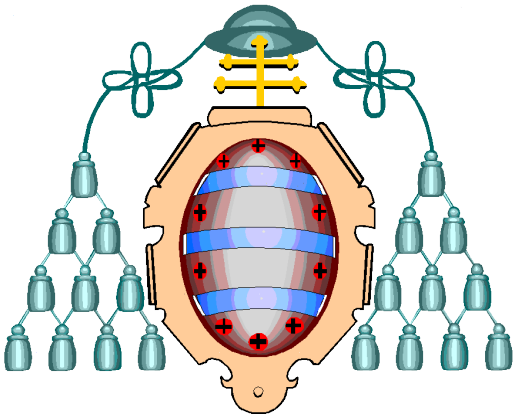


UNIVERSIDAD DE OVIEDO

DEPARTAMENTO DE ADMINISTRACIÓN DE EMPRESAS

“Aplicaciones de las tecnologías de autoidentificación de personas”

TESIS DOCTORAL

DIRIGIDA POR:

DR. D. DAVID DE LA FUENTE

PRESENTADA POR:

D. BERNARDO MONTES LATORRE

GIJÓN, 2011

A mi amigo David, que tan repentina e injustamente nos dejó justo al terminar tan brillantemente su tesis doctoral dejándonos para siempre el recuerdo de la grandeza de su persona y el don de su amistad.

A María y a los “peques”: María, Carmen, Lola y Rodrigo que tantas alegrías me dan y que tan bien consiguen compensar con la intensidad de su cariño la brevedad del tiempo que puedo estar junto a ellos.

A mis padres, por su paciencia, su comprensión y su constante desvelo por apoyarme y ayudarme siempre.

Agradecimientos

Al Director del presente trabajo, Dr. D. David de la Fuente, por su ayuda para poder compaginar el trabajo investigador con las obligaciones profesionales y, sobre todo, por su capacidad de infundir el ánimo y perseverancia necesarios para avanzar.

A Dña. Sandra García Álvarez, Dña. Yaiza García García y D. Sergio Fernández Casado: las personas que me confiaron su tiempo, su esfuerzo y su ilusión en la realización de sus proyectos fin de carrera y que tanto me han aportado para el desarrollo de este trabajo.

Resumen

La capacidad de identificar personas para permitir su acceso a espacios protegidos o a documentación ha sido a lo largo de la historia objeto de diferentes enfoques acordes con los recursos disponibles en cada momento: desde el enterramiento de objetos valiosos en ubicaciones secretas, la utilización de guardianes para el control del acceso a salas, la codificación de documentos para que sólo pudieran ser interpretados por personas previamente iniciadas o autorizadas hasta la utilización de cerraduras y llaves de los más variados tipos.

Las técnicas de autoidentificación (aquellas que permiten identificar objetos y personas sin intervención humana) han sufrido una gran evolución en los últimos años y están cambiando en gran medida la forma en que satisfacemos la necesidad de proteger nuestros bienes y nuestro conocimiento. El imparable desarrollo de la tecnología de identificación por radiofrecuencia (RFID) y de las tecnologías de identificación biométrica hacen posibles a día de hoy aplicaciones que recientemente no lo eran.

El desarrollo de estas tecnologías no está agotado. Tanto en grado de implantación como en diferentes aplicaciones existe aún un largo camino por recorrer. El objetivo de este trabajo ha sido analizar las posibilidades reales de utilización de estas tecnologías en diferentes aplicaciones de identificación de personas y su desarrollo esperable en el futuro.

El trabajo se ha desarrollado en tres grandes fases: primero se ha estudiado el estado el arte y se ha comprendido su evolución y las causas de ésta. En segundo lugar se han analizado posibles aplicaciones, contrastando algunas mediante encuestas, y se han desarrollado algunos prototipos para comprobar la viabilidad real de las tecnologías, sus ventajas e inconvenientes, para permitir, a partir de los dos pasos anteriores, establecer conclusiones.

