavelink Studio® tiene cuatro componentes:

- Wavelink Development Library
- Wavelink Server
- Wavelink Program Manager
- Wavelink Client

7.4.2.- Instalación de Wavelink Studio®

Este software deberá ser instalado en la máquinaque actuará como servidor de aplicaciones y sobre el cual se desarrollará el aplicativo software.

Para instalar la plataforma de desarrollo software, previamente será necesario descargar el correspondiente programa de instalación según el sistema operativo del servidor.

Es posible descargar Wavelink Studio® desde el siguiente enlace [CWLSTDOW]:

http://www.wavelink.com/Download-Studio_mobile-device-application-development-Software

En este caso se ha elegido la plataforma Windows, por lo tanto se descarga el instalador

Wavelink Studio COM Server v3.70-00

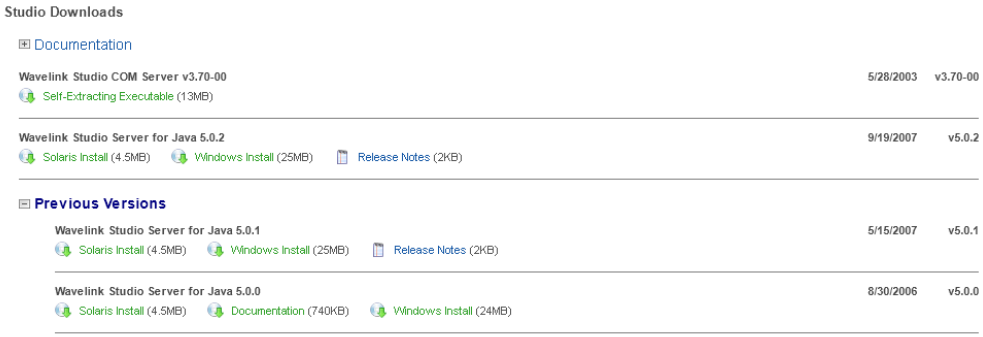

Ilustración 29: Descargas de Wavelink Studio

Se seguirán los pasos que indica el instalador e instalarán todos sus componentes.

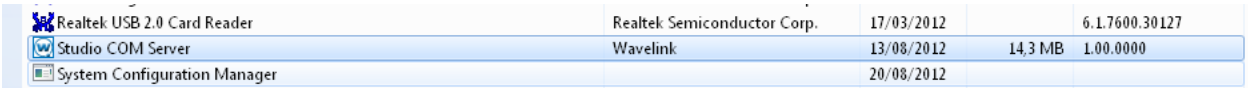

Ilustración 30: Wavelink Studio COM Server en el Panel de Control

Como se puede observar en la ilustración (30), el paquete aparece como *Studio COM Server.*

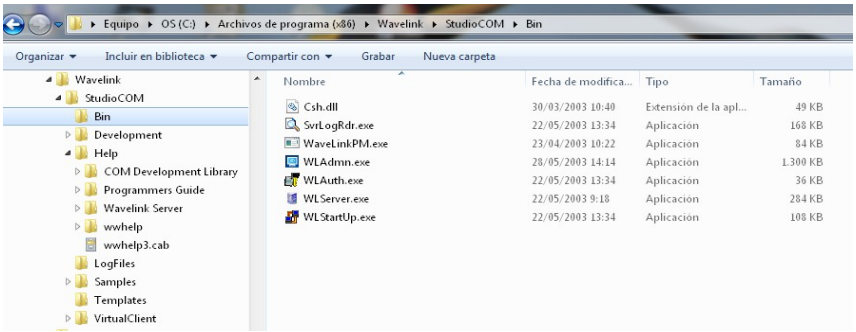

Ilustración 31: Estructura de Archivos de Studio COM Server

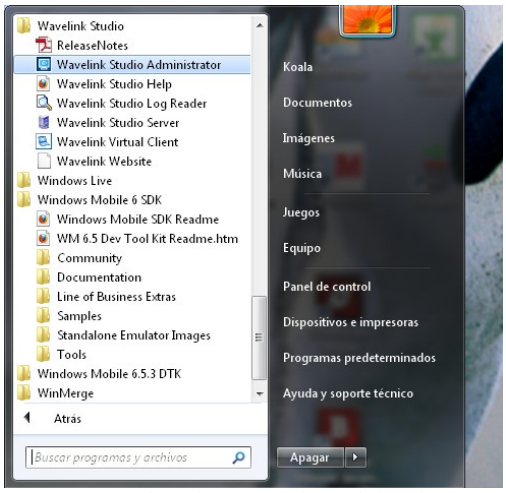

Ilustración 32: Archivos de Programa de Wavelink Studio

En el menú de archivos de Windows aparecerán los siguientes accesos a programas:

- Wavelink Studio Help
- Wavelink Studio Administrator
- Wavelink Studio Server
- Wavelink Studio Virtual Client

En la ilustración (31) se puede apreciar la estructura de archivos donde se encuentran los programas de Wavelink en el sistema de archivos de la máquina Windows.

7.4.2.1.- Wavelink Development Library

Se trata de una integración de JAVA y librería COM para redes y dispositivos inalámbricos. Utiliza lenguajes de programación orientada a objetos como Java, Visual Basic y Visual C++.

7.4.2.2.- Wavelink Server

Se trata del módulo que ejecuta y da servicio a las aplicaciones software en el servidor. Este módulo en sí mismo no tiene interfaz de usuario y simplemente es un servicio que se ejecuta en el servidor y da acceso a toda la funcionalidad de los módulos COM.

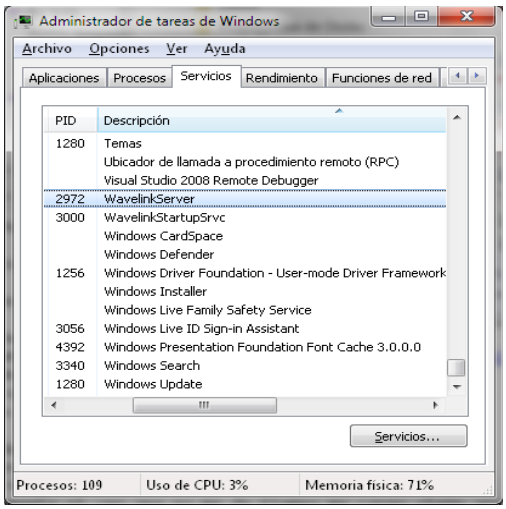

Ilustración 33: Servicio Windows de Wavelink Server

7.4.2.3.- Wavelink Administrator

Es el software que permite configurar y gestionar las conexiones con el servidor COM y, a través del Program Manager configura y despliega aplicaciones software junto con sus privilegios de acceso.

7.4.2.3.1.- Configuración de Wavelink Administrator

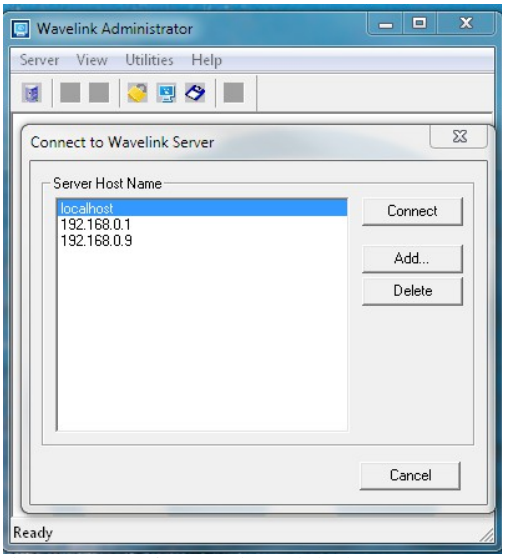

Ilustración 34: Configuración de Wavelink Administrator

El primer paso a dar para trabajar con Wavelink es configurar la conexión con un servidor. No hay que olvidar que pueden existir varios servidores de aplicaciones con Wavelink.

En la ilustración (34) se observa la pantalla de conexión de WaveLink Administrator. En esta pantalla es posible añadir una conexión nueva con el botón *Add.*

Bastará con poner el nombre de la máquina en su dominio de Internet o directamente su dirección IP.

En este ejemplo, se puede acceder a través del nombre *localhost* o la dirección IP *192.168.0.9.*

Una vez que existe una conexión a una máquina correctamente configurada, Wavelink Administrator lanzará un monitor sobre la misma y la mostrará como se puede apreciar en la ilustración (35). En esta pantalla de información sobre la conexión, se puede ver si se trata de una conexión serie o TCP. En este caso es TCP en el puerto 2001 (predeterminado por Wavelink).

Ahora que Wavelink Administrator está conectado, cualquier conexión de un dispositivo con WaveLink Server, incluso si se trata del Cliente Virtual aparecerá colgando del tipo de conexión con la que se efectúa. Enel ejemplo que se trata, se lanza el cliente virtual de Wavelink para simular una conexión con el servidor y se puede monitorizar su actividad.

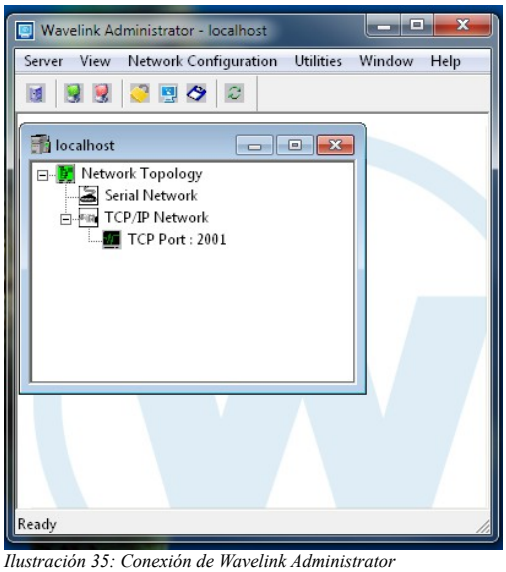

Ilustración 35: Conexión de Wavelink Administrator

7.4.2.4.- Wavelink Client

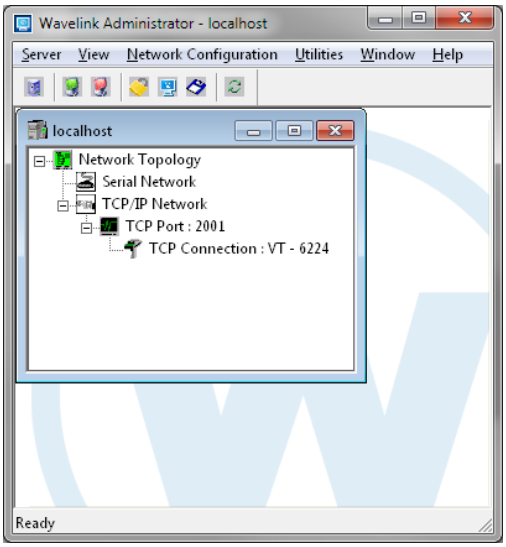

Ilustración 36: Wavelink Administrator con conexiones activas

Se instala y funciona en el terminal portátil y permite desde el mismo ejecutar de forma remota la aplicación del servidor y, al mismo tiempo, utilizar las tecnologías propias del terminal portátil para gestionar la captura de datos (lectura de códigos de barras, tarjetas inteligentes, ...) y todos los aspectos propios y específicos del dispositivo. Para que una aplicación de Wavelink pueda acceder a las funciones específicas del dispositivo (scanner, batería, red inalámbrica, …).

Para facilitar la labor de desarrollo software sin tener que probar las aplicaciones sobre los dispositivos, Wavelink Studio® proporciona un Emulador tipo Cliente Virtual en el que se pueden probar las aplicaciones antes de telecargarlas en el dispositivo.

7.4.2.4.1.- Wavelink Virtual Client

Se trata de una utilidad para el desarrollador de software que permite probar la aplicación en el servidor como si se tratase de un terminal portátil remoto.

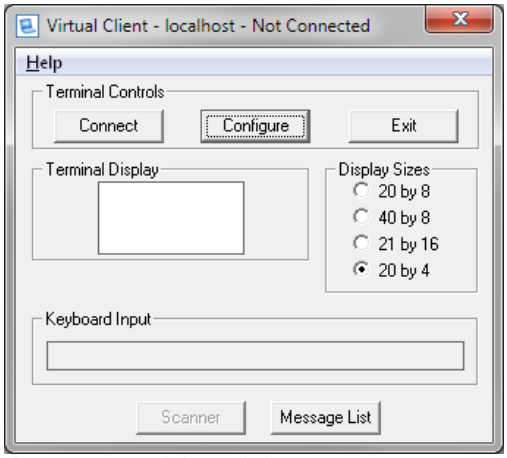

Ilustración 37: Wavelink Virtual Client

Al iniciar *Wavelink Virtual Client* aparece la pantalla que se muestra en la ilustración (37).

En este emulador de terminal es posible cargar una aplicación y simularla como si se estuviese ejecutando en un terminal portátil remoto.

Las configuraciones de pantalla que muestra vienen expresadas en caracteres x filas. Esto quiere decir que el tipo de pantalla (20 by 8) correspondería a un dispositivo con una pantalla que representaría 8 líneas de texto con 20 caracteres por línea.

7.4.2.4.1.1.- Configuración de Wavelink Virtual Client

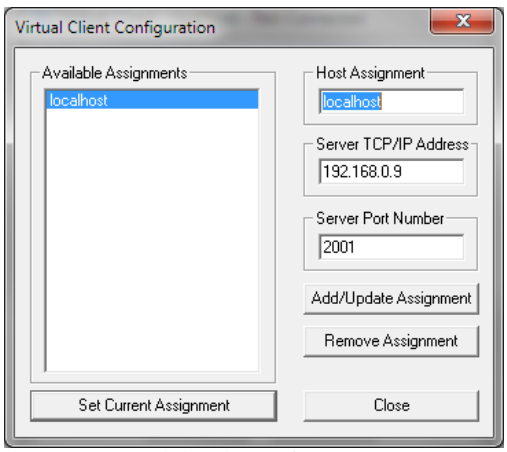

Ilustración 38: Wavelink Studio - Configuración

Existe esta sencilla pantalla de configuración que se muestra, en la cual se podrá indicar los parámetros de la conexión con el servidor de Wavelink Studio.

Básicamente se trata de indicar el nombre del servidor y su dirección IP, así como el puerto de conexión (por defecto 2001).

Una vez configurada la aplicación, se conectará al servidor de Wavelink (Connect) y tendrá opción de ejecutar la aplicación que se haya seleccionado para el dispositivo.

7.4.2.4.1.2.- Ejecución de Wavelink Virtual Client

En este caso, se ha lanzado una de las aplicaciones de demo incluidas con Wavelink (*VB Barcode Demo*), que es la que se muestra en la ilustración (39).

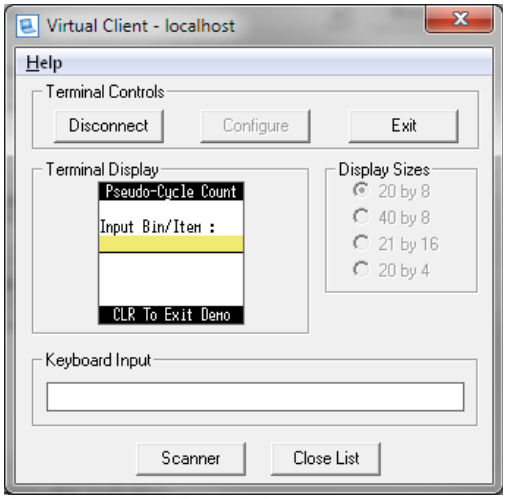

Ilustración 39: Wavelink Virtual Client en ejecución

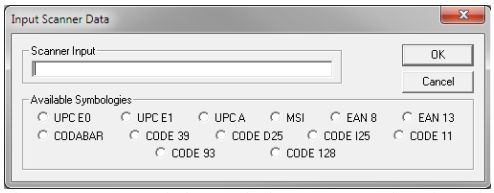

Ilustración 40: Wavelink Virtual Client - Captura de códigos de barras

Además de ejecutar la aplicación, es posible simular entradas de datos por teclado o mediante captura de códigos de barras y se dispone de cuatro configuraciones posibles de tamaño de pantalla (en modo texto).

Detalle de mensajes intercambiados

También se podrán ver los mensajes exactos que se intercambian el cliente Wavelink con el servidor de aplicaciones y sus diferentes parámetros. Esta pantalla aparece con la opción *Message List.*

Si se desglosa cada parte del mensaje intercambiado es posible ver incluso los atributos de visualización o de captura en el terminal portátil. Todos estos mensajes son específicos del protocolo de intercambio de datos de Wavelink.