Summary

The ability to allow or deny access to selected individuals to protected areas or sensible documentation has been an ongoing concern for humankind since our first times on earth. This was accomplished through the burying or caching of valuable objects since the beginning of times. Later on guards were used and we even developed the ability to encode information in a way that only authorized people that had been initiated or had a key for decoding could access the knowledge contained, then we came up with locks and keys and nowadays we have auto-id technologies (the technologies that allow identification of objects and people with no need of constant human intervention).

Auto-id technologies have gone through constant and fast evolution, especially in recent years. They have are changing how we satisfy our need to protect our goods and information. The continuous development of the RFID (Radio Frequency Identification) technologies and the biometric identification technologies are making some applications a reality that was not possible yesterday.

The development of these technologies is not drained. Both in the number of implementations and in the new application possibilities there is a long way to go. The objective of this work has been to analyze the real possibilities of using these technologies in people identification and the expectable future development of new technologies and applications.

This work has been developed in three phases: first state of the art and its evolution path and triggers were analyzed and understood. Second different applications have been analyzed, some of them checked through surveys, and some prototypes have been developed to understand the actual feasibility of the solutions, their pros and cons. Finally, from the results and understanding gained through these previous steps, conclusions were drawn.

Contenido

Resumen 7

Summary 8

Índices de tablas e ilustraciones 10

Índice de ilustraciones 10

Índice de tablas 13

1 Introducción 15

2 Análisis del estado del arte 22

2.1 Introducción a los sistemas de autoidentificación 23

2.2 Problemática de la tecnología RFID 98

2.3 Identificación biométrica 129

2.4 Sistemas de auto-identificación aplicados a personas 148

2.5 Experiencias en aplicación de las tecnologías de auto-identificación al control de personas 159

3 Análisis del interés de las posibles aplicaciones al campo docente. 204

3.1 Realización de la encuesta 205

3.2 Descripción de las aplicaciones de sistemas de auto-identificación en centros docentes 249

4 Trabajo de desarrollo realizado 270

4.1 Descripción de prototipos realizados 270

5 Conclusiones y extensiones 291

Bibliografía 296

ANEXOS 302

Índices de tablas e ilustraciones

Índice de ilustraciones

Ilustración 1.-Código de barras 25
Ilustración 2.-Se necesita tener visión directa entre el lector y el código de barras. 27
Ilustración 3.-Estructura básica código de barras lineal: 1. Quite Zone; 2.-Carácter de inicio (derecha)/ terminación (izquierda); 3.-Carácter de datos; 4.-Checksum o suma de verificación 30
Ilustración 4.-Ejemplo de código de barras bidimensional 30
Ilustración 5.-Matrices de símbolos 31
Ilustración 6.-Ejemplo de código de barras U.P.C. 32
Ilustración 7.-Código UPC-E 33
Ilustración 8.-Código EAN-13 y EAN-8 respectivamente 33
Ilustración 9.-Código 39 34
Ilustración 10.-Code 93 35
Ilustración 11.-Código 128 35
Ilustración 12.-. Entrelazado 2 de 5 36
Ilustración 13.-Codabar 36
Ilustración 14.-Código Posnet 37
Ilustración 15.-PDF417 39
Ilustración 16.-MaxiCode 39
Ilustración 17.-Cuatro matrices integran este DataMatrix 40
Ilustración 18.-Los tres cuadrados de las esquinas permiten detectar al lector la posición del código QR 41
Ilustración 19.-Dirección lectura del código 44
Ilustración 20.-Lector lápiz; Lector por ranura; Lector láser; Lector omnidireccional ... 44
Ilustración 21.-Botones de memoria de contacto 45
Ilustración 22.-Diferencia entre el código EAN-13 y el código EPC 54
Ilustración 23.-Esquema backscatter para tags RFID 63
Ilustración 24.-Etiqueta activa 64
Ilustración 25.-Campo cercano y lejano respectivamente 71
Ilustración 26.-Lector RFID portátil (PDA UHF GUN) 72
Ilustración 27.-Impresora RFID 78
Ilustración 28.-Frecuencias utilizadas en cada una de las bandas por los diferentes continentes o país 82
Ilustración 29.-Logotipo de EPCglobal. 87
Ilustración 30.-Interferencia mutua 102
Ilustración 31.-Página en contra de la implantación del sistema RFID en la empresa textil Benetton. 126

Ilustración 32.-Versión original y española del libro publicado en 2006 por la asociación CASPIAN 126
Ilustración 33.-Aspecto macroscópico de un microchip asociado a tumor. El chip (flecha) se ha retirado de la cavidad donde residía in-situ (punta de flecha). "*Experimental and Toxicologic Pathology52 (2001); 483-491*" 128
Ilustración 34.-Análisis del iris como identificación biométrica 129
Ilustración 35.-Patrones de huellas digitales 133
Ilustración 36.-Puntos característicos 133
Ilustración 37.-Modelo de dos dimensiones generado por el software 134
Ilustración 38.-Funcionario fichando en los juzgados de Oviedo. Foto: Armando Álvarez 136
Ilustración 39.-Reconocimiento mediante iris 137
Ilustración 40.- Iriscode mostrado gráficamente junto al ojo correspondiente, de la web de John Daugman, Universidad de Cambridge. (Boulat, 2002) 138
Ilustración 41.- Fotografía de John Daugman en su trabajo para National Geographic con objeto de la localización de la niña afgana de la portada de la revista en 1985. .. 139
Ilustración 42.-Lector biométrico según forma de la mano 140
Ilustración 43.-Fondo del ojo 141
Ilustración 44.-Identificación mediante voz 142
Ilustración 45.-Reconocimiento facial 143
Ilustración 46.-Imagen obtenida mediante el procedimiento 145
Ilustración 47.-Fotografía de la palma de la mano, imagen de rayos infrarrojos, patrón de venas y sensor respectivamente 146
Ilustración 48.-Tamaño de la tarjeta magnética 150
Ilustración 49.-Tarjetas de banda magnética 151
Ilustración 50.-Distintos tipos de receptáculos para los chips 153
Ilustración 51.-Tarjeta con dispositivo RFID 154
Ilustración 52.-Tarjeta ciudadana de Gijón 155
Ilustración 53.-Logotipo de etiquetas RFID implantables en humanos 160
Ilustración 54.- Logotipo de emrpesa Positive ID 160
Ilustración 55.- Chip implantable 161
Ilustración 56.-Esquema de funcionamiento de un RFID implantable 162
Ilustración 57.-Oran Barber/Beth Israel Deaconess Medical Center 162
Ilustración 58.-La inserción se realiza mediante jeringuilla 163
Ilustración 59.-Implante RFID en humano 164
Ilustración 60.-Entrada de la discoteca Baja Beach Club 166
Ilustración 61.-Uso de una tarjeta identificadora con RFID 170
Ilustración 62.-El sistema RFID puede ser muy útil para el sistema penitenciario. 171
Ilustración 63.-Gestión de activos de alto valo 173
Ilustración 64.-Monitoreo de pacientes usando tecnología RFID 175