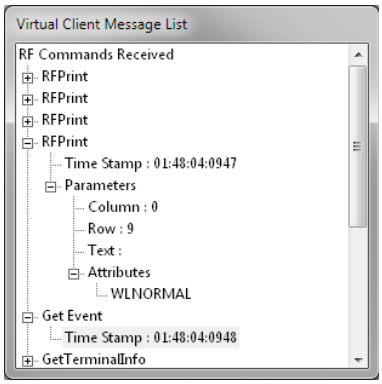

Ilustración 41: Wavelink Virtual Client - Message List

7.4.3.- Ventajas de Wavelink Studio®

Estas serían las principales ventajas e inconvenientes que se pueden resaltar del uso de Wavelink Studio® para el desarrollo software y ejecución de aplicaciones:

- **Gran facilidad de desarrollo de las aplicaciones**

  El desarrollador prácticamente se puede abstraer de la plataforma del terminal portátil y sus detalles técnicos, no tiene que emplear unas librerías específicas para cada tipo de dispositivo empleado ni conocer las peculiaridades de programación y ejecución de aplicaciones en cada terminal portátil diferente. Todo el proceso de desarrollo se realiza y prueba en el servidor.

- **Gran facilidad para introducir cambios en las aplicaciones**

  La arquitectura *Thin-Client* de este sistema permite que cualquier cambio efectuado en la aplicación que se ejecuta en el servidor se reflejen automáticamente en los terminales portátiles, sin asistencia alguna ni reconfiguración del dispositivo.

- **Gran facilidad de despliegue de terminales**

  Añadir un terminal portátil al sistema es tan fácil como configurarlo con los parámetros de conexión y conectarlo a la red de Wavelink Studio. Este nuevo terminal portátil ejecutará sin problemas la aplicación que le corresponde en el servidor.

Muchos fabricantes incluso ofrecen opciones con el cliente y la licencia de Wavelink Studio® preinstalados en el terminal, lo que convierte el proceso de puesta en marcha del terminal portátil dentro de la red en algo casi tan sencillo como Plug & Play.

- **Plataforma muy estable y testada ideal para aplicaciones en tiempo real con conexión**

  Sistema muy optimizado para el uso efectivo de las comunicaciones RF en comparación con otros sistemas *Thin-Client*. No hay que olvidar que este sistema se generó cuando aún estaban dando sus primeros pasos las redes 802.11a y 802.11b, con lo que los anchos de banda eran de 1 Mbit/s y el ancho de banda útil efectivo aún menor, lo cual obligó a trabajar en la forma de optimizar el tráfico de datos a través de la red inalámbrica.

- **Sistema independiente del tipo de terminal utilizado.**

  Se carga un cliente Wavelink en cada dispositivo que sirve de interfaz entre el dispositivo y ejecuta el protocolo de comunicaciones específico que envía y recibe datos de la aplicación que se ejecuta en el servidor.

  Una aplicación del servidor, se puede programar de manera que detecte el tipo de dispositivo que la está ejecutando remotamente y adaptar la visualización al tipo y tamaño de pantalla del dispositivo remoto y otros aspectos, lo cual puede ser simplemente una parte de inicialización del software de aplicación.

- **Requiere pocos recursos de memoria, almacenamiento y procesamiento en el terminal portátil**

  Al tratarse de un modelo *Thin-Client*, es en el servidor donde se ejecutan las aplicaciones y donde habrá que hacer la conveniente provisión de recursos como memoria RAM, espacio en sistemas de almacenamiento, velocidad de procesamiento (multi-procesador / array de servidores /...).

- **Permite el uso de sesiones persistentes**

  Un equipo puede estar entrando y saliendo del área de cobertura sin perder el estado de la sesión de aplicación. Así mismo, puede permanecer desconectado, cambiar la batería e incluso reiniciarse sin perder el estado de la aplicación.

7.4.4.- Inconvenientes de Wavelink Studio®

- **No es adecuado para aplicaciones que no trabajen en tiempo real con el servidor**

  No es el sistema idóneo para aquellas aplicaciones que trabajen en batch o permanentemente fuera de línea y que simplemente requieran conexiones limitadas para posteriores verificaciones, carga y descarga de datos.

  Aunque Wavelink Studio® permite el uso de conexiones persistentes y la entrada y salida de los terminales portátiles de la zona de cobertura sin mayor problema, no está pensado para que el terminal trabaje de forma autónoma y envíe datos al servidor de forma selectiva o fuera de la secuencia de la aplicación del servidor.

- **Punto único de fallo en el servidor.**

  Un fallo en el servidor inhabilita todos los dispositivos conectados al mismo y que pueden estar ejecutando aplicaciones independientes entre sí.

  Esto se subsanaría, en parte, repartiendo las diferentes aplicaciones entre varios

servidores, pero no resolvería el problema de que un fallo en la ejecución de una aplicación (porque una parte del sistema de archivos en la que está esa aplicación queda fuera de línea) bloquearía todos los terminales dependientes de la misma.

- **Sistema poco evolucionado para la utilización de interfaces de usuario gráficos**

  Aunque se pueden utilizar elementos gráficos e incluso existe un componente/utilidad (*widget*) para captura de firma, en realidad, el sistema sigue estando principalmente orientado a los anteriores interfaces de usuario con interacción modo texto, utilizando campos de entrada de datos secuenciales.

- **Emulador de Cliente Virtual principalmente pensado para reproducir aplicaciones con interfaz modo texto.**

  Esto también viene derivado de los orígenes de Wavelink Studio como herramienta de desarrollo software para terminales con interfaz de usuario modo texto.

8.- SISTEMAS DE IDENTIFICACIÓN AUTOMÁTICA Y CAPTURA DE DATOS

Se ha querido utilizar para este apartado el término en español *"Identificación Automática y Captura de Datos"* que equivale a la expresión en inglés ampliamente reconocida en todo tipo de documentación técnica y estándares, AIDC (***A**utomatic **I**dentification and **D**ata **C**apture*).

En este apartado se verá en detalle las tecnologías de lectura de códigos de barras 1D y 2D, las tarjetas de banda magnética, etc.. y como se utilizarían en un software de aplicación final que funcione en uno de estos dispositivos.

Se puede obtener información adicional en la web de la Asociación para la Identificación Automática y Mobilidad (USA): http://www.aimglobal.org/ [CAIM]

8.1.- Estandarización y normalización de los códigos de barras.

Actualmente, la generación, lectura y procesamiento de los códigos de barras está perfectamente estandarizada y normalizada, gracias en gran medida a su amplia utilización y a la gran interacción que tienen entre diferentes tipos de sectores y actividades de ámbito global, como por ejemplo la logística y el transporte.

La mayor organización encargada de la normalización y la estandarización de los códigos de barras a nivel mundial es la GS1 [CGS1GLOB]. GS1 es la organización resultante de la unión las siguientes tres organizaciones de normalización y estandarización de códigos de barras: La europea EAN (*European Article Numbering*), la norteamericana UCC (*Uniform Code Council*) y la canadiense ECCC (*Electronic Commerce Council of Canada*).

8.2.- Códigos de Barras 1D

Ilustración 42: Un código de barras 1D

Un código de barras 1D o líneal como también se les conoce es una imagen que contiene información codificada en forma de barras y espacios. El criterio es asignar a cada carácter a codificar un determinado número de espacios y barras y un determinado espesor.

El objetivo de un código de barras es que la información que contiene pueda ser leída posteriormente por un lector de códigos de barras, automatizando el proceso y evitando errores.

Algunos de los códigos de barras mostrados en el presente trabajo han sido generados mediante el software de generación on-line de Raco Industries disponible en:

http://www.racoindustries.com/barcodegenerator/ [RIBCGEN]

En el código de barras que se muestra en la ilustración (42), están codificados los caracteres 501234567890 y 0 como dígito de control, el cual es calculado por el sistema que genera el código y, que en este caso forma parte de la especificación EAN-13.

Si el usuario lo tuviese que teclear en la pantalla de un dispositivo podría cometer un error, y que duda cabe, que el proceso le llevaría varios segundos (dependiendo de la habilidad del operador). Esto mismo se puede hacer en milisegundos y sin posibilidad de error con un lector de códigos de barras bien configurado y correctamente utilizado.

Sin duda es el sistema más básico de captura de datos, junto con el teclado del dispositivo (ya sea físico o virtual) en un terminal portátil. La práctica totalidad de los principales fabricantes de terminales portátiles (handhelds) poseen de serie o permiten incorporar un lector de códigos de barras 1D.

8.2.1.- Densidad del código de barras

Se ha dicho que un código de barras está formado por barras y espacios. Estas barras y espacios tendrán dos posibles codificaciones cada uno: Barra Fina, Barra Gruesa, Espacio Fino y Espacio Grueso.

BG= ▌ BF= │ Si estas son los dos tipos de barra que empleamos, normalmente los espacios será igual en espesor. EG = BG EF = BF, aunque puede existir un espacio largo (EL) que puede hacer de separador __ entre caracteres o entre partes del código (por ejemplo en la zona de inicio y fin de código), y todo esto dependerá de como utiliza todos estos elementos cada simbología en concreto.

Así pues, en base a este criterio, se definirá como densidad, el tamaño de una barra o un espacio de menor tamaño. Puesto que normalmente BF = EF, entonces densidad en milímetros es el tamaño de uno de esos elementos.

Se dirá que un código es de alta densidad siempre que el tamaño de EF o BF sea inferior a 0,25 mm.

8.2.2.- Ratio del código de barras

Se entiende por ratio la relación que existe entre la barra fina (BF) y la barra gruesa (BG) en espesor, que será la misma que exista entre el espacio fino (EF) y el espacio grueso (EG). Esto quiere decir que, si la barra fina es de 0,5 mm y la barra gruesa es de 1 mm, el ratio es 2:1.

Normalmente se utilizan ratios 2:1 y 3:1. El ratio 3:1 permite mayor facilidad de lectura por parte de los lectores de códigos de barras (mejor cuanto mayor ratio para distinguir elementos finos y gruesos) aunque requiere mayor espacio para representar en el código la misma cantidad de caracteres.

8.2.3.- Dígito de control

Normalmente, en casi todas las simbologías se le añade al código un carácter o varios caracteres o dígitos de control para su posterior verificación en el momento de la lectura.

Una de las posibilidades para el caso de un único carácter DC es el cálculo del DC en módulo 10 que sería de la siguiente forma:

$$SumaImpares\ ,\ SumaPares\ ,\ Acumulador\ son\ números\ enteros\ ;$$

$$SumaImpares = \sum Todos\ los\ dígitos\ \ impares$$
$$SumaPares = \sum Todos\ los\ dígitos\ \ pares$$
$$Acumulador = SumaImpares + (SumaImpares \times 3)$$

$$DigitoDeControl = (((\frac{Acumulador}{10}) + 1) \times 10) - Acumulador$$
$$Si\ DigitoDeControl = 10\ entonces\ DigitoDeControl = 0$$

Ilustración 43: Cálculo del DC módulo 10 de un código de barras

Adicionalmente, en los SDK suministrados por los fabricantes de dispositivos para acceder a las funcionalidades específicas de los terminales portátiles, se incluyen todas las funciones necesarias para la configuración del lector, la lectura de datos del mismo (en respuesta al evento *trigger* que se genera cuando se presiona el gatillo o botón disparador), procesar los datos obtenidos y extraer la información necesaria.

Entre las múltiples simbologías de códigos de barras disponibles, se pueden destacar las que se detallan a continuación.

8.2.4.- Código 39

Ilustración 44: Ejemplo de Código 39

También conocido como:

- ANSI/AIM Code 39
- USS Code 39 (*Uniform Symbology Specification Code 39*)
- Código 3 de 9
- Código Alpha 39
- Código USD-3
- Código LOGMARS

El Código 39 ha sido el primer código de barras desarrollado y aún se utiliza en la actualidad en entornos que no sean la distribución. Es un estándar empleado por el Departamento de Defensa de los Estados Unidos de América y también por el HIBCC (*Health Industry Bar Code Council*).

8.2.4.1.- Características del código

- Longitud variable

- Alfanumérico
- De propósito general
- Con autocomprobación.
- Omnidireccional
- Ratio de impresion

$$\frac{EG}{EF}=\frac{BG}{BF}=\frac{EG}{BG}=2{,}25$$

Cada carácter que compone el código se codifica con 5 barras y 4 espacios intercalados, ambos codificados como BF, BG, EF y EG, cumpliéndose que EF = BF y EG = BG.

Si EG = BG = Símbolo Grueso (SG) y EF = BF = Símbolo Fino (SF), el código de barras ha sido configurado para que cada carácter codificado ocupe el mismo espacio, de modo que dispone de 3 SG y 6 SF en cualquier combinación de barras o espacios.

Total: 2^9 combinaciones posibles (512 combinaciones) de caracteres para representar simplemente 33.

Con redundancia de codificación, no se puede generar caracteres erróneos durante su lectura

Puede codificar los caracteres [A-Z],[0-9] [punto] [espacio] $ / + – %

8.2.4.2.- Ventajas

- Puede codificar alfanumérico de cualquier número de caracteres
- Es fiable y autocomprobado. MUY RECOMENDABLE.

8.2.4.3.- Inconvenientes

- Baja densidad de caracteres por codificación. Suponiendo BF = 0,3 mm daría un código de (6 x 0,3 + 3 x 0,9) = 6,6 mm por carácter. Esto quiere decir que para codificar 10 caracteres se necesitarían 66 milímetros de longitud física de código + 13,2 milímetros de caracteres de inicio y fin de código. Total 79,2 mm. GRANDE.

8.2.5.- Código 93

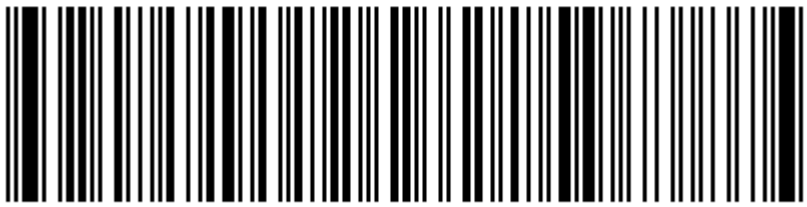

Ilustración 45: Ejemplo de Código 93

También conocido como:

- ANSI/AIM Code 93

- USS Code 93 (*Uniform Symbology Specification Code 93*)
- Código 9 de 3

El Código 93 fue desarrollado para complementar y mejorar el Código 39. Es también alfanumérico, pero cada carácter a codificar se representa con longitud variable y produce un código más denso que puede codificar más caracteres en menos espacio que el código 39. Resulta incluso más denso que el Código 128.

8.2.5.1.- Características del código

- Alfanumérico
- Con autocomprobación
- De propósito general
- Omnidireccional
- Tiene dos modos de codificación (Estándar y Full ASCII)
  - Modo estándar
    - Puede codificar los caracteres [A-Z],[0-9] [punto] [espacio] $ / + – %
  - Modo Full ASCII
    - Puede representar los 128 caracteres del código ASCII, con la excepción de * que es el carácter de inicio y fin de código

8.2.5.2.- Ventajas:

- Gran densidad de caracteres por espacio.
- Fiable y autocomprobado
- Alfanumérico Full ASCII

8.2.5.3.- Inconvenientes:

- No se ha extendido mucho. El GS1-128 ha ocupado su lugar

8.2.6.- GS1-128

Ilustración 46: Ejemplo de Código GS1-128

También conocido como:

- EAN-128
- Código 128
- ANSI/AIM Code 128
- USS Code 128 (*Uniform Symbology Specification Code 128*)

8.2.6.1.- Características del código

- Capacidad para codificar 48 caracteres alfanuméricos
- Code 128-A, B y C
- No omnidireccional
- Alta densidad de codificación de caracteres por espacio
- Propósito general, aunque muy estandarizado para logística y transporte
    - Incorpora identificadores de aplicación
    - Incorpora un identificador único GS1
- Incorpora un dígito de control para verificación, y además, cada carácter del código dispone de control de paridad
- Puede codificar los 128 caracteres del código ASCII y los juegos extendidos.

Puede codificar tres juegos de caracteres diferentes:

Juego de caracteres A

Incluye todas las letras mayúsculas y los caracteres de puntuación además de los de control, caracteres del (0 al 95 ambos inclusive) y siete caracteres especiales.

Juego de caracteres B

Incluye todas las letras mayúsculas y minúsculas junto con los caracteres de puntuación (códigos ASCII del 32 al 127 ambos inclusive) y siete caracteres especiales.