Ilustración 65.-Lectura del chip RFID en una pulsera que posee el paciente..... 177
Ilustración 66.-Entrada del Hospital de Cabueñes (Gijón)..... 179
Ilustración 67.-Simbolo de un pasaporte que utiliza tecnología RFID..... 181
Ilustración 68.-Símbolo RFID en un pasaporte 181
Ilustración 69.- Pasaporte de Suecia..... 182
Ilustración 70.-Sistema YourDay permite grabar tus movimientos en el parque temático 183
Ilustración 71.-Los transponder ChampionChips..... 184
Ilustración 72.-Empleado insertando tag en la carpeta del documento. 187
Ilustración 73.-Insignia de un colegio con chip RFID en su interior..... 187
Ilustración 74.-Estudiante acerca la tarjeta RFID identificativa al lector 189
Ilustración 75.- "Kiosk" de la empresa IntuiteK 189
Ilustración 76.-Alumna de Brittan School con su tarjeta identificativa RFID 192
Ilustración 77.- Estudiantes de la escuela Rikkyo Elementary a la entrada del centro.193
Ilustración 78.-Funcionamiento del sistema "fob" 198
Ilustración 79.-Sistema "fob" 199
Ilustración 80.-Esquema de funcionamiento del sistema 200
Ilustración 81.-Sistema BioGlitz 202
Ilustración 82.- Punto de acreditación en congreso 271
Ilustración 83.- Pantalla de bienvenida al paso de dos visitantes. 272
Ilustración 84.- Punto de control oculto en columnas promocionales. 273
Ilustración 85.- Visualización en tiempo real de la situación de las personas en el edificio..... 274
Ilustración 86.- Cámara de reconocimiento de iris en primer plano sobre la columna y antenas RFID ocultas en falso techo. 275
Ilustración 87.- Varios equipos de protección individual 279
Ilustración 88.- Identificador RFID para su remachado sobre metal. 281
Ilustración 89.- Ejemplo de lista de comprobación de extintores sobre PDA 282
Ilustración 90.- Visualización web de una detección georeferenciada. 283
Ilustración 91.- PDA industrial con conectividad GPRS, cámara y wifi corriendo aplicación de O2E para la inspección en campo de la actividad del Oso pardo cantábrico. 284
Ilustración 92.- Aplicación para control de presencia en movilidad. 285
Ilustración 93.- Identificación en terminal biométrico facial en aplicación de control de asistencia a centros docentes. 287
Ilustración 94.- Entorno de usuario de la solución para control de asistencia en centros docentes..... 288
Ilustración 95.- Visión en pantalla de un informe y ventana de exportación. 289

Índice de tablas

Tabla 1.-Comparativa general entre las distintas tecnologías de Auto-ID 57
Tabla 2.-Tabla resumen de las principales características del sistema RFID frente al código de barras 59
Tabla 3.-Principales características de los modos de propagación 68
Tabla 4.- Protocolos EPC 88
Tabla 5.-Fiabilidad de lectura Vs Distancia antena 99
Tabla 6.-Grado de atenuación según el tipo de materia 108
Tabla 7.-Efecto de los diferentes materiales sobre la señal de RF 109
Tabla 8.-Resumen de los centros docentes analizados. 188
Tabla 9.-Tipos de tarjeta magnética 151
Tabla 10.-Resumen de características de los diferentes sistemas biométricos 130
Tabla 11.-Tabla comparativa entre las diferentes tecnologías de auto-identificación personal 158
Tabla 8.1.-Población por municipios. Fuente: Instituto Nacional de Estadística (2009) 208
Tabla 8.2. Número de centros según el tipo. 214
Tabla 8.3.- Número de centros distribuidos entre los 3 municipios 214
Tabla 8.4. Nivel de confianza 215
Tabla 8.5. Datos de la muestra 216
Tabla 8.6.- Número de centros en cada municipio 217
Tabla 8.7.- Número de centros encuestados en cada municipio 217
Tabla 8.8.- Resumen de características de la muestra 218
Tabla 8.9. Listado de centros encuestados 220
Tabla 8.10.- Escala de puntuación 222
Tabla 8.11.- Puntuación dependiendo de la calificación otorgada por los centros 227
Tabla 8.12.- Resumen de la nota media y desviación típica para las diferentes características del sistema en función del tipo de centro. 238
Tabla 8.13.- Resumen de las ventajas y desventajas de utilizar distinta tecnología para realizar la auto-identificación personal. 254
Tabla 8.14.- Comparativa de costes 254
Tabla 8.15. Coste de los elementos caso 1. Fuente: Oxígeno Empresarial 266
Tabla 8.16.- Costes de elementos caso 2. Fuente Oxígeno Empresarial 266
Tabla 8.17.-Coste elementos caso3. Fuente: Oxígeno Empresarial 267
Tabla 8.18.- Costes caso 4. Fuente: Oxígeno Empresarial 268
Tabla 8.19.- Costes caso 5.- Fuente Oxígeno Empresarial 269

1 Introducción

No cabe duda, de que los sistemas de auto-identificación (códigos de barras, identificación por radiofrecuencia, identificación biométrica, etc.) presentan numerosas ventajas a la hora de etiquetar productos, herramientas y máquinas cambiando para siempre la forma en que operan nuestras empresas. Este trabajo ahonda en las posibilidades de identificación automática de personas y sus aplicaciones: se analizan las aplicaciones de este tipo de sistemas en campos tan diferentes como el control horario, el control de accesos, la prevención de riesgos laborales mediante la localización de personas o el control de equipos de protección individual, etc.

Las primeras aplicaciones a personas de los sistemas de autoidentificación se han dirigido a la optimización de procesos administrativos (códigos de barras en formularios, carnets de identificación en sistemas de toma de datos en planta, etc.) y en control de accesos y presencia (tarjetas de fichaje, llaves magnéticas, etc.). Su aplicación ha crecido de forma rapidísima por sus ventajas en cuanto a costes y control eficaz. En el momento actual tras la incorporación de las tecnologías RFID y con las emergentes tecnologías biométricas se han abierto nuevas posibilidades de generación de valor.

El objetivo de este trabajo ha sido analizar las posibilidades de estas tecnologías y su aplicación a partir del estado del arte actual, los resultados de la experiencia acumulada y del estudio de la posible proyección futura.

Las tecnologías de autoidentificación están sufriendo un desarrollo vertiginoso y el know-how está distribuido entre, fundamentalmente, las diferentes empresas que a nivel mundial se dedican a su explotación y desarrollo. Esto dificulta en cierta medida el trabajo investigador en este tipo de temas ya que normalmente los últimos avances y el estado del arte no quedan reflejados en artículos o ponencias hasta un tiempo después de su consecución.

A modo de ejemplo introductorio sobre la actualidad e interés práctico del objeto del estudio se describen a continuación brevemente algunos casos de utilización de estas tecnologías.

Prevención de riesgos laborales: Evacuación, localización rápida, autorización de utilización de equipos, etc.

La prevención de riesgos laborales es un pilar fundamental de la concepción actual de la gestión empresarial excelente. Cada vez en mayor medida las pequeñas y grandes empresas son conscientes de ello. Es bien conocido que las consecuencias de un accidente para una empresa son nefastas tanto económica como moralmente y, en caso de demostrarse negligencia empresarial, pueden acarrear serias consecuencias en la forma de responsabilidades penales.

Un aspecto importante y común a prácticamente todos los sistemas de prevención es la gestión de la evacuación en caso de emergencia. Se define evacuar como la acción de desalojar a los habitantes de un lugar para evitarles algún daño. La clasificación de las evacuaciones puede darse según sus características en total o parcial, vertical u horizontal, permanente o temporal, real o simulada, etc., pero su importancia radica en buscar trasladarse de un sitio eventualmente peligroso a uno más seguro.

Para que la evacuación del personal se realice de manera satisfactoria es muy conveniente disponer de una localización rápida y eficaz de la situación de todo el personal en la empresa para proceder a su traslado hacia un lugar seguro.

Esta localización instantánea de cada trabajador en la empresa debería ser fiable y en tiempo real para evitar que una información errónea cause ineficacia en labores de rescate o evacuación. Esta ubicación en tiempo real de los trabajadores puede ser proporcionada de manera eficaz a través de la utilización de métodos de identificación automática en personas, entre los que destaca el sistema RFID.