Juego de caracteres C

Incluye un juego de 100 pares de dígitos (del 00 al 99 inclusive), junto con 3 caracteres

especiales. Esto permite que los datos numéricos puedan ser codificados con dos dígitos por carácter, representado con el doble de la densidad de datos estándar. Los caracteres 96 al 102 son caracteres sin equivalente ASCII, son especiales y tienen significado concreto para el lector de códigos de barras

8.2.6.2.- Ventajas

- Alta densidad de codificación por espacio
- Muy estandarizado y extendido
- Muy fiable

8.2.7.- UPC-A

Ilustración 47: Ejemplo de código UPC-A

También conocido como:

- Universal Product Code version A
- GS1-12
- UCC-12

Utilizado en el etiquetado de productos de venta al público y distribución en USA.

Los códigos de identificación de fabricante son controlados y asignados por el UCC (Uniform Code Council).

8.2.7.1.- Características del código

- Omnidireccional. Apropiado para lectura en TPVs
- Puede codificar 12 caracteres numéricos
- Puede incorporar un segundo código adicional (Add-On) con 2 o 5 caracteres

La composición de un código UPC-A es la siguiente:

- 1 dígito de tipo de sistema con uno de los siguientes valores:
  - Items de peso aleatorio marcados en la tienda (2)
  - Artículos de farmacia y relacionados con la Sanidad (3)
  - Sin restricciones de formato. Para uso dentro de la tienda sobre artículos no alimentarios (4)
  - Para uso con cupones (5)
  - Códigos regulares UPC (7)
  - Reservados (1, 6, 8 y 9)
- 5 dígitos para el código de fabricante (Asignado por el UCC)
- 5 dígitos para el código de producto (Asignado por el fabricante)

- 1 dígito para control

El código puede imprimir los indicadores de margen (>) y (<) para proteger los márgenes a la derecha y la izquierda del código y facilitar la detección del principio y fin del código a los lectores de códigos de barras.

Ilustración 49: Ejemplo de código UPC-A + 2 Add-On

Ilustración 48: Ejemplo de código UPC-A+5 Add-On

UPC-A puede ir acompañado de un código adicional más pequeño, que puede ir impreso al lado, a la derecha del código principal, incluyendo un suplemento (*Add-On*) de 2 o 5 dígitos que incluirán información suplementaria al código principal, especialmente aplicable a libros y revistas.

8.2.8.- UPC-E

Ilustración 50: Ejemplo de Código UPC-E

También conocido como:

- Universal Product Code version E

8.2.8.1.- Características del código

- Código numérico
- Capacidad de almacenamiento de 6 dígitos
- Omnidireccional
- Se puede leer en cualquier TPV

Se trata de una variante del UPC-A al que se le eliminan los 5 dígitos del fabricante y en el que se codifican 6 dígitos con el primero dígito (Número de sistema) que puede tener el valor 0 o 1.

8.2.8.2.- Ventajas

- Muy estandarizado y extendido
- Lo puede leer cualquier TPV
- Alta densidad de codificación de caracteres por espacio

8.2.8.3.- Inconvenientes

- Solo numérico y de longitud fija

8.2.9.- EAN-13

Ilustración 51: Ejemplo de código EAN-13

También conocido como:

- European Article Number 13
- UPC-13
- GS1-13
- EAN/UCC-13

EAN-13 se basó en el estándar UPC-A y fue implementado por la organización EAN (*European Article Association*) en Europa.

EAN-13 se configuró como una ampliación de UPC-A. De hecho, un lector capaz de leer EAN-13 también puede leer UPC-A si no se le especifica longitud del código. La única diferencia es que el tipo de sistema que en UPC-A es un único dígito, en EAN-13 son dos dígitos de 00 a 99 que se utiliza básicamente como código de país.

8.2.9.1.- Características del código EAN-13

Las mismas que UPC-A con la diferencia de que codifica 13 dígitos en vez de 12

Estructura de un código EAN-13:

- 2 o 3 dígitos para código de país
- 4 o 5 dígitos para código de fabricante. En cada país existe una autoridad encargada de asignar estos números.
- 5 dígitos para código de producto

Los márgenes con (>) y (<) y los códigos suplementarios se generan exactamente igual que con UPC-A.

8.2.9.2.- Ventajas

- Muy extendido y estandarizado
- Alta densidad de codificación de caracteres por espacio
- Lo puede leer cualquier sistema de lectura de un TPV

8.2.9.3.- Inconvenientes

- Solo numérico
- Código de longitud fija

8.2.10.- EAN-8

Ilustración 52: Ejemplo de código EAN-8

También conocido como:

- European Article Number 8
- UPC-8
- GS1-8
- EAN/UCC-8

Un EAN-8 es el mismo sistema de codificación que EAN-13, pero se ha configurado para usar menos espacio y se le han eliminado los dígitos identificadores del código de fabricante.

Así pues, el código en cuestión simplemente identificará un país y un código de producto de un determinado fabricante.

Está especialmente pensado para aquellas cajas pequeñas en las que no cabe o no es apropiado un código EAN-13.

El concepto es equivalente al que se consigue en USA con UPC-A y el UPC-E

8.2.10.1.- Características de EAN-8

- Las mismas que EAN-13, pero sin los dígitos del fabricante

8.2.10.2.- Ventajas

- Las mismas que EAN-13

8.2.10.3.- Inconvenientes

- Los mismos que EAN-13

8.2.11.- Codabar

Ilustración 53: Ejemplo de código Codabar

También conocido como:

- ABC Codabar
- USD-4
- NW-7
- Código 2 de 7
- Monarch
- Code-27
- Ames code
- Rationalized Codabar
- ANSI/AIM Codabar

- USS Codabar (*Uniform Symbology Specification Codabar)*

Codabar fue desarrollado en 1972 por Pitney Bowes, Inc

Utilizado en librerías, bancos de sangre, laboratorios de fotografía, tickets de aviación, y en los manifiestos aéreos de FedEx.

8.2.11.1.- Características del código

- Código autocomprobado y muy seguro
- Comienza y termina con una letra de las siguientes A,B,C o D
- Tiene capacidad para codificar hasta 16 caracteres más 4 caracteres de inicio y fin de código

8.2.11.2.- Ventajas

- Muy estandarizado y extendido
- Autocomprobado y muy seguro

8.2.11.3.- Inconvenientes

- Solo numérico

8.2.12.- Industrial 2 de 5

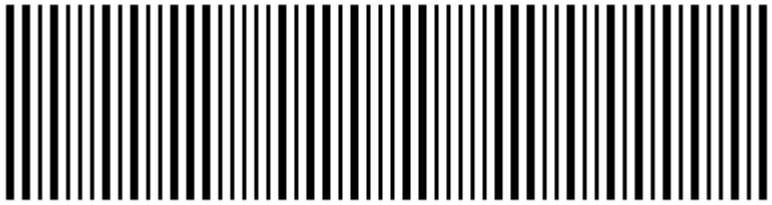

Ilustración 54: Ejemplo de cógido 2 de 5 Industrial

También conocido como:

- Código 2/5 Estándar
- Código 2 de 5

El código industrial o estándar 2 de 5 que está en uso desde los años 60. Se ha utilizado en almacén para etiquetado de organización y también para tickets de compañías aéreas. Principalmente empleado para etiquetar cajas de cartón.

Es un código de baja densidad numérica (pocos caracteres codificados por espacio de impresión) debido a que solamente las barras codifican información. De hecho los espacios se pueden poner todos iguales o de diferente ancho si se desea sin afectar a la codificación.

Se generó posteriormente una versión mejorada de este código denominada 2 de 5 Entrelazado.

8.2.12.1.- Características del código

- Numérico de 14 dígitos de longitud
- No omnidireccional
- Baja densidad de codificación de caracteres por espacio
- Los espacios no contienen información

8.2.12.2.- Inconvenientes

- Muy antiguo
- Solo numérico
- Baja densidad de codificación
- Código de longitud fija

8.2.13.- ITF-14 (2 de 5 Entrelazado)

Ilustración 55: Ejemplo de código ITF-14 (2 de 5 Entrelazado)

También conocido como:

- 2 de 5 Entrelazado. Así es como siempre se le ha conocido
- ANSI/AIM ITF 25
- ANSI/AIM I-2/5
- USS ITF 2/5 (*Uniform Symbology Specification ITF*)
- ITF
- I-2/5

El código 2 de 5 Entrelazado fue generado para corregir deficiencia del 2 de 5 industrial en lo concerniente a la densidad de codificación de caracteres por espacio que era muy reducida. El código 2 de 5 Entrelazado utiliza el mismo sistema que el Industrial, pero consigue codificar el doble de caracteres en el mismo espacio físico utilizando los espacios entre barras para codificar también información.

8.2.13.1.- Características del código

- Tiene las mismas aplicaciones que el 2 de 5 industrial.
- No se usa en los TPVs, solo en cajas contenedoras de cartón.
- Utilizado en venta, librerías, etiquetado industrial, ...

8.2.13.2.- Ventajas

- Buena densidad de codificación de caracteres por espacio

8.2.13.3.- Inconvenientes

- Solo numérico

8.2.14.- Código 11

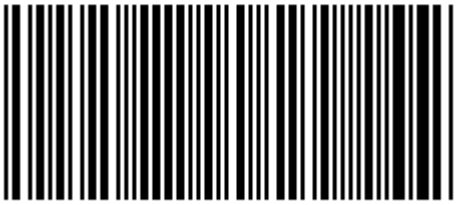

Ilustración 56: Ejemplo de Código 11

También conocido como:

- USD-8

8.2.14.1.- Características del código

- Numérico
- Alta densidad de codificación por espacio
- Permite codificar los números [0-9] y el símbolo – junto con dos caracteres de [inicio] y [fin] de código
- Este código ha sido usado principalmente en equipamiento de telecomunicaciones
- No es un código muy seguro y pequeñas imperfecciones en la impresión del código o posteriores deterioros del mismo pueden fácilmente dar una lectura errónea de un dígito en otro distinto. Se puede añadir integridad incorporando en los datos a codificar algún dígito de control. De cualquier forma, el código en si mismo no es muy recomendable.

8.2.14.2.- Ventajas

- Alta densidad de codificación por espacio

8.2.14.3.- Inconvenientes

- Solo numérico
- Poco fiable

8.2.15.- Código ISBN

Ilustración 57: Ejemplo de código ISBN

Regulado por el estándar ISO 2108

El código ISBN (***I**nternational **S**tandard **B**ook **N**umber*) sirve como identificador único asignado a cada libro o a la edición de cada libro publicado, como código de producto específico para los libros.

El código ISBN se creó inicialmente como un código de 10 dígitos, y ha servido a su propósito durante más de tres décadas, sin embargo, la Agencia Internacional ISBN ha considerado que en un futuro no muy lejano los diez dígitos originales se quedarán cortos para codificar las ediciones de libros y publicaciones.

En 2007 se ha diseñado una nueva versión del código de 13 dígitos denominado ISBN-13. En el caso del código ISBN-13 existe el prefijo GS1 que puede ser 978 o 979, el código de pais o el código de idioma. El número de editor, que es asignado por la Agencia ISBN correspondiente, el número de artículo. Un carácter de suma de comprobación verifica que el código ISBN es correcto. Las partes del código ISBN pueden tener diferente longitud e ir separadas por el carácter (–). La letra X que aparece en algunos códigos ISBN es la forma de poner el número 10 en letras romanas en un código suplementario de un carácter. Los códigos adicionales (Add-On) pueden tener 2 o 5 dígitos, al igual que con los UPC-A y representan generalmente el precio sugerido de venta al público. Existen los separadores de margen imprimibles mediante los caracteres (>) y (<) cuya finalidad es dejar un espacio de margen para que los lectores de códigos de barras puedan fácilmente delimitar el inicio y el fin del código.

Se puede obtener más información en la web de la Agencia ISBN [CISBN]:

http://www.isbn.org

8.2.16.- Código GS1 DataBar

Ilustración 58: Ejemplo de código GS1 DataBar

La familia de códigos GS1 DataBar ha sido desarrollada por el GS1 y tiene como finalidad complementar y, en algunos casos sustituir a los códigos EAN/UPC.

El objetivo de estos códigos es que puedan ser leídos en todos los TPVs, ser más pequeños y codificar más caracteres en el mismo espacio que un código EAN/UPC, y además, incorporar información adicional dentro del mismo código, como por ejemplo números de serie, números de lote o fechas de caducidad.

Se está trabajando en la futura implementación de los códigos GS1 DataBar en los TPVs ya que permitirá todas las teclas GS1 y atributos y además codificarlo en menos espacio que un código EAN/UPC.

Actualmente, los códigos GS1 DataBar ya han sido aprobados para su uso global en artículos de Sanidad que no pasan por los TPVs.

Los algoritmos de los códigos GS1 DataBar están disponibles en el estándar ISO/IEC 24724

8.3.- Códigos de Barras 2D

Se trata de códigos de barras bidimensionales, los más representativos y conocidos son el PDF417, QR y GS1 DataMatrix.

En el enlace que se indica se puede ver la normativa IATA que regula el uso de algunos de estos códigos en el sector de la aviación [IATA2D]:

http://www.iata.org/whatwedo/stb/Documents/BCBP_Implementation_Guidev4_Jun2009.pdf

8.3.1.- Códigos de Barras 2D Apilados

Se forman por el apilado de varios códigos 1D. No se van a detallar todos los existentes, pero si los más conocidos y utilizados en el mercado a fecha de hoy.

8.3.1.1.- Código 16K

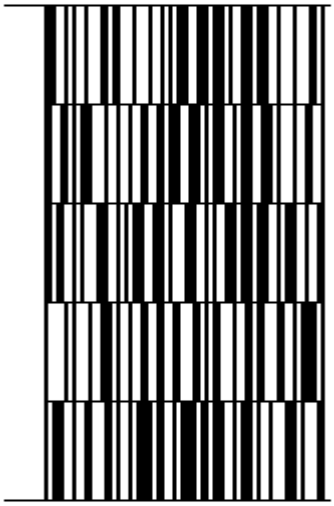

Ilustración 59: Ejemplo de código 16K

También conocido como:

- Code16K

El Código 16K fue desarrollado por Ted Williams en 1989 para proveer una forma simple de imprimir y decodificar simbologías de múltiples filas. Ted Williams también desarrolló en sus orígenes el Código 128 y, por lo tanto, se basó en el para elaborar esta simbología. Se basa en el apilamiento en vertical de varios códigos 128 horizontales.

Y puede codificar el juego completo de caracteres ASCII 128. Es utilizado principalmente en la sector de la Sanidad.

8.3.1.1.1.- Características del código

- Alfanumérico
- El código es continuo
- Tiene longitud variable

8.3.1.2.- PDF417

Ilustración 60: Ejemplo de código PDF417

También conocido como:

- Portable Data File 417
- PDF 417

Es el código 2D más común y extendido en la actualidad.

Se trata de un código de dominio público definido en el estándar ISO/IEC 15438.

El código PDF417 o simplemente *Archivo Portátil de Datos 417* es un código 2D que apila códigos de barras horizontales 1D verticalmente. Es por eso que se considera un código 2D apilado.

8.3.1.2.1.- Características del código

Se trata de un código que es capaz de codificar hasta 1KB de datos por etiqueta. Fue desarrollado por Symbol Technologies (1989-1992) y actualmente es mantenido por el organismo ISO/IEC 15438 [IS15438].

El código PDF417 permite almacenar grandes cantidades de datos en alta densidad de forma que consume poco espacio.

Cada símbolo PDF417 consiste en varias líneas de *codewords* apilados.

Cada *codeword* se representa como un código de barras 1D de poca altura.

Cada *codeword* representa uno de los 929 posibles valores desde de los tres posibles *clusters*.

Para cada fila se selecciona un *cluster* diferente, repitiéndose *cluster* cada tres filas.

Los datos son codificados utilizando uno de los tres modos de codificación posibles:

- Texto
    - Permite codificar todos los caracteres imprimibles ASCII (códigos del 32 al 126 inclusive) de acuerdo con el estándar ISO/IEC 646, junto con determinados caracteres de control como TAB (ASCII 9), LF (ASCII 10) y CR (ASCII 13)
- Binario
    - Permite codificar los 256 posibles valores de 8 bits (ISO/IEC 8859-1). Esto incluye todos los valores ASCII con valor de 0 a 127 y permite el soporte de juegos de caracteres internacionales.
- Numérico
    - Se trata de un método eficiente para codificar cadenas de datos numéricas

PDF417 utiliza el método de detección y corrección de errores Reed Solomon en vez de dígitos de control.

Este sistema de corrección de errores permite que el código pueda ser leido incluso con cierto deterioro del mismo sin que se produzca pérdida de datos.

Existen 9 niveles de corrección de errores [0-8] y el nivel mínimo recomendado es 2.