En algunos sectores esta localización se vuelve un factor clave como es el caso de la minería. Por ejemplo la compañía Wtek (Identec - www.wtek.no) ha utilizado la tecnología RFID para crear un sistema de localización diseñado para esta industria mediante el cual los trabajadores transportan en sus equipos un chip RFID mediante el cual pueden ser localizados en cada momento. Este sistema es muy útil en casos de emergencia y evacuación, cuando no sólo es necesario conocer la localización de los mineros sino también la de los equipos de rescate. Cuando una mina ha de ser explosionada, es crucial saber si todos los trabajadores están fuera.

También a efectos de evacuación de la población de sus propias viviendas debido a catástrofes naturales como huracanes, seísmos o grandes tormentas el sistema RFID ayuda a identificar y tener una localización exacta de las personas que son evacuadas y puestas a salvo. Por ejemplo la empresa Texas Instruments ha desarrollado un sistema de evacuación de emergencia basado en sistema RFID (Texas Instruments (www.ti.com)) que permite controlar a los evacuados durante los momentos del desastre natural. Cada año, el personal de rescate se ve desbordado por llamadas que preguntan por familiares que no pueden ser localizados por ello la empresa ha desarrollado el sistema Texas Special Needs Evacuation Tracking System, que se basa en códigos de barras y RFID. Cuando un evacuado sube a un autobús, se le da una pulsera especial y se escanea. La información se recopila y se combina con los datos GPS acerca de la ubicación del autobús. De esta manera, el personal de rescate tiene información en tiempo real para ofrecer a los familiares que esperan reunirse con sus seres queridos.

También es necesario para una prevención eficaz garantizar que sólo personas con la formación necesaria y con las autorizaciones que correspondan pueden utilizar ciertas máquinas o acceder a zonas peligrosas. Este control puede extenderse también a que se estén utilizando los EPIs adecuados. Estos controles resultan complicados y costosos por métodos tradicionales pero pueden ser viables mediante las técnicas de autoidentificación.

Control de accesos

En la actualidad, las exigencias empresariales demandan cada vez más, que los sistemas de acceso sean no sólo seguros y eficaces sino que permitan ser con total garantía, eficientes y cómodos para el usuario y que autoricen su utilización sólo a aquellos para los que están destinado su uso, permitiendo de esta manera aumentar el rendimiento del trabajo y garantizando la total confianza en el sistema y en los usuarios que hacen empleo de él.

Hoy en día, a la preocupación tradicional por la seguridad de los activos físicos, se añade – en muchos casos con una importancia mucho mayor – la seguridad de los datos: una fuga o pérdida de información como causa de una intrusión puede causar grandes daños y perjuicios económicos.

Los sistemas de seguridad, utilizan principalmente tres tipos de métodos para obtener la autentificación del personal:

- Algo que el individuo conozca como una contraseña o un número de identificación personal (PIN).
- Algo que el individuo posea, ya sea una tarjeta identificativa, una llave o una tarjeta de proximidad.
- Algo que el individuo "es": parámetros biométricos propios de cada persona como por ejemplo la identificación mediante huella dactilar, iris o reconocimiento mediante voz.

Como se ha dicho anteriormente las empresas necesitan aunar seguridad y rapidez en los accesos llegando a un compromiso aceptable entre el nivel de seguridad alcanzado y el coste de implantarlo, operarlo y mantenerlo. Los sistemas de identificación automática son una excelente opción.

Las tarjetas de identificación por radiofrecuencia (RFID) combinan rapidez y comodidad en su uso dado que el usuario solo debe acercar la tarjeta al lector o incluso, mediante algunas tecnologías, incluso sin sacarla del bolsillo o cartera pueda acceder al área requerida. Así pues, su utilización está ampliamente extendida en servicios cotidianos que precisan estas características como puede ser el servicio de transporte público o el servicio de pago de los peajes de las autopistas. En muchas ciudades como por ejemplo en Gijón, la tarjeta de transporte urbano posee una

etiqueta RFID que identifica al usuario y realiza el pago del viaje de una forma ágil y cómoda.

Control de presencia o asistencia

El control de asistencia al puesto de trabajo es normalmente una necesidad en muchas empresas. Realizar este control a través de métodos tradicionales es poco eficaz y poco eficiente por la facilidad de falsificación y lo laborioso del tratamiento de los datos.

Por otra parte el control de asistencia también es cada vez más un factor importante en la enseñanza universitaria. En los colegios e institutos se debe tener un control de asistencia de todo el alumnado puesto que la educación es obligatoria y la asistencia un requisito.

En algunos colegios se han implantado sistemas para el control de asistencia de los niños de manera que el colegio recoge de manera automatizada en qué lugar del colegio se encuentra cada niño y los padres pueden conocer esta información a través de un mensaje enviado a su teléfono móvil si requieren de esta información (www.cr80news.com, 2010).

En las universidades, la asistencia hasta ahora no era obligatoria si bien a partir del nuevo plan de estudios “Plan Bolonia” la asistencia se interpreta en cada vez más casos como una clave de éxito del sistema docente.

Ayuda a personas dependientes

Las personas dependientes tales como ancianos o enfermos requieren una especial atención por nuestra parte dado el grado de dependencia que tienen. La supervisión de estas personas resulta fundamental y requiere gran cantidad de esfuerzo por parte de las personas a su cargo.

En los hospitales existe gran cantidad de enfermos con diferentes necesidades que deben ser atendidos de manera eficaz y correcta. Para evitar por ejemplo que el personal sanitario deba transportar las múltiples carpetas de historiales de los pacientes un sistema automatizado de auto-identificación ofrece la posibilidad de evitar estos incómodos transportes y además permite obtener de manera sencilla los datos del paciente y así poder suministrarle la medicación correcta evitando posibles errores humanos en su administración. Además es posible saber también donde se encuentra el paciente (en la habitación, en una consulta, en quirófano, etc.)

Los enfermos mentales requieren una gran atención por parte de los cuidadores toda tecnología que complemente y facilite su trabajo (localización, registro de protocolos, administración de fármacos, incidencias, etc.) será de gran utilidad. Un centro psiquiátrico debe gestionar la estancia de sus residentes para facilitar el tránsito de personas por sus diferentes áreas. Además debe cubrir todas sus necesidades de control de los accesos de los residentes, visitantes y profesionales. Con un control automatizado se puede conocer en cada instante dónde están las personas que sufren problemas de orientación o enfermedades seniles que pueden perderse dentro de la instalación o incluso salir o escapar de ella.

Cada vez más centros hospitalarios, geriátricos, residencias y centros de día usan las nuevas tecnologías RFID con la finalidad de monitorizar la posición en entornos o áreas críticas, como las salidas. Estos sistemas de control permiten la integración directa con sistemas de busca para aviso entre enfermeras en caso de situación crítica, indicando la posición del individuo.

Desarrollo del trabajo investigador

El trabajo investigador se ha dividido en las siguientes tareas:

- Análisis del estado del arte
- Vigilancia tecnológica: análisis del estado de la técnica y su desarrollo y previsión de su evolución a corto y largo plazo.
- Concepción de nuevas posibilidades y aplicaciones que generen nuevas tendencias a partir del resultado de los dos puntos anteriores
- Desarrollo de prototipos y retroalimentación de resultados de los mismos y de aplicaciones reales.
- Redacción del documento

La actividad profesional del autor está ligada a la aplicación empresarial de las tecnologías objeto de estudio de la presente tesis lo que facilita enormemente la actualización del estado de la técnica puesto que, como es lógico por el esfuerzo de protección de los intereses comerciales y los retornos de las actividades de las empresas, los artículos científicos llevan algo de retraso con respecto a la dinámica empresarial en lo referente a nuevas tecnologías y sus aplicaciones. Además le ha permitido desarrollar y analizar prototipos de soluciones innovadores que se describen más adelante con el fin de ayudar a contrastar el potencial real.