Más información sobre este código se puede encontrar en el estándar ISO/IEC correspondiente o en el siguiente trabajo de disponible en Internet en la web del CSIC:

http://digital.csic.es/bitstream/10261/21259/1/Codbidimens.pdf [CSIC2D]

8.3.1.2.2.- Ventajas

- Gran cantidad de información en poco espacio

- Control de errores muy sofisticado

8.3.1.2.3.- Desventajas

- Requiere de un lector láser especial para su lectura o tratamiento digital de imágenes

8.3.1.3.- Micro PDF417

Ilustración 61: Ejemplo de código Micro PDF417

También conocido como:

- Micro Portable Data File 417

Se basa en el estándar PDF 417

Se utiliza cuando el tamaño del código impreso es una prioridad y PDF417 resulta consumir mucho espacio.

8.3.1.3.1.- Características del código

Puede almacenar hasta 150 bytes, 250 caracteres alfanuméricos o 366 dígitos numéricos cuando el tamaño es una prioridad.

A diferencia del Código PDF417, el Micro PDF 417 solamente puede ser impreso en un cierto número de combinaciones de filas, columnas y codewords de corrección de errores, todo esto hasta un máximo de 4 columnas de datos por 44 filas.

En la correccción de errores del código Micro PDF417, cada símbolo generado contiene al menos siete codewords para corrección de errores.

Los códigos Micro PDF son bidireccionales y pueden ser leidos por un lector de códigos en cualquier dirección.

8.3.1.3.2.- Ventajas

- Mucha densidad y gran cantidad de información en muy poco espacio

8.3.1.3.3.- Desventajas

- No tiene tantas opciones como el PDF417
- No tiene tanta capacidad de almacenamiento como el PDF417
- Igual que el PDF417 requiere de lector especial láser o técnicas de procesamiento digital de imagen

8.3.2.- Códigos 2D Matriciales

Se basan en una matriz de datos en dos dimensiones. Son auténticos códigos bidimensionales y no se originan de la composición de varios códigos 1D como en el caso anterior.

Como en el apartado anterior, no se van a detallar todos los existentes, pero si los más conocidos y utilizados en el mercado a fecha de hoy.

8.3.2.1.- Código Azteca

Ilustración 62: Ejemplo de código Azteca

También conocido como:

- Aztec Barcode
- ANSI/AIM BC13 ITS/97/002

El Código Azteca fue desarrollado por Welch Allyn y es muy utilizado para el marcado de pequeños componentes utilizando una amplia variedad de tecnologías de impresión.

También se puede leer desde el display de teléfonos móviles y otros dipositivos.

Existe Código Azteca Pequeño (Small Aztec Code) que es una versión reducida del Código Azteca.

8.3.2.1.1.- Características del código

- Puede codificar los 128 caracteres ASCII y también los 256 caracteres del Juego de caracteres ISO-8859-1. Alfabeto Latin-1.
- Utiliza el sistema de detección y corrección de errores Reed Solomon con porcentajes de corrección seleccionables por el usuario (de 5% al 95%).
- Es un código 2D de dominio público

Este código 2D se basa en una muestra de referencia cuadrada formada por un punto cuadrado pequeño con dos anillos concéntricos también cuadrados negros alrededor. Este punto marca el centro de la imagen y alrededor se dibujan pequeños cuadrados que pueden ser espacios blancos o negros de igual tamaño.

8.3.2.2.- GS1 Datamatrix

(01)07612345678900(17)100503

(10)AC3453G3

Ilustración 63: Ejemplo de código DataMatrix

También conocido como:

- Data Matrix
- ECC200

Desarrollado por RVSI Acuity CiMatrix.

Solo se puede leer con tecnologías de procesamiento de imagen.

DataMatrix se utiliza para codificar códigos de producto y números de serie en placas de calificación, para marcar instrumentos quirúrgicos en Japón, identificar lentes, circuitos electrónicos y otros elementos durante la fabricación.

8.3.2.2.1.- Características del código

- Capacidad para 3116 caracteres numéricos
- Capacidad para 2335 caracteres alfanuméricos
- Puede contener identificadores de aplicación
- Puede contener un identificador único GS1
- Algoritmos de detección y corrección de errores Reed Solomon que permiten reconstruir códigos con hasta un 60% de deterioro.

En función de los juegos de caracteres que puede contener el código su codificación sería:

- ASCII para los caracteres del 0 al 127
- C40 para codificar números y letras mayúsculas
- Texto para codificar numericos y minúsculas
- Base256 para codificar los valores de 8 bits.

8.3.2.3.- Código QR

Desarrollado por Nippondenso ID Systems.

Ilustración 64: Ejemplo de código QR

Aunque inicialmente se utilizó para el seguimiento de piezas en la industria de la fabricación de vehículos, posteriormente ha tenido una mayor utilización en otros entornos, incluyendo aplicaciones de seguimiento comercial y otras dirigidas a los usuarios de teléfonos móviles conocidas como *Mobile Tagging*.

Dispone de patrones cuadrados de detección de posición en tres de sus cuatro esquinas.

Utiliza una matriz de pequeños cuadrados que se codifican como blancos o negros (0 o 1).

8.3.2.3.1.- Características del código

- Puede codificar caracteres japoneses Kanji y Kana
- De dominio público
- Solo se puede leer con técnicas de procesamiento de imagen

8.3.2.3.2.- Ventajas

- Muy extendido y en aumento

8.3.2.4.- Semacode

Ilustración 65: Ejemplo de código Semacode

También conocido como:

- URL Barcode
- Códigos de barras de dirección de internet (URL)
- Tag Semacode

Sirve para codificar direcciones de internet en un código de barras, generalmente para que sean fácilmente capturadas e introducidas desde un PDA o SmartPhone. Utiliza la codificación 2D de DataMatrix.

8.3.2.4.1.- Características del código

- Las mismas que DataMatrix

8.3.2.4.2.- Ventajas

- Código abierto y de dominio público
- Muy extendido y en aumento

8.4.- Tarjetas con banda magnética

Las tarjetas con banda magnética fueron ideadas por IBM en 1960 en base a un contrato con el gobierno de los Estados Unidos de América para un sistema de seguridad. Sus tecnologías de grabación y el contenido de sus pistas están definidos en los siguientes estándares ISO/IEC:

- ISO/IEC 7811-2 Técnicas de grabación de bandas magnéticas (Baja Coercitividad) [IS78112]
- ISO/IEC 7811-6 Técnicas de grabación de bandas magnéticas (Alta Coercitividad) [IS78116]
- ISO/IEC 7811-7 Técnicas de grabación de bandas magnéticas (Alta Coercitividad y Alta Densidad) [IS78117]
- ISO/IEC 7811-8 Técnicas de grabación de bandas magnéticas (Coercitividad de 57,7 kA/m (650 Oe) [IS78118]
- ISO/IEC 7813 Tarjetas de transacción financiera [IS7813]
- ISO/IEC 4909 Datos de la banda magnética para la Pista 3 [IS4909]

En lo que a nuestros proyectos se refiere, interesará únicamente la parte electrónica y de comunicación de datos con este tipo de dispositivos. Se asume que las tarjetas cumplen con los estándares ISO en lo relativo a estampado (ISO/IEC 7811-1), dimensiones, materiales y otros aspectos (ISO/IEC 7810).

Lo más importante para el diseñador de una solución móvil basada en terminales portátiles es qué tipo de datos y con qué formato se pueden grabar y extraer de estas tarjetas.

Normalmente, en los terminales portátiles solamente se incorporan interfaces de lectura y no de grabación, y se asume que el proceso de grabación se efectúa en centros de proceso de datos (CPD) y según criterios de la organización.

Será posible tener acceso a tres pistas de información en una tarjeta con banda magnética (*Magnetic Stripe*), denominadas genéricamente Pista 1, Pista 2 y Pista 3.

8.4.1.- Especificaciones ISO de una banda magnética

Nº Pista	Tipo Pista	Norma	Densidad (bpp)	Bits por carácter	Capacidad Caracteres	Carácter Inicio	Carácter Separador	Carácter Fin
1	Alfanumérica	IATA Ver [[CIATA]	210	7	76	%	^ o - Offset=20H	?
2	Numérica	ABA Ver [CABA]	75	5	37	;	= Offset=30H	?
3	Numérica	THRIFT	210	5	104	;	No Tiene	?

Tabla 6: Especificaciones ISO de las pistas de una banda magnética

Aunque internamente los lectores de bandas magnéticas trabajen con codificaciones de

caracteres de 5 o 7 bits (incluido el bit de paridad), el interfaz lector le pasa los datos al dispositivo en formato ASCII de 8 bits, eliminando el bit de paridad.

8.4.1.1.- Formato de las pistas

El siguiente será el formato que respetarán todas las pistas en cuanto a los datos contenidos en las mismas, sus delimitadores y separadores:

[Inicio] datos [separador] datos ... [separador] datos [Fin][LRC]

LRC = Longitudinal Redundancy Check

El estándar ISO 1155 establece como algoritmo de cálculo para el LRC el siguiente:

LRC será el complemento a 2 de la suma de todos los bytes en módulo 2^8

Se calcula sobre todos los caracteres del mensaje, incluido el de inicio y el de fin, con sus bits de datos y paridad.

8.4.1.2.- Juegos de caracteres codificables

- Los caracteres que se pueden codificar en la pista 1 son: [0-9], [A-Z], espacio, $ ( ) . / y el delimitador que no se esté utilizando ^ o –.
- Los caracteres que se pueden codificar en las pistas 2 y 3 son los números [0-9].

8.4.2.- Lector de tarjetas con banda magnética (MSR)

Normalmente en los terminales se podrá disponer de un lector de bandas magnéticas o MSR (*Magnetic Stripe Reader*) de tres formas:

- Totalmente integrado en el propio equipo (Esta sería la forma más deseable)
- Como accesorio externo con conectividad Bluetooth, WLAN o IrDA[3]
- Como accesorio acoplable al terminal (Add-On)[4]

Ilustración 66: Accesorio Snap-On MSR de Motorola MSR5000

En caso de no poder tener el lector totalmente integrado en el dispositivo, se elegirá un accesorio acoplable (*Snap-On*) de forma que una vez acoplado quede lo más consistente posible y no perjudique sus condiciones de sellado, protección ante golpes, etc. Aunque existen periféricos como el de la ilustración (67), solamente serán aplicables en determinado tipo de aplicaciones por su volumen y el hecho de ser otro dispositivo más añadido al usuario con todas las problemáticas asociadas de alimentación, comunicaciones y ergonomía.

Estos dispositivos de lectura generalmente se encargarán de enmascarar todo lo expuesto anteriormente y, una vez que la tarjeta con banda magnética es leída correctamente, devuelve una cadena de caracteres al controlador de dispositivo en el terminal con el contenido de los datos de las pistas solicitadas, excluyendo caracteres de inicio, fin o LRC, aunque dejando delimitadores.

3 La ilustración que se muestra se ha obtenido del sitio web de Intermec y es del producto PB2
4 La ilustración que se muestra se ha obtenido del sitio web de Motorola y es del producto MSR5000

Ilustración 67: Impresora Bluetooth con MRS de Intermec PB3

En las herramientas de desarrollo software y SDKs de los fabricantes se incluye los métodos accesibles para configurar el lector de bandas magnéticas y capturar los datos de las pistas una una vez se genera el evento correspondiente tras el paso de la tarjeta por el lector.

En una sola pasada de la tarjeta se podrán capturar los datos de 1, 2 o las tres pistas incluidas en su banda magnética. Esto dependerá del tipo de lector que incorpore el dispositivo y como se configure.

Se puede tener lectores para pista 1, 2, 1 y 2, 1 y 3, etc... en diferentes combinaciones.

A pesar de que la mayoría de bancos y entidades financieras están cambiando sus soportes hacia las nuevas tarjetas inteligentes (*SmartCards*), comúnmente llamadas *Tarjetas-Chip*, e intentando erradicar las tarjetas con banda magnética, aún quedan muchas tarjetas con banda magnética en el mercado y muchas aplicaciones donde el uso de la banda magnética tiene sentido por su bajo conste y sencillez de implementación.

8.5.- Tarjetas Inteligentes (SmartCards)

Las características físicas de estas tarjetas también están definidas, como en el apartado anterior, en el estándar ISO/IEC 7810. En este apartado interesará únicamente lo concerniente a las características electrónicas y de intercambio de datos. Se asume que las tarjetas han sido generadas en base al estándar indicado y estampadas conforme al estándar ISO 7811-1.

A diferencia de las tarjetas con banda magnética cuyos datos son accesibles por cualquier lector homologado correctamente configurado, en el caso de las tarjetas inteligentes, existen mecanismos de seguridad y control tanto para el acceso seguro al dispositivo incorporado y los datos que contiene, como para la grabación y posterior modificación de datos en función a unos determinados criterios. Puede contener datos encriptados y protocolos de seguridad para el acceso y modificación de los mismos, motivo por el cual son ahora el sustituto natural de las antiguas tarjetas con banda magnética allí donde se requieren criterios más estrictos de seguridad y confidencialidad de los datos contenidos en la tarjeta, especialmente en tarjetas destinadas a la banca y entornos de transacciones financieras.

Los siguientes estándares ISO/IEC son aplicables a este tipo de tarjetas:

Aspectos físicos, eléctricos y de comunicación de datos

- ISO/IEC 7816-1 Especifica las características físicas de las tarjetas con contactos [IS78161]
- ISO/IEC 7816-2 Especifica las dimensiones y la ubicación de los contactos
- ISO/IEC 7816-3 Especifica el interfaz eléctrico y los protocolos de transmisión para tarjetas asíncronas
- ISO/IEC 7816-10 Especifica el interfaz eléctrico y la respuesta al reset de tarjetas asíncronas
- ISO/IEC 7816-12 Especifica el interfaz eléctrico y los procedimientos operativos para tarjetas USB

Aspectos independientes de la parte física. Aplicables a tarjetas con o sin contactos

- ISO/IEC 7816-4 Especifica la organización, seguridad y comandos para intercambio de datos
- ISO/IEC 7816-5 Especifica el registro de proveedores de aplicación
- ISO/IEC 7816-6 Especifica elementos de datos para intercambios interindustria
- ISO/IEC 7816-7 Especifica comandos SCQL (*Structured Card Query Language*)
- ISO/IEC 7816-8 Especifica comandos para la gestión de la seguridad
- ISO/IEC 7816-9 Especifica comandos para la gestión de la tarjeta
- ISO/IEC 7816-11 Especifica la verificación personal mediante métodos biométricos
- ISO/IEC 7816-13 Especifica comandos para la gestión de aplicación en un entorno multi-aplicación
- ISO/IEC 7816-15 Especifica la aplicación de criptografía de la información

8.5.1.- Lector de tarjetas inteligentes (SCR)

Normalmente en los terminales se podrá disponer de un lector de tarjetas inteligentes o SCR (*Smart Card Reader*) de tres formas:

- Totalmente integrado en el propio equipo (Esta sería la forma más deseable)
- Como accesorio externo con conectividad Bluetooth, WLAN o IrDA
- Como accesorio acoplable al terminal (*Add-On*)[5]

Al igual que se indicaba para el caso de los lectores de bandas magnéticas, se buscará siempre que, o bien estén integrados en el terminal, o en caso de no ser posible, que se puedan acoplar de forma eficiente, segura y compacta al mismo, mediante un accesorio acoplable (*Snap-On*).

El accesorio que se muestra en la ilustración (68) incorpora además de lector de tarjetas inteligentes el lector de tarjetas con banda magnética.

Ilustración 68: Accesorio Lector de Tarjetas Inteligentes DCR7X00

5 La ilustración que se muestra se ha obtenido del sitio web de Motorola y es del producto DCR7X00-200R

8.6.- Captura de firmas digitalizadas

Una de las capturas de datos más útiles en las aplicaciones móviles actuales es la digitalización de firma en la pantalla del dispositivo móvil. Esta funcionalidad está cada vez más extendida entre los aplicativos actuales y permite, entre otras cosas, la validación y verificación in-situ en el momento de la ejecución de una operación con el cliente final del consentimiento del mismo (cliente) para la ejecución de dicha operación o como registro comprobante de operación, por ejemplo en el proceso de entrega en una empresa de correo o paquetería.

Para poder llevar a cabo esta premisa, existen tres requisitos mínimos que debe cumplir el dispositivo:

- Resolución de pantalla en ppp (puntos por pulgada) adecuada para la visualización de la firma y los trazos efectuados
- Resolución del digitalizador pen/táctil en ppi adecuada para captar los trazos con exactitud y definición
- Velocidad de procesamiento gráfico para permitir el trazado y redibujado de pantalla sin retardo

Actualmente, la inmensa mayoría de los últimos dispositivos presentes en el mercado cumplen con estas premisas, a diferencia de lo que ocurría hace años.

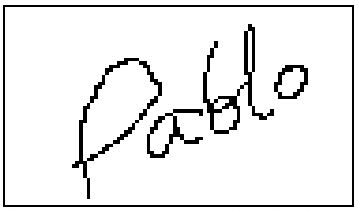

Ilustración 69: Firma digitalizada a resolución incorrecta

En sus primeros comienzos, no era difícil ver aplicaciones de captura de firma en las que el dispositivo difícilmente era capaz de emular el trazo del usuario al firmar, o que en caso de hacerlo, no era capaz de representar el trazo con la suficiente rapidez y precisión, generando trazos poligonales, o generando errores en el usuario que, al no ver el trazo generado en un intervalo de tiempo razonable, intentaba redibujarlo desfigurando el contorno de la firma.

Será siempre recomendable que un dispositivo en el que se vaya a efectuar captura de firma exista al menos una resolución de pantalla (y digitalizador) en puntos, de al menos HVGA (Half VGA 320x480), que daría una resolución de digitalización de 164 ppp con aspecto 3:2 para una pantalla de 3,5” de tamaño típica en este tipo de dispositivos. No deberían contemplarse resoluciones inferiores a 100 ppp para que la firma digitalizada cumpla con unos criterios mínimos de calidad. Idealmente se debería buscar una pantalla VGA (640x480), con aspecto 4:3, la cual daría una resolución de digitalización de 228 ppi.

Por lo tanto:

- Tamaño mínimo de pantalla: 3,5”
- Resolución mínima de pantalla y digitalizador: HVGA 320x480

Se podría usar una pantalla de menor tamaño con igual resolución de pantalla y digitalizador, lo cual daría una mayor resolución en ppi (puntos por pulgada), pero resultaría incómoda e inapropiada para la interacción con el usuario final que firma en dicha pantalla. El usuario final se sentiría incómodo firmando en una pantalla con poco espacio físico o en donde resultan ilegibles (por pequeños) o insuficientes (por falta de espacio para incluirlos) los textos e indicaciones alrededor del área de captura de firma.

Aunque legalmente no está reconocida la validez de una firma digitalizada, ni existen normativas claras al respecto, si sería conveniente en una aplicación en la que se prevea una prueba basada en firma digitalizada, no recoger el gráfico (bitmap) de la firma, sino los trazos que se han originado durante la firma sobre el digitalizador de la pantalla del terminal portátil (nº de trazo, posición (x,y) de origen, … secuencia de posiciones (x,y) de paso, posición (x,y) final, y así para cada uno de los trazos que componen la firma, entendiendo como trazo cualquier forma dibujada en la pantalla sin levantar la presión del puntero sobre la misma. De esta forma, una firma digitalizada ya no sería un simple archivo gráfico, sino que además contendría información adicional con los trazos que componen la firma para el posterior análisis si fuese preciso.

9.- COMUNICACIONES INALÁMBRICAS

Existirán diferentes alternativas para efectuar las comunicaciones de datos con nuestros sistemas centrales utilizando redes inalámbricas:

9.1.- Redes WPAN (Bluetooth)

El término ***W**ireless **P**ersonal **A**rea **N**etwork* sirve para definir todas aquellas redes inalámbricas de tipo cercano en el rango de alcance de una persona (distancia < 10 m). La más conocida y empleada de este tipo de redes es la basada en la especificación Bluetooth y que es la que se encontrará en la inmensa mayoría de terminales portátiles.

Además de servir para las comunicaciones de datos con un sistema informático de sobremesa o un laptop, podrá servir también para interconectar nuestro terminal portátil con otros dispositivos y periféricos, como por ejemplo con una impresora de tickets dotada de conectividad Bluetooth, o unos auriculares con micrófono para el usuario e incluso el sistema manos libres integrado en un vehículo.

9.2.- Redes WLAN (Wi-Fi)

Con el término WLAN (***W**ireless **L**ocal **A**rea **N**etwork*) se hace referencia a las redes wireless LAN o Wi-Fi como más son conocidas en la actualidad en su formato estandarizado basadas en el estándar IEEE 802.11.

Este tipo de redes serán las más utilizadas en los entornos industriales y empresariales, allí donde el punto de utilización de la aplicación tiene presencia informática de la organización y, por lo tanto existe una red de infraestructura LAN, dotada de puntos de acceso inalámbricos (Access Points) que darán acceso a la red de infraestructura a nuestros terminales portátiles.

9.3.- Redes WAN 2G/3G (GSM / GPRS / UMTS / HSDPA / HSUPA)

Este tipo de redes de área amplia (***W**ireless **W**ide **A**rea **N**etwork*) serán las que se emplearán cuando el punto de utilización de la solución con terminales portátiles no disponga de una infraestructura de red WLAN con la que conectar para intercambiar datos con los servicios centrales.

El hecho de que este tipo de redes lleven asociados unos costes por utilización de un operador externo (tarificación por consumo o tiempo de utilización del canal), hace que se deba ser especialmente cuidadosos en la utilización de las mismas y, utilizarlas solo cuando la alternativa de una red WAN de acceso no esté disponible.

Actualmente las redes 3G están ofreciendo velocidades de subida y bajada en España del orden de 7,5 Mbps, y se está trabajando en las redes de cuarta generación (LTE) que permitirán velocidades 10 veces mayores, sin embargo, mientras el despliegue de las redes 4G no sea completo, la cobertura de las redes 3G actuales y sus tasas de transferencia de datos quedarán lejos de las que se obtendrían utilizando una red Wi-Fi.

10.- SEGURIDAD EN LAS COMUNICACIONES

Un apartado vital en una aplicación móvil es la seguridad e integridad de los datos que se intercambian en nuestra red inalámbrica, incluso en aplicaciones cuyos datos sean poco sensitivos, ya que un fallo puede provocar en el mejor de los casos grandes trastornos posteriores, tales como mercancías mal ubicadas en un almacén, incoherencia de datos en servidores o fraudes en mercancías, y puede comprometer toda la organización al completo.

El lector puede encontrar información concerniente a la seguridad en redes inalámbricas y ampliar sus conceptos sobre seguridad en redes de datos en las dos siguientes referencias:

- El capítulo 17 del libro *"Cryptography and Network Security – Principles and Practice", 5ª Edición* de William Stallings [BSTALLI1]
- El capítulo 8 del libro "Computer Networking – A top-Down approach – 5th Edition" de James F. Kurosse y Keith W. Ross [BKUROSS1]

10.1.- Acceso a la red Wi-Fi (WLAN)

El primer punto de seguridad será el acceso a la red inalámbrica.

Es amplia la documentación existente al respecto, aunque en el presente trabajo se detallará simplemente aquella que resulta especialmente relevante y de aplicación práctica.

Se parte de la base de que es descartada cualquier conexión inalámbrica basada en encriptados WEP o WPA (***W****i-Fi* ***P****rotected* ***A****ccess*) ya que se han detectado ciertas vulnerabilidades sobre los mismos. De hecho, el estándar IEEE 802.11i ya ha tenido en cuenta esto y en base a esas recomendaciones se desarrolló WPA2.

Resumiendo toda la problemática que ha dado lugar a la aparición de WPA2, se dirá que WPA2 aporta la seguridad del encriptado AES (***A****dvanced* ***E****ncryption* ***S****tandard*) frente a TKIP (***T****emporal* ***K****ey* ***I****ntegrity* ***P****rotocol*) utilizado por WPA.

10.2.- Acceso a la red Wi-Fi con WPA2-PSK (WPA2-Personal)

Para redes domésticas o SOHO, bastará con seleccionar el mecanismo de autenticación de WPA2-PSK (***P****re-****S****hared* ***K****ey*), también denominado WPA2-Personal, aunque para redes empresariales y con mayor número de equipos existen diferentes alternativas más seguras.

Mediante este sistema, todos los equipos que acceden a un punto de acceso inalámbrico (AP), deben disponer de una clave compartida (PSK). Esta clave puede ser de hasta 64 caracteres, lo cual aporta un alto grado de seguridad con el encriptado AES.

10.3.- Acceso a la red Wi-Fi con WPA2-Enterprise o 802.1X

En el caso de redes industriales y empresariales, este sería el tipo de acceso recomendado a la red desde los terminales portátiles.

Tanto si se utiliza WPA2-Enterprise o 802.1X [IS8021X] para el acceso a la red inalámbrica, existirá un servidor AAA (***A**utentication **A**uthorization and **A**ccounting server*) para las conexiones de autenticación de los equipos. Este servidor, utilzará uno de los protocolos actualmente implantados como pueden ser RADIUS o Diameter en la red de infraestructura.

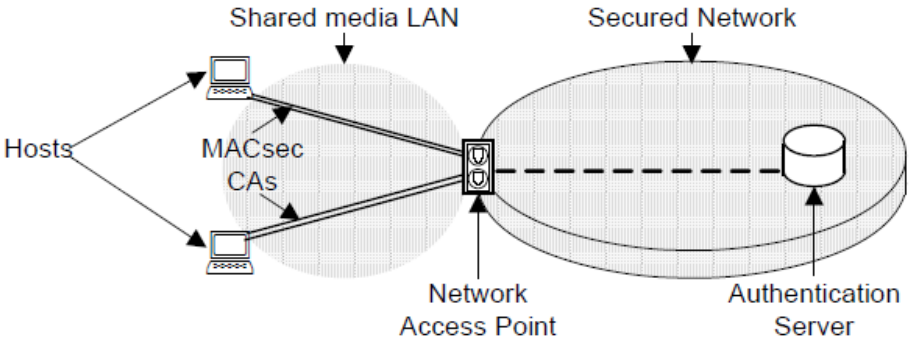

Ilustración 70: Autenticación según 802.1X o WPA2-Enterprise

El procedimiento de acceso a la red Wi-Fi es precedido por una autenticación del equipo/usuario en cuatro pasos:

1. El cliente se conecta al punto de acceso utilizando uno de los posibles protocolos de autenticación y solicita autorización.
2. El punto de acceso requiere las credenciales al dispositivo.
3. El punto de acceso, con las credenciales aportadas por el dispositivo, solicita la autenticación a un servidor AAA ubicado en la red de infraestructura LAN (fuera de la visibilidad de la red inalámbrica).
4. Si el proceso de autenticación es correcto, el punto de acceso acepta la conexión y devuelve al cliente una clave maestra para la sesión PMK (***P**airwise **M**aster **K**ey*).

En el esquema de autenticación y acceso mostrado en la ilustración (71)[6] se observa una implementación con el protocolo EAP-TLS y EAPOL en el enlace entre el suplicante (PAE), o terminal portátil y el autenticador (PAE) o punto de acceso a la red inalámbrica.

6 Las imagenes que se muestran han sido obtenida del estándar 802.1X del IEEE

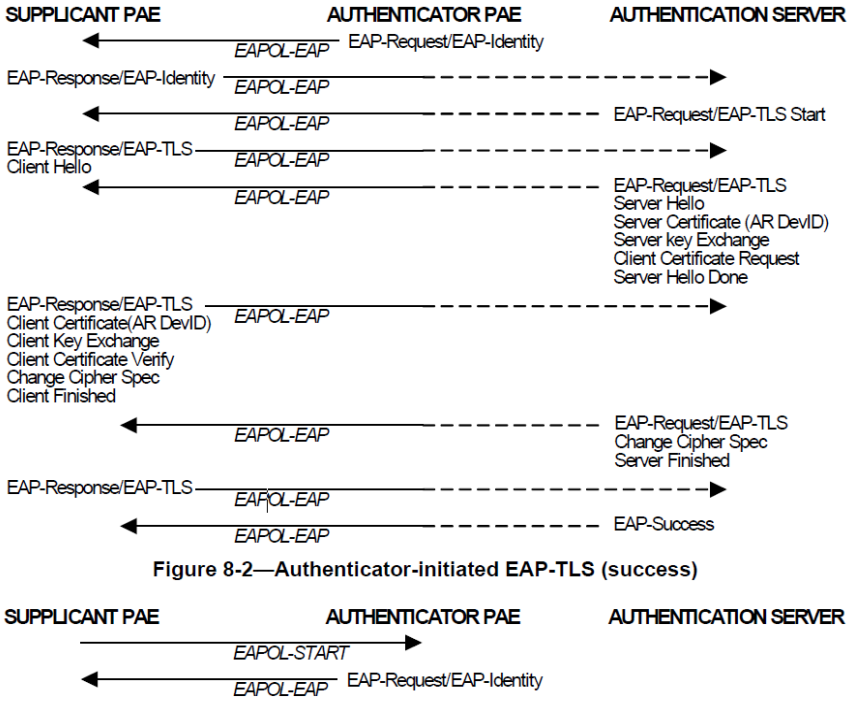

Figure 8-2—Authenticator-initiated EAP-TLS (success)

Ilustración 71: Secuencia de autenticación EAP-TLS inciada por suplicante (PAE)

Este sistema permite que los permisos y control de acceso de usuarios ya no estén en los puntos de acceso, sino oculto y bien protegido en el interior de la red de infraestructura. Los puntos de acceso a la red inalámbrica se configurarán con la clave compartida de acceso al servidor RADIUS y pedirán a este la autorización del equipo que intenta acceder a la red en cada momento.Aunque actualmente está más extendido el protocolo *RADIUS* en el servidor *AAA*, *Diameter* surge como una alternativa que pretende resolver algunas de sus deficiencias y se verá en el futuro próximo cual es la evolución en la implantación de estos protocolos.

En cuanto a los protocolos de autenticación para los dispositivos que acceden a la red inalámbrica, existen las siguientes opciones fiables y robustas basadas en el protocolo EAP (***E****xtensible* ***A****uthentication* ***P****rotocol*) definido en las RFC 3748 y RFC4017 del IETF.

- EAP-TLS (***E****xtensible* ***A****uthentication* ***P****rotocol over* ***TLS*** *tunel)*

  [ISEAPTLS]

  Definido por Microsoft en la RFC 5216 del IETF del año 2008

- PEAP v0 o simplemente PEAP (***P****rotected* ***E****xtensible* ***A****uthentication* ***P****rotocol*) [ISPEAP4]

  Definido por Microsoft en un Internet Draft del IETF en el año 2002

- PEAP v2

  [ISPEAP2]

  Definido por Microsoft y Cisco en un Internet Draft del IETF en el año 2004

10.4.- Acceso a la red WWAN

Todas las consideraciones de seguridad serán las mismas que para el acceso a través de la red WLAN, con unas ciertas diferencias.

No existe un punto de acceso inalámbrico, por lo tanto no existirá nada de lo relaccionado con el acceso a la red de infraestructura a través de un punto de acceso inalámbrico (802.1X, WPA2, ...).

El terminal remoto accede a nuestra red desde el exterior, a través de una pasarela o router de frontera y, por lo tanto, se le tratará igual que si se tratase de un usuario que se conecta a la red interna desde Internet.

Se utilizarán las técnicas de control de acceso y autenticación de usuarios disponibles para Internet.

Existirá un servidor AAA dedicado a dar servicio al router de frontera o la pasarela de acceso a nuestra red corporativa, autenticando las conexiones de los usuarios/equipos remotos, que puede ser el mismo que de acceso a las conexiones LAN, debidamente configurado, protegido y aislado.

Existen tres opciones:

- Un túnel con IPSec y establecer una conexión segura a nivel de red
- Un túnel con TLS y establecer una conexión segura a nivel de transporte
- Una conexión estándar y establecer una conexión segura con SSL a nivel de aplicación

Será decisión del diseñador de la arquitectura en función de las características de las infraestructura de red y servicios ya implantados en la corporación.

10.5.- Consideraciones acerca de las claves compartidas y contraseñas de usuario

De nada servirían todos los sistemas de seguridad anteriormente expuestos si nuestro sistema es vulnerable en el lado más simple, en la longitud y composición de las contraseñas, o en la custodia y control de las mismas por parte de los administradores de sistemas o usuarios en los que puedan recaer esa responsabilidad en un momento dado.

En cuanto a las contraseñas y claves empleadas, tanto para los usuarios como para las claves compartidas (PSK), lo más recomendable es utilizar la extensión máxima permitida, y además, emplear diferentes tipos de caracteres intercalados de forma pseudoaleatoria.

- Ejemplo 1 de clave correcta:
  - “A1k-mu78+98@77-?%32y9AZu Hmi#008yOa&9 zjHx23ap!19**##89@”
- Ejemplo 2 de clave incorrecta:
  - “navidad blanca”

La segunda clave podría hacer que un sistema pudiese ser vulnerable a un ataque por fuerza bruta basado en diccionarios. Un atacante podría capturar los mensajes encriptados de negociación con el punto de acceso, por ejemplo con un ataque de tipo 0 que obligase a la desasociación y, posteriormente intentar obtener las claves mediante el uso de diccionarios y fuerza bruta sobre los mensajes capturados. Con una clave como la primera, sería materialmente imposible un intento de descifrado por fuerza bruta asistido por diccionarios o de cualquier tipo.

En realidad, lo que sucede no es que el sistema WPA2-PSK sea vulnerable, sino que el usuario está dejando un agujero de seguridad al no configurar correctamente la clave compartida. En el ejemplo 2 se ha utilizado una clave de longitud reducida y además formada por palabras fácilmente extraibles de un diccionario y combinables.

Aunque la clave compartida sea un problema a la hora de introducirla en un pantalla de configuración (del punto de acceso o del terminal portátil), es necesario para la integridad del sistema, y únicamente hay que efectuarlo una vez.

La custodia de claves deberá ser minuciosamente vigilada por el administrador del sistema y el responsable de seguridad, de modo que, cada cierto tiempo sean cambiadas si fuese preciso, o en cualquier otra circunstancia (alta y baja de usuarios, etc...).

10.6.- Certificación Cisco CCX

Si se necesita interoperar con redes de infraestructura cuyos routers y otros elementos deban cumplir con estándares de compatibilidad de Cisco, habrá que asegurar que los equipos en cuestión tienen certificación CCX versión 4 o superior [CISCOCCX].

Cualquier equipo o software que acredite cumplir con las especificaciones Cisco CCX mostrará el siguiente logotipo:

Ilustración 72: Logotipo Cisco CCX Compatible

Mediante esta certificación, Cisco Systems acredita que un equipo va a poder interaccionar en una red homogénea con otros equipamientos de Cisco.

A continuación se muestran las versiones del programa CCX y sus certificaciones de interoperabilidad según la versión de la certificación.

La tabla (7)[7] servirá de referencia a la hora de ver que cumple un equipo en función de la versión de CCX que certifica.

Standards	v1	v2	v3	v4	v5	ASD	CCX Lite (Available June 2011)			
							Foundation	**Voice**	**Location**	**Management**
IEEE 802.11x	X	X	X	X	X	X	X			
Wi-Fi compliance	X	X	X	X	X	X	X			
IEEE 802.1X	X	X	X	X	X	X	X			
Windows Hardware Quality Labs (WHQL) – for Windows only	X	X	X	X	X		X			
Wi-Fi Protected Access (WPA)		X	X	X	X	X	X			
IEEE 802.11i – WPA2			X	X	X	X	X			
Wi-Fi Multimedia (WMM)			X	X	X	X		X		
Security	**v1**	**v2**	**v3**	**v4**	**v5**	**ASD**	**Foundation**	**Voice**	**Location**	**Management**
IEEE 802.1X	X	X	X	X	X	X	X			
LEAP	X	X	X	X	X	*See note 1*				
PEAP with EAP-GTC (PEAP-GTC)		X	X	X	X	*optional*				
EAP-FAST			X	X	X	*See note 1*	**X**			
PEAP with EAP-MSCHAPv2 (PEAP-MSCHAP)				X	X	*optional*				
EAP-TLS				X	X	*See note 1*				

7 La tabla que se muestra con las versiones de CCX ha sido obtenida de la web de Cisco Systems

Wi-Fi Protected Access (WPA): 802.1X + WPA TKIP		X	X	X	X	X	**X**			
With LEAP		X	X	X	X	*See note 1*				
With PEAP-GTC		X	X	X	X	*optional*				
With EAP-FAST			X	X	X	*See note 1*	**X**			
With PEAP-MSCHAP				X	X	*optional*				
With EAP-TLS				X	X	*See note 1*				
IEEE 802.11i – WPA2: 802.1X + AES			X	X	X	X	**X**			
With LEAP			X	X	X	*See note 1*				
With PEAP-GTC			X	X	X	*optional*	X			
With EAP-FAST			X	X		*optional*	**X**			
With PEAP-MSCHAP				X	X	*optional*				
With EAP-TLS				X	X	*optional*				
Network Admission Control (NAC)				X	X					
Management Frame Protection					X	X	**X**			
Mobility	**v1**	**v2**	**v3**	**v4**	**v5**	**ASD**	**Foundation**	**Voice**	**Location**	**Management**
AP-assisted roaming		X	X	X	X	X	**X**			
Fast 802.1X reauthentication via Cisco Centralized Key Management (CCKM)						*See note 1*	**X**			
With LEAP		X	X	X	X	*See note 1*	**X**			
With EAP-FAST			X	X	X	*See note 1*	**X**			
With PEAP-GTC				X	X		**X**			
With PEAP-MSCHAP				X	X		**X**			
With EAP-TLS				X	X	*optional*	**X**			
Status/result code Interpretation				X	X					
Quality of Service (QoS) and VLANs	**v1**	**v2**	**v3**	**v4**	**v5**	**ASD**	Foundation	**Voice**	**Location**	**Management**
Interoperability with APs that support multiple SSIDs and VLANs	X	X	X	X	X	X				
Wi-Fi Multimedia (WMM)			X	X	X	X		**X**		
Call Admission Control				X	X	X		**X**		
Expedited Bandwidth Request				X	X	*optional*		**X**		
Performance and Management	**v1**	**v2**	**v3**	**v4**	**v5**	**ASD**	**Foundation**	**Voice**	**Location**	**Management**
RF scanning and reporting		X	X	X	X	X	**X**			

AP-specified maximum transmit power		X	X	X	X	X	**X**			
Facility for migrating from LEAP to EAP-FAST*			X	X	X	*See note 1*	**-**			
Single signon on Windows for LEAP and EAP-FAST			X	X	X	*optional*	**-**			
Recognition of proxy ARP information element			X	X	X	X	**X**			
Keep Alive				X	X	*optional*	**-**			
Link Test				X	X	*optional*				**X**
UPSD				X	X	X				
Voice Metrics				X	X	X		**X**		
Location				X	X	*optional*			**X**	
Performance					X	X	**X**			
Troubleshooting connectivity	**v1**	**v2**	**v3**	**v4**	**v5**	**ASD**	**Foundation**	**Voice**	**Location**	**Management**
Diagnostic Channel					X	X				**X**
Client Reporting					X	X				**X**
Roaming and real time Diagnostics					X	X				**X**

Tabla 7: Versiones de Cisco CCX

10.7.- Certificación FIPS 140-2

Esta acreditación [USFIPS2] la da el NIST (*National Institute of Standards and Technology*) en USA, y acredita que un dispositivo dispone de algoritmos y técnicas de criptografía segura para operar en instituciones del gobierno de los Estados Unidos de América.

En caso de trabajar con altos requerimientos de seguridad, esta certificación en el software de criptografía del equipo dará un plus de seguridad. En el caso de tener que instalar nuestros equipos en una institución oficial USA será imperativo que nuestros equipos dispongan de esta certificación.

11.- CONSIDERACIONES PARA REALIZAR UNA PRUEBA PILOTO

Existen algunas consideraciones que deberán ser tenidas en cuenta con respecto a la realización de un prueba piloto de una solución móvil profesional con terminales portátiles. De todas las posibles consideraciones a tener en cuenta, se han elegido dos que afectarán en gran medida en los proyectos que involucran terminales portátiles.

- Ubicación de la prueba piloto
- Número de equipos involucrados

11.1.- Elección de la ubicación de la prueba piloto

Imaginemos una empresa con múltiples delegaciones a lo largo de todo el territorio. En este caso, una primera tentación sería realizar la prueba piloto en la más pequeña y cercana a las oficinas centrales de todas las delegaciones. Esto, que sería correcto en otro tipo de soluciones con entornos de aplicación homogéneos, sería nefasto en nuestro caso.

Ahora imaginemos que el punto crítico de nuestra solución son las condiciones ambientales en lo concerniente al polvo y agua. En este caso, se debería elegir como lugar para la prueba piloto aquella ubicación en la que las condiciones de polvo y agua sean las peores posibles en un momento determinado del tiempo, y en esos momentos determinados (en plena manipulación con gran cantidad de polvo) se deberían hacer la prueba piloto.

Si el punto crítico de la solución fuesen las altas temperaturas que tuviesen que soportar los equipos, entonces se debería elegir la ubicación más calurosa y en la época más calurosa del año.

Esto es así, porque a menudo se olvida la famosa frase de *"La realidad siempre supera a la ficción"* y, del mismo modo, el entorno real, en muchos casos, supera todos los cálculos y precauciones iniciales en requerimientos y especificaciones. Un ejemplo, podría ser un equipo que se ha pensado que debería soportar temperaturas de no más de 45ºC y que, al poner en marcha la prueba piloto, se observa que los equipos superan ampliamente ese límite.

Un estudio posterior, podría mostrar que eso es debido a que los conductores del vehículo dejan los equipos en el salpicadero, quedando el mismo cerrado mientras van a comer a un restaurante de carretera en una zona casi desértica.

Idealmente, este tipo de prueba ambiental se debería haber efectuado también en la fase de pruebas de los terminales, pero como en esa fase no interviene el usuario final del equipo (el camionero), al técnico que efectuase las pruebas probablemente no se le pasaría por la cabeza esa situación, de modo que, solamente sería descubierta en la prueba piloto.

No se elegirán las condiciones más cómodas para la prueba piloto, sino las más exigentes.

11.2.- Número de equipos para prueba piloto

Teniendo en cuenta las singularidades de cada usuario final de los equipos y el número de

usuarios total en la ubicación donde se lleva a cabo la prueba piloto, para que esta arroje resultados amplios y representativos, el número mínimo de usuarios participando en la prueba debería ser al menos del 20% del total. Esto sería 2 de cada 10 usuarios de la ubicación. Idealmente podría ser el total de la ubicación, pero en ocasiones esto no es posible, especialmente si se trata de un entorno de trabajo 24h con requerimientos de alta disponibilidad (fabricación intensiva) y actividades críticas (que no se pueden ver afectadas en gran medida por el fallo de un equipo).

El número de equipos involucrados en la prueba piloto debería ser el máximo y, siempre que no pueda ser la totalidad, se intentará que exista al menos un volumen representativo del 20%.

12.- CONSIDERACIONES PARA EL DESPLIEGUE (ROLL-OUT) DE UNA SOLUCIÓN

Solamente habrá que tener en cuenta a la hora de hacer el despliegue de una solución móvil (Roll-Out) y es que, puesto que este tipo de soluciones son altamente dependientes del entorno de aplicación y del usuario final que la va a utilizar, se debererá ser especialmente cuidadosos si, en el último momento se pretende cambiar el listado de ubicaciones físicas en las que se va a efectuar el despliegue de la solución.

No hay que olvidar que, desde las primeras etapas del proyecto, se basaron los requerimientos, se seleccionaron los terminales portátiles y, redactaron las especificaciones del desarrollo software e integración de sistemas teniendo en mente el entorno definitivo en el que sería utilizada la solución móvil. No será válido, por lo tanto, introducir una nueva ubicación al despliegue cuyas condiciones ambientales, perfiles de usuarios y operativa de trabajo difiera sustancialmente de los parámetros definidos inicialmente para el proyecto.

Este es un error muy común, y se puede ilustrar con el ejemplo siguiente:

La empresa X ha desarrollado una solución móvil basada en terminales portátiles para una red de inspectores de calderas de calefacción. Durante todo el proyecto se definió entre otros, que algunos de los requerimientos fundamentales que marcarían el proyecto serían:

- Sellado IP 42
- Rango de Temperaturas de operación de -10 a 40º C
- Resistencia a caída libre MIL-STD-810G (1,22 m)
- Perfil de usuario: medio y sin guantes

Una vez realizado el despliegue de todas las ubicaciones contempladas en el proyecto incial, se decide incluir en el mismo una última ubicación, para otros inspectores que utilizarán el mismo software y los mismos procedimientos, pero para inspeccionar maquinaria industrial de campo.

De repente, se ha incluido un nuevo proyecto sin darse cuenta, ya que la última ubicación tiene algunos requerimientos que difieren de los del proyecto inicial:

- Sellado IP 67
- Rango de Temperaturas de operación de -10 a 50º C
- Resistencia a caída libre MIL-STD-810G (1,22 m) + 1,8 m posible
- Resistencia a vibraciones y caída repetida en movimiento
- Perfil de usuario: medio con guantes gruesos de trabajo
- Luminancia de pantalla +1000 NIT para trabajo a luz del sol directa

El simple hecho de que el usuario incorpore guantes gruesos de trabajo ya obligará a cambiar todo el interfaz de usuario de los aplicativos y los requerimientos del entorno obligarán a empezar de nuevo todo el proceso de selección de terminales. ¡OTRO PROYECTO DISTINTO!

13.- CONCLUSIONES Y TRABAJO FUTURO

El presente trabajo abre la puerta a futuros estudios y guías de referencia acerca del diseño de soluciones móviles profesionales mediante terminales portátiles, la utilización de tecnologías de identificación automática, captura avanzada de datos y comunicaciones inalámbricas.

Sería muy interesante en un futuro que se profundice en algunos apartados y pueda incluir más cantidad de documentación y especificaciones.

Un apartado dedicado a las interfaces de usuario sería especialmente interesante, así como la gestión de la energía y las comunicaciones en entornos híbridos (WLAN-WWAN-WPAN).

El entorno de la seguridad en las redes de datos y especialmente los entornos wireless y el impacto de las nuevas tecnologías como WiMAX / LTE serían también bienvenidos en un futuro trabajo.

DIAGRAMAS

No existe contenido en esta sección.

Esta página se deja deliberadamente en blanco.

PLIEGO DE CONDICIONES

1.- ESTÁNDAR IEC 60529 (INGRESS PROTECCION)

En lo concerniente a la protección ante el ingreso de sólidos (polvo) o agua en terminales portátiles, el estándar más empleado a nivel internacional es el IEC 60529, también conocido como *"Estándar IP"*. Este estándar [ISTDIP] define un sistema de clasificación para los niveles de protección provistos por las carcasas, cubiertas y sellados que protegen los componentes y partes internas de los equipos eléctricos / electrónicos, frente a amenazas externas como el ingreso de agua y partículas sólidas así como del contacto de las partes interiores con objetos externos. El estándar IP (no confundir con el protocolo IP en comunicaciones de datos), también especifica de forma clara y concisa los test que deben pasar los equipos para poder ser identificados con un determinado código de protección IP.

1.1.- Niveles de protección según la codificación IP

Los niveles de protección IP se establecen mediante un código formado por las letras *IP*, seguidas por 2 números (*SA*) y 2 letras (*CT*) opcionales. De esta forma, se definen todos los posibles grados de protección de la siguiente forma: ***IP SACT***

1.2.- S (Sólidos)→ 1º dígito del nivel de protección *IP*

El dígito S determina el nivel de protección ante el acceso a partes peligrosas y el ingreso de sólidos. *S* es un número del 0 al 7 que indica el nivel de protección del equipo ante el posible acceso a sus partes peligrosas del interior y, simultáneamente, ante el ingreso de sólidos en el interior del equipo. El nivel más alto (7) corresponde al mayor nivel de protección posible según el estándar y el 0 indica que el equipo carece de protección alguna. El significado detallado de cada uno de los niveles de protección indicados por el primer dígito del código *IP* se puede encontrar en la tabla que se muestra a continuación.

S: 1er Dígito (Código IP)	Acceso a partes peligrosas	Ingreso de sólidos
0	**No protegido**	**No protegido**
1	**Protegido ante el acceso con el dorso de la mano** Una sonda de prueba esférica de 50 mm Ø debería quedar libre del acceso a partes peligrosas del equipo	**Protegido ante sólidos de 50 mm Ø** Un objeto esférico de prueba de 50 mm Ø no debería penetrar completamente
2	**Protegido ante el acceso con un dedo de la mano** Una sonda de prueba de 12 mm Ø y 80 mm de longitud, debería quedar libre del acceso a partes peligrosas	**Protegido ante sólidos de 12,5 mm Ø.** Un objeto esférico de prueba de 12,5 mm Ø no debería penetrar completamente
3	**Protegido ante el acceso con una herramienta** Una sonda de prueba de 2,5 mm Ø no debería penetrar	**Protegido ante sólidos de 2,5 mm Ø** Un objeto esférico de prueba de 2,5 mm Ø no debería penetrar

S: 1er Dígito (Código IP)	Acceso a partes peligrosas	Ingreso de sólidos
4	**Protegido ante el acceso con hilo/alambre** Un sonda de prueba de 1 mm Ø no debería penetrar	**Protegido ante sólidos de 1,0 mm Ø** Un objeto esférico de prueba de 1,0 mm Ø no debería penetrar
5	**Protegido ante el acceso con hilo/alambre** Un sonda de prueba de 1 mm Ø no debería penetrar	**Protegido ante el polvo** El ingreso de polvo en el equipo, aunque no sea evitado en su totalidad, no debería penetrar en cantidad suficiente para interferir el óptimo funcionamiento del equipo en prueba
6	**Protegido ante el acceso con hilo/alambre** Una sonda de prueba de 1 mm Ø no debería penetrar	**Sellado ante el polvo** El polvo no debería penetrar de ninguna forma en el interior del equipo

Tabla 8: Nivel de Protección IP - 1º dígito numérico

1.3.- A (Agua)→ 2º dígito del nivel de protección *IP*

El dígito *A* determina el nivel de protección frente al ingreso de agua. Se trata de un número del 0 al 8 que determina el nivel de protección del equipo frente al ingreso de agua en el interior del equipo. El nivel más alto (8) corresponde al mayor nivel de protección posible según el estándar y el 0 indica que el equipo carece de protección alguna.

A: 2º Dígito (Código IP)	Protección ante el ingreso de agua
0	**No protegido**
1	**Protegido ante gotas de agua en vertical** El equipo debe soportar gotas de agua que caigan en vertical sobre el mismo en su posición habitual de funcionamiento sin sufrir efectos perjudiciales
2	**Protegido ante gotas de agua entre +15º y -15º respecto a la vertical** El equipo debe soportar gotas de agua que caigan en cualquier ángulo comprendido entre +15º y -15º (ambos inclusive) con respecto a la vertical sobre el mismo en su posición habitual de funcionamiento sin sufrir efectos perjudiciales
3	**Protegido ante lluvia fina de agua entre +60º y -60º respecto a la vertical** El equipo debe soportar lluvia fina de agua proyectada en cualquier ángulo comprendido entre +60º y -60º (ambos inclusive) con respecto a la vertical sobre el mismo en su posición habitual de funcionamiento sin sufrir efectos perjudiciales
4	**Protegido ante salpicaduras de agua** Cualquier salpicadura de agua proyectada sobre el equipo desde cualquier dirección no debería tener efectos perjudiciales sobre el equipo
5	**Protegido ante chorros de agua** Cualquier chorro de agua proyectado sobre el equipo desde cualquier dirección no debería tener efectos perjudiciales sobre el equipo

A: 2º Dígito (Código IP)	Protección ante el ingreso de agua
6	**Protegido ante chorros de agua a presión** Cualquier chorro de agua a presión proyectado sobre el equipo desde cualquier dirección no debería tener efectos perjudiciales sobre el equipo
7	**Protegido ante la inmersión temporal** La inmersión del equipo en agua, de forma temporal, en condiciones estandarizadas de tiempo y presión no deberían provocar entrada de agua en el equipo suficiente para ocasionar efectos perjudiciales en el mismo
8	**Protegido ante la inmersión continua** La inmersión del equipo en agua, de forma continua, en condiciones acordadas entre el fabricante del equipo y el usuario final, siempre que se supere el umbral de protección correspondiente al nivel 7, no deberían provocar entrada de agua en el equipo suficiente para ocasionar efectos perjudiciales en el mismo

Tabla 9: Nivel de Protección IP – 2º dígito numérico

1.4.- C (Contacto)→ Letra Adicional

La letra *C* determina el nivel de protección frente al contacto con partes internas del equipo. Se trata de una letra opcional que el fabricante puede decidir aportar o no en función de las características y objetivo de uso del equipo. La el valor de C=D corresponde al mayor nivel de protección posible según el estándar y C=A indica que el equipo carece de protección alguna.

C: Letra Adicional	Significado
A	**Protegido ante el acceso con el dorso de la mano** Un objeto de prueba de 50 mm Ø no debería poder acceder a partes peligrosas
B	**Protegido ante el acceso con un dedo** Un objeto de prueba de 12 mm Ø y 80 mm de longitud no debería poder acceder a partes peligrosas
C	**Protegido ante el acceso con una herramienta** Un objeto de prueba de 2,5 mm Ø y 100 m de longitud debería quedar libre del acceso a partes peligrosas
D	**Protegido ante el acceso con un hilo/alambre** Un objeto de prueba de 1,0 mm Ø y 100 mm de longitud no debería poder acceder a partes peligrosas

Tabla 10: Nivel de Protección IP - Letra C Adicional

1.5.- T (Tipo)→ Letra Suplementaria

La letra *T* provee de información suplementaria sobre el tipo de pruebas efectuadas sobre el equipo.

Al igual que en el caso anterior, también se trata de una letra opcional que el fabricante puede decidir incorporar o no en la certificación de su equipo. Puede tener los valores que se indican a continuación.

T: Letra Suplementaria	Significado
H	Aparato de alta tensión
M	Probado ante los efectos perjudiciales del ingreso de agua cuando sus partes móviles (por ejemplo un rotor) se encontraban en movimiento
S	Probado ante los efectos perjudiciales del ingreso de agua cuando sus partes móviles (por ejemplo un rotor) no se encontraban en movimiento
W	Adecuado para su uso bajo las condiciones meteorológicas especificadas y provisto de otras funcionalidades protectoras o procedimientos

Tabla 11: Nivel de Protección IP - Letra T Suplementaria

1.6.- Posibilidades de codificación IP

IP44 – Sin letra adicional ni opción

IPX5 – Omisión de la primera cifra característica

IP2X – Omisión de la segunda cifra caracterísitica

IP20C – Utilización de una letra adicional

IPXXC – Omisión de las cifras características y utilización de una letra adicional

IPX1C – Omisión de la primera cifra característica y utilización de una letra adicional

IP3XD – Omisión de la segunda cifra característica y utilización de una letra adicional

IP23S – Utilización de una letra suplementaria

IP21CM – Utilización de una letra adicional y otra suplementaria

IPX5/IPX7 – Indicación de dos grados de protección diferentes de una carcasa frente a los chorros de agua y la inmersión temporal

1.7.- Condiciones generales para el ensayo de equipos

Todos los equipos deben ser testados siguiendo las directrices del estándar IEC 60068-1, que son las siguientes:

- Rango de temperatura: 15ºC a 35ºC
- Humedad relativa: 25% a 75%
- Presión atmosférica: de 860 mbar a 1060 mbar (86 kPa a 106 kPa)

Aparte de las condiciones atmosféricas para el test de los equipos, la norma del estándar IEC 60529 establece condiciones estrictas y detalladas a la hora de efectuar los mismos. Se detallan las medidas de las sondas y objetos de prueba a emplear, así como por ejemplo, el volumen de agua con el que deben ser sometidos los equipos, la fuerza con que se debe intentar penetrar en un orificio por parte de un objeto de prueba o las condiciones de inmersión de un equipo en agua.

2.- ESTÁNDAR IEC 60590-01, APARTADO 4.2.6

Este estándar mucho más amplio, establece en su apartado 4.2.6 los requerimientos que deben pasar los equipamientos portátiles con respecto a la protección frente a caídas.

En este particular, la norma establece que, deberán estar protegidos frente a impacto por caída, todos los equipos que cumplan las siguientes características:

- Dispositivos portátiles (Hand-held Equipment)
- Equipos de conexión directa con el usuario (Direct Plug-In Equipment)
- Equipos transportables (Transportable Equipment)
- Equipos de escritorio con una masa de 5 Kg o menos, que se encuentren conectados con el usuario final mediante un cable, head-set u otro dispositivo acústico.

Todos estos aparatos deben soportar pruebas de caida con los siguiente requerimientos mínimos:

- Caídas desde 750 mm +- 10 mm de altura para equipos de sobremesa
- Caídas desde 1000 mm +- 10 mm para terminales portátiles (hand-held)

Además de esta normativa, ya obsoleta por otras posteriores del IEC, los principales fabricantes aplican test más estrictos y exigentes, o en algunos modelos incluso certifican la especificación militar de los Estados Unidos de América MIL-STD-810G [US810G], excediendo sus requerimientos.

3.- ESTÁNDAR MILITAR MIL-STD-810-G (USA)

Este estándar [US810G] asegura que todos los equipos que cumplen esta especificación puedan ser utilizados por el ejército de los Estados Unidos de América como equipamiento de serie en los propósitos para los que ha sido certificado.

Este tipo de estándar se centra más en pruebas y test orientados a garantizar el funcionamiento del equipo en situaciones reales adversas y diferentes tipos de riesgos. Se encarga de garantizar que un equipo certificado con esta norma puede soportar las peores condiciones previstas en el uso diario por los miembros del ejército y, para este propósito, está compuesto por toda una serie de métodos y procedimientos de test que permiten evaluar los equipos ante determinadas situaciones.

En la tabla que se muestra a continuación[8] (12) se relacionan los diferentes métodos de test contemplados en este estándar militar.

No.	Title	Pages	No. of pages
500	Low Pressure (Altitude)	500.5-1 – 500.5-7	7
501	High Temperature	501.5-1 – 501.5-13	13
502	Low Temperature	502.5-1 – 502.5-9	9
503	Temperature Shock	503.5-1 – 503.5-13	13
504	Contamination by Fluids	504.1-1 – 504.1C-1	15
505	Solar Radiation (Sunshine)	505.5-i – 505.5C-8	33
506	Rain	506.5-1 – 506.5-11	11
507	Humidity	507.5-1 – 507.5A-1	21
508	Fungus	508.6-1 – 508.6B-1	13
509	Salt Fog	509.5-1 – 509.5-10	10
510	Sand and Dust	510.5-1 – 510.5-13	13
511	Explosive Atmosphere	511.5-1 – 511.5-8	8
512	Immersion	512.5-1 – 512.5-7	7
513	Acceleration	513.6-1– 513.6A-6	19
514	Vibration	514.6-i – 514.6E-8	93
515	Acoustic Noise	515.6-1 – 515.6B-2	15
516	Shock	516.6-i – 516.6C-4	59
517	Pyroshock	517.1-i – 517.1-24	26
518	Acidic Atmosphere	518.1-1 – 518.1-7	7
519	Gunfire Shock	519.6-i – 519.6E-7	83
520	Temperature, Humidity, Vibration, and Altitude	520.3-i – 520.3-22	24
521	Icing/Freezing Rain	521.3-1 – 521.3-7	7
522	Ballistic Shock	522.1-1 – 522.1-14	14
523	Vibro-Acoustic/Temperature	523.3-i – 523.3A-9	28
524	Freeze-Thaw	524-1 – 524-6	6
525	Time Waveform Replication	525-i – 525B-11	57
526	Rail Impact	526-1 – 526-7	7
527	Multi-Exciter Testing	527-i – 527D-3	37
528	Mechanical Vibrations Of Shipboard Materiel (Type I – Environmental And Type II – Internally Excited)	528-i – 528B-3	27
Part One	Environmental Engineering Program Guidelines	PART ONE-i – PART ONE D-1	63
Part Two	Laboratory Test Methods	PART TWO-1 – 528B-3	683
Part Three	World Climatic Regions – Guidance	PART THREE-i – PART THREE C-2	53

Tabla 12: MIL-STD-810G - Métodos de Test

8 Tabla extraída del documento del estándar MIL-STD-810G, Fuente: US Department of Defense

A pesar de ser una norma de uso militar, también es utilizada como referencia para certificar aparatos que deban cumplir unos determinados requerimientos o protecciones para trabajar en entornos exigentes.

El presente estudio, se centrará en revisar aquellos apartados susceptibles de ser aplicados o requeridos a un terminal portátil.

3.1.- METHOD 516.6 – SHOCK

Este método de test en sus diferentes procedimientos pone a prueba la capacidad del equipo de soportar caídas y golpes. En el estándar [US810G] se establece el método de test nº 516.6 (SHOCK) compuesto por los siguientes procedimientos de test:

- Procedure I - Functional Shock.
- Procedure II - Materiel to be packaged.
- Procedure III – Fragility.
- Procedure IV - Transit Drop.
- Procedure V - Crash Hazard Shock Test.
- Procedure VI - Bench Handling.
- Procedure VII - Pendulum Impact.
- Procedure VIII - Catapult Launch/Arrested Landing

De los procedimientos indicados, solamente son aplicables a los terminales portátiles en su uso habitual por un operador o en su manipulación convencional los procedimientos I, IV y VI, que son los que se verán con más detalle. El resto, solamente serían de aplicación si los terminales portátiles tuviesen que ir montados en vehículos, embarcaciones o aeronaves y/o tuviesen que soportar impactos extremos o accidentes más allá del uso habitual por parte de un operador.

3.1.1.- Procedimiento I – Impacto funcional (*Functional Shock*)

Este procedimiento ha sido diseñado para probar material eléctrico, hidraúlico y electrónico, en su modo funcional (encendido y operando), y evaluar su integridad física, continuidad y funcionalidad ante un impacto.

En general al equipo se le requiere que funcione durante la prueba de impacto y sobreviva sin daños ni malfuncionamiento a los impactos que pueda tener que soportar durante la misma.

Este procedimiento se basa en el análisis del SRS (*Shock Response Spectrum*) del equipo en respuesta a un impacto, mostrando las aceleraciones sufridas antes, durante y después del impacto. También utiliza la distribución espectral de energías ESD (*Energy Spectral Density*), las energías absorbidas y disipadas por el equipo durante y después del impacto.

Estos datos son tratados y procesados con métodos estadísticos y deben resultar dentro de unos rangos aceptables para el equipo sin sufrir daños ni malfuncionamiento. A continuación se muestran dos gráficas[9] de SRS (ilustración 73) y de ESD (ilustración 74).

9 Imágenes extraídas del documento del estándar MIL-STD-810G. Fuente: US Department of Defense

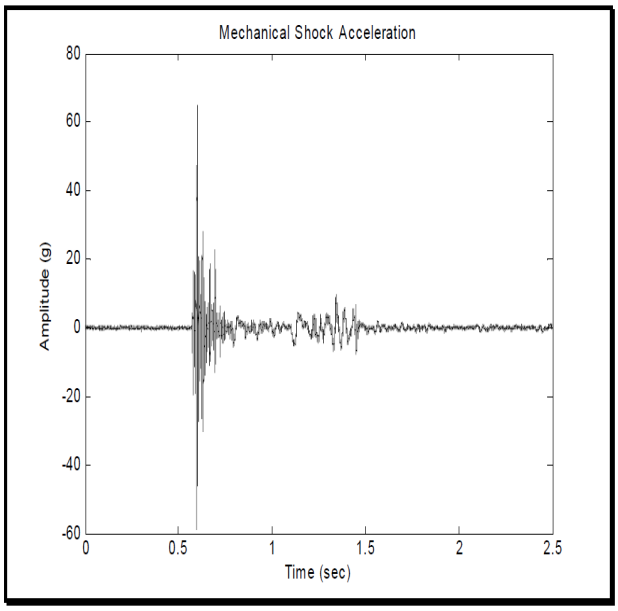

Ilustración 73: MIL-STD-810G METHOD 516.6 Proc I - SRS

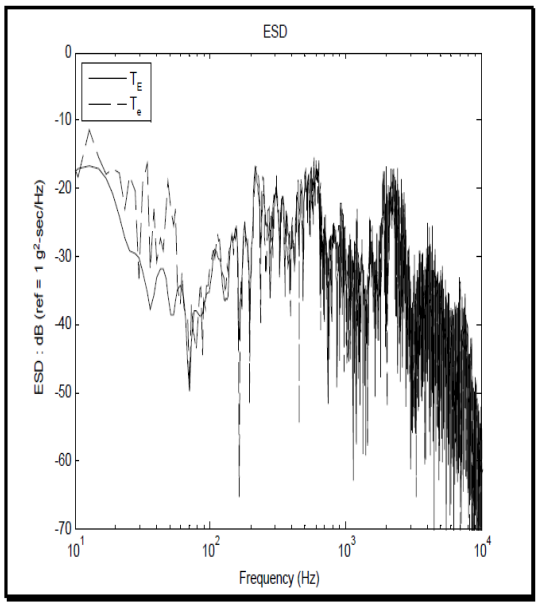

Ilustración 74: MIL-STD-810G METHOD 516.6 Proc. I - ESD

3.1.2.- Procedimiento IV – Caida en tránsito (*Transit Drop*)

Este procedimiento es utilizado para determinar si un equipo puede soportar las operaciones habituales de transporte, carga y descarga, mantenimiento, en su retirada de un estante o alojamiento, en su colocación en elementos de transporte, o una combinación de varias acciones,

Table 516.6-VI. Transit drop test.

Weight of Test Item & Case kg (lbs)	Largest Dimension, cm (in)	Notes	Height of Drop, h cm (in)	Number of Drops
Under 45.4 (100) Manpacked or man-portable	Under 91 (36)	A/	122 (48)	Drop on each face, edge and corner; total of 26 drops D/
	91 & over	A/	76 (30)	
45.4 - 90.8 (100 – 200) inclusive	Under 91	A/	76 (30)	Drop on each corner; total of eight drops
	91 & over	A/	61 (24)	
90.8-454 (200 – 1000) inclusive	Under 91	A/	61 (24)	
	91 – 152 (36 – 60)	B/	61 (24)	
	Over 152	B/	61 (24)	
Over 454	No limit	C/	46 (18)	Drop on each bottom edge. Drop on bottom face or skids; total of five drops

Tabla 13: MIL-STD-810G Transit Drop Test

así como los posibles impactos accidentales o caídas a los que puede estar sometido durante las mismas.

El equipo a ser probado deberá tener la misma configuración que es usada en una situación de transporte, manipulación o combate y, mediante este procedimiento de test es con el que realmente se simula la caída libre del objeto desde una altura determinada sobre el suelo.

La superficie de prueba debe ser una madera contrachapada de al menos 50,8 mm (2 inch) de espesor sobre una base de apoyo de hormigón.

En la tabla[10] (13) se pueden observar las diferentes alturas a las que deben ser probados los equipamientos en caída libre y el número mínimo de impactos que deben soportar, todo esto en función de su peso y sus medidas máximas.

Para el caso que se trata (terminales portátiles), siendo equipos con peso inferior a 45,4 Kg (100 lbs) y medida máxima inferior a 91 cm (36 inch), serán probados desde una altura de 1,22 m (48 inch) que es considerada la altura típica a la cual el operador sujeta o manipula estos dispositivos.

Los equipos son soltados en caída libre y deben soportar al menos 26 impactos, de forma que se cubra con un impacto al menos todas sus posibles caras, bordes y esquinas. Esto se ha considerado así para contemplar el hecho de que la mayoría de las carcasas de dispositivos tienen forma hexaédrica y disponen de 6 caras, 12 aristas y 8 esquinas, con un total de 26 zonas diferenciadas de posible impacto.

3.1.3.- Procedimiento VI – Manipulación en banco de trabajo (*Bench handling*)

Este procedimiento evalua la capacidad de soportar múltiples impactos durante las labores de empaquetado y mantenimiento o utilización en banco de trabajo del equipo en cuestión.

Solamente será aplicable a aquellos equipos cuya carcasa tenga la mayor de sus medidas superior a 23 cm (9 in). La inmensa mayoria de terminales portátiles disponen de medidas inferiores.

El test se basa en soltar el equipo sobre sus aristas para impactar sobre una mesa de pruebas de madera. La mesa debe tener un espesor mínimo de 4,25 cm (1,675 in). Se suelta el equipo para impactar sobre esta mesa en caída libre desde una altura de 100 mm (4 in) y, se efectúa de forma que en el momento de soltar el equipo en caída libre sobre la mesa el plano horizontal de la cara de la carcasa a probar forme 45º con la horizontal del banco de prueba. La prueba se repite cuatro veces sobre cada una de las posibles caras de utilización o colocación del equipo.

3.2.- Condiciones generales para el ensayo de equipos

Todos los equipos deben ser evaluados bajo dos posibles condiciones ambientales, según el diferente tipo de prueba a efectuar.

3.2.1.- Ambiente estándar (Standard Ambient)

Cuando se especifica ambiente estándar se utilizan los valores indicados a continuación:

- Temperatura: 25° ± 10°C (77 ± 18°F)
- Humedad Relativa: 20% a 80%
- Presión Atmosférica: La de la ubicación del test

10 Tabla extraída del documento del estándar MIL-STD-810G, Fuente: US Department of Defense

3.2.2.- Ambiente Controlado (Controlled Ambient)

En aquellas pruebas en las que las condiciones de ambiente deban ser controladas se mantienen las siguientes condiciones ambientales:

- Temperatura: 23° ± 2°C (73 ± 3.6°F)
- Humedad Relativa: 50% + 5%
- Presión Atmosférica: 96.45 +6.6 / -10.0 kPa (28.5 +2.0 / -3.0 in Hg)

PRESUPUESTO

PRESUPUESTO PARA LA REALIZACIÓN DEL PRESENTE TRABAJO

Concepto	Cantidad	Importe Total
Ordenador Personal con Windows 7 (unidades)	1	599
Equipo multifunción A4 color láser (unidades)	1	575
Ordenador Personal con Linux Ubuntu (unidades)	1	425
Cables de conexión USB, Ethernet, … (unidades)	3	15
Punto de Acceso Inalámbrico Wi-Fi (unidades)	1	75
Switch Fast Ethernet 5 puertos (unidades)	1	50
Análisis y estudio de equipos y características (días/hombre)	10	2400
Análisis y estudio de tecnologías específicas de dispositivos (días/hombre)	10	2400
Análisis y estudio de normativas y directivas diversas (días/hombre)	5	1200
Análisis y estudio de SDKs y herramientas de desarrollo (días/hombre)	10	2400
Recopilación de resultados y conclusiones (días/hombre)	5	1200
Redacción del documento final del trabajo (días/hombre)	20	4800
Documentos PDF de estándares IEC 60068-2-32 (16 CHF), 60068-2-31 (70 CHF), 60068-2-27 (200 CHF), 60068-2-64 (200 CHF), 60529 Edic. 2.1 (250 CHF), 60749-37 (90 CHF) Total 6 documentos por importe total de 826 CHF (1 CHF = 0,82087 EUR)	5	686
Documentos PDF de estándares del IEEE 802.11-2012 (5 USD), 802.11i-2004 (5 USD). Total 2 documentos por importe total de 10 USD (1 USD = 0,79269 EUR)	2	8
Documentos PDF de estándares UL 913 (798 USD) y NEC (80 USD). Total 2 documentos por importe total de 878 USD (1 USD = 0,79269 EUR)	1	696
Microsoft Visual Studio 2008 Professional	1	550
Acceso a Internet ADSL 6 Mbps (cuota mensual)	3	145
Edición y encuadernado de 3 libros	3	30
Total Presupuesto (EUR) por todos los conceptos anteriores		**18.254 EUR**

Tabla 14: Presupuesto del trabajo

Este presupuesto ha contemplado el caso más desfavorable con costes de personal externo (30 € / hora, 240 € / día / hombre) para la realización del trabajo. De no ser así, habría que deducir del presente presupuesto los costes de personal subcontratado.

MANUAL DE USUARIO

No existe contenido en esta sección.

Esta página se deja deliberadamente en blanco.

BIBLIOGRAFÍA

[CINSHT0] Instituto Nacional de Seguridad e Higiene en el Trabajo, Corporate Web Site, 2012, http://www.insht.es/portal/site/Insht/

[CINSHT6] Instituto Nacional de Seguridad e Higiene en el Trabajo (INSHT), Enciclopedia de Salud y Seguridad en el Trabajo - El cuerpo humano - Sistema musculoesquelético, 2012, http://www.insht.es/InshtWeb/Contenidos/Documentacion/TextosOnline/EnciclopediaOIT/tomo1/6.pdf

[CINSHT29] Instituto Nacional de Seguridad e Higiene en el Trabajo (INSHT), Enciclopedia de Salud y Seguridad en el Trabajo - Ergonomía - Herramientas y enfoques, 2012, http://www.insht.es/InshtWeb/Contenidos/Documentacion/TextosOnline/EnciclopediaOIT/tomo1/29.pdf

[CESPERGO] Asociación Española de Ergonomía, Corporate Web Site, 2012, http://www.ergonomos.es/

[CINTERGO] International Ergonomics Association, Corporate Web Site, 2012, http://www.iea.cc/

[KYOCE1] Kyocera International, Inc, Notes on reflective mode displays, , http://americas.kyocera.com/kicc/lcd/notes/reflective.html

[KYOCE2] Kiocera International, Inc, Notes on transmissive mode displays, , http://americas.kyocera.com/kicc/lcd/notes/transmissive.html

[KYOCE3] Kyocera International, Inc, Notes on transflective mode displays, , http://americas.kyocera.com/kicc/lcd/notes/transflective.html

[KYOCE4] Kyocera International, Inc, Notes on resistive touch panels, , http://americas.kyocera.com/kicc/lcd/notes/touchpanels.html

[CESDA] Electrostatic Discharge Association, Corporate Web Site, 2012, http://www.esda.org/

[US810G] US Deparment of Defense, TEST METHOD STANDARD MIL-STD-810G - ENVIRONMENTAL ENGINEERING CONSIDERATIONS AND LABORATORY TESTS, 2008

[UGEHUM] Georgia State University - Department of Physics & Astronomy, Humedad Relativa, 2012, http://hyperphysics.phy-astr.gsu.edu/hbasees/kinetic/relhum.html

[IECEX] International Electrotechnical Commission System for Certification to Standards Relating to Equipment for use in Explosive Atmospheres, , , http://www.iecex.com

[IS60790] International Electrotechnical Commission (IEC), IEC 60079-0 International Standard – Edition 6.0 – Explosive atmospheres – Part 0: Equipment – General requirements, 2011, http://www.iec.ch

[IS0079101] International Electrotechnical Commission (IEC), IEC 60079-10-1 INTERNATIONAL STANDARD – Edition 1.0 – Explosive atmospheres –

Part 10-1: Classification of areas – Explosive gas atmospheres, 2008, http://www.iec.ch

[IS0079102] International Electrotechnical Commission (IEC), IEC 60079-10-2 International Standard – Edition 1.0 – Explosive atmospheres – Part 10-2: Classification of areas – Combustible dust atmospheres, 2009, http://www.iec.ch

[IS6007911] International Electrotechnical Commission (IEC), IEC 60079-11 International Standard – Edition 6.0 – Explosive atmospheres – Part 11: Equipment protection by intrinsic safety "i", 2006, http://www.iec.ch

[IS007925] International Electrotechnical Commission (IEC), IEC 60079-25 International Standard – Edition 2.0 – Explosive atmospheres – Part 25: Intrinsically safe electrical systems, 2010, http://www.iec.ch

[IS949CE] Parlamento Europeo y Consejo de la Unión Europea, Directiva 94/9/CE Relativa a la aproximación de las legislaciones de los Estados miembros sobre los aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas, 1994, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1994:100:0001:0029:ES:PDF

[ISATEX1] European Commissión - Enterprise and Industry, ATEX Guidelines, 2009, http://ec.europa.eu/enterprise/sectors/mechanical/files/atex/guide/atexguidelines-may2011_en.pdf

[IS068227] International Electrotechnical Commission (IEC), ISO/IEC 60068-2-27 – International Standard – Edition 4.0 – Environmental testing – Part 2-27: Tests – Test Ea and guidance: Shock, 2008, http://www.iec.ch

[IS068231] International Electrotechnical Commission (IEC), ISO/IEC 60068-2-31 International Standard – Edition 2.0 – Environmental testing – Part 2-31: Tests – Test Ec: Rough handling shocks – primarily for equipment-type specimens, 2008, http://www.iec.ch

[IS068264] International Electrotechnical Commission (IEC), IEC 60068-2-64 - International Standard – Edition 2.0 – Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance, 2008, http://www.iec.ch

[CMCSFT1] Microsoft Corporation, Downloads, 2012, http://www.microsoft.com/es-es/download/default.aspx

[CINTERM1] Intermec Technologies, Corp, Downloads, 2012, http://www.intermec.com/support/downloads/index.aspx:

[MOTOSOL1] Motorola Solutions, Inc, Software Downloads, , http://support.symbol.com/support/product/softwaredownloads.do

[CORJAVA] Oracle, Java, , http://www.oracle.com/technetwork/java/javase/downloads/index.html

[WLSTUD] Wavelink Corporation, Wavelink Studio®, 2012, http://www.wavelink.com/p/mobile-device-application-development

[CWLSTERM] Wavelink Corporation, Wavelink Supported Terminals, 2012, http://www.wavelink.com/p/mobile-device-application-development_supported-devices

[CWLSTDOW] Wavelink Corporation, Wavelink Downloads, 2012, http://www.wavelink.com/Download-Studio_mobile-device-application-development-Software

[CAIM] Association for Automatic Identification and Mobility, Corporate Web Site, , http://www.aimglobal.org/

[CGS1GLOB] AG1 AISBL, Corporate Web Site, , http://www.gs1.org/

[RIBCGEN] Raco Industries, LLC, On-Line Barcode Generator, 2012, http://www.racoindustries.com/barcodegenerator/

[CISBN] International Standard Book Number Agency, Corporate Web Site, 2012, http://www.isbn.org/standards/home/index.asp

[IATA2D] International Air Transport Association, Simplifying the BusinessBar Coded Boarding PassImplementation Guide, 2009, http://www.iata.org/whatwedo/stb/Documents/BCBP_Implementation_Guide v4_Jun2009.pdf

[IS15438] International Electrotechnical Commission (IEC), International Standard ISO/IEC 15438 - Second Edition - Information technology — Automatic identification and data capture techniques — PDF417 bar code symbology specification, 2006, http://www.iec.ch

[CSIC2D] F.J. Espinosa García, L. Hernández Encinas y A. Martín del Rey, Codicacion de informacion mediante codigos bidimensionales, 2012, http://digital.csic.es/bitstream/10261/21259/1/Codbidimens.pdf

[IS78112] International Electrotechnical Commission, International Standard - ISO/IEC 7811-2 - Third edition - Identification cards — Recording technique — Part 2: Magnetic stripe — Low coercivity, 2001, http://webstore.iec.ch/preview/info_isoiec7811-1%7Bed3.0%7Den.pdf

[IS78116] International Electrotechnical Commission, International Standard ISO/IEC 7811-6 - Third edition - Identification cards — Recording technique — Part 6: Magnetic stripe — High coercivity, 2008, http://webstore.iec.ch/preview/info_isoiec7811-6%7Bed3.0%7Den.pdf

[IS78117] International Electrotechnical Commission, International Standard ISO/IEC 7811-7 - First edition - Identification cards — Recording technique — Part 7: Magnetic stripe — High coercivity, high density, 2004, http://webstore.iec.ch/preview/info_isoiec7811-7%7Bed1.0%7Den.pdf

[IS78118] International Electrotechnical Commission, International Standard ISO/IEC 7811-8 - First edition - Identification cards — Recording technique — Part 8: Magnetic stripe — Coercivity of 51,7 kA/m (650 Oe), 2008, http://webstore.iec.ch/preview/info_isoiec7811-8%7Bed1.0%7Den.pdf

[IS7813] International Electrotechnical Commission, International Standard ISO/IEC 7813 - Sixth edition - Information technology — Identification cards — Financial transaction cards, 2006, http://webstore.iec.ch/preview/info_isoiec7813%7Bed6.0%7Den.pdf

[IS4909] International Electrotechnical Commission, International Standard ISO/IEC 4909 - First edition - Identification cards — Financial transaction cards — Magnetic stripe data content for track 3, 2006, http://webstore.iec.ch/preview/info_isoiec4909%7Bed1.0%7Den.pdf

[CIATA] International Air Transport Association (IATA), Corporate Web Site,

2012, http://www.iata.org/Pages/default.aspx

[CABA] American Bankers Association, Corporate Web Site, 2012, http://www.aba.com/Pages/default.aspx

[IS78161] International Electrotechnical Commission (IEC), International Standard ISO/IEC 7816-1 – Second edition – Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics, 2011, http://www.iec.ch

[BSTALLI1] William Stallings, Cryptography and Network Security - Principles and Practice, 2011, Prentice Hall, 17, 521-565

[BKUROSS1] James F. Kurose and Keith W. Ross, Computer Networking – A top-Down approach, 2010, Pearson Education, 8, 687-769

[IS8021X] Institute of Electrical and Electronics Engineers (IEEE), 802.1X Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control, 2010, http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

[ISEAPTLS] Internet Engineering Task Force (IETF), RFC 5216 - The EAP-TLS Authentication Protocol, 2008, http://tools.ietf.org/html/rfc5216

[ISPEAP4] Internet Engineering Tark Force (IETF), Internet Draft - Microsoft's PEAP version 0 (Implementation in Windows XP SP1), 2002,

[ISPEAP2] Internet Engineering Task Force (IETF), Internet Draft - Protected EAP Protocol (PEAP) Version 2, 2004, http://tools.ietf.org/id/draft-josefsson-pppext-eap-tls-eap-10.txt

[CISCOCCX] Cisco Systems, Inc., Cisco Compatible Extensions (CCX, , http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html

[USFIPS2] National Institute of Standards and Technology (NIST), FIPS PUB 140-2: FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION - SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, 2002, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[ISTDIP] International Electrotechnical Commission (IEC), International Standard IEC-60529 - Edition 2.1 - Degrees of protection provided by enclosures (IP Code), 2001, http://webstore.iec.ch/webstore/webstore.nsf/mysearchajax?Openform&key=60529&sorting=&start=1&onglet=1