Además, el autor ha tenido la satisfacción de co-dirigir con el Director de la tesis tres proyectos fin de carrera de alumnos de la Escuela de Ingeniería de Gijón integrados en el desarrollo del presente trabajo en las siguientes líneas de trabajo:

- ✓ Dña. Yaiza García García: *Plan de marketing para comercialización de soluciones RFID para control de seguridad.*

- ✓ Dña. Sandra García Álvarez, *Análisis de posibilidades de tecnologías de auto-identificación para la ubicación de personas y su aplicación a centros docentes.*

- ✓ D. Sergio Fernández Casado, *Aplicación de las tecnologías de identificación por radiofrecuencia (RFID) a la prevención de riesgos (control de EPIs).*

2 Análisis del estado del arte

En este capítulo se realiza un estudio del estado actual del arte de los sistemas de autoidentificación referidos principalmente a su aplicación en auto-identificación de personas, estudiando los diversos casos favorables para su utilización. Así pues, el capítulo recorre las diferentes aplicaciones, estudios y pruebas que se están realizando en este campo, desde los chips implantables en humanos y sus aplicaciones presentes y futuras, hasta el chip RFID utilizado en control de pacientes en hospitales pasando por múltiples aplicaciones que permiten vaticinar el gran impacto que tendrá esta tecnología unida a la biométrica en el futuro como auto-identificador de personas.

Se describen también aplicaciones del sistema RFID en combinación con sistemas biométricos que permiten aumentar la seguridad en la auto-identificación personal.

Se aborda con más profundidad el estado del arte actual referido a su aplicación en centros docentes, donde se realiza un estudio cronológico de las diversas incursiones que han tenido los sistemas de autoidentificación en los centros docentes para permitir la auto-identificación de los alumnos. Se analizarán sus ventajas y los problemas creados al producirse su implantación en algunos centros.

2.1 Introducción a los sistemas de autoidentificación

En este capítulo se realiza una descripción sobre los diversos sistemas de auto-identificación existentes en la actualidad, realizando una comparativa introductoria entre cada uno de ellos. Posteriormente, para ayudar a analizar y entender el potencial de la tecnología se compararán de manera exhaustiva el código de barras y el sistema RFID dada la enorme relevancia del código de barras como técnica de autoidentificación más difundida.

2.1.1 Tecnologías de auto-identificación

Las tecnologías de auto-identificación se han ido desarrollando sin cesar desde su nacimiento hasta la actualidad. Durante años el código de barras ha dominado el panorama tecnológico y hoy en día, aunque resultan "obsoletos" para muchas aplicaciones siguen y, muy probablemente seguirán durante muchos años, siendo la aplicación idónea para muchas aplicaciones (logística de detalle, etc.). Aunque la tecnología de RFID (identificación por radiofrecuencia) parece ser la sucesora natural de los códigos de barras aún hoy en día no ha conseguido suplantarlos de manera definitiva. Cada tecnología de auto-identificación tiene sus ventajas y desventajas dependiendo del fin para el que sea utilizada. Es por ello, que en la actualidad las diferentes tecnologías coexisten en diferentes aplicaciones. Las tecnologías de auto-identificación que se estudiarán de forma general en este capítulo serán el código de barras (como tecnología de referencia), las memorias de contacto y el sistema RFID profundizando más en este último por ser el que más posibilidades abre y analizando a continuación con más detalle las tecnologías aplicadas a la auto-identificación personal incluyendo los sistemas biométricos.

2.1.2 Código de barras

La tecnología del código de barras es sin lugar a dudas la referencia en auto-identificación siendo la más utilizada y extendida en la actualidad. Resulta muy familiar y cotidiano encontrarse con códigos de barras impresos en cualquier objeto, ya sean alimentos de un supermercado, ropa de tiendas o en productos farmacéuticos por ejemplo. Aunque su uso se encuentre generalizado posee una serie de limitaciones como por ejemplo la necesidad de visibilidad directa entre el código de barras y el lector que ha hecho que otras tecnologías se afiancen en algunos campos.

Ilustración 1.-Código de barras

2.1.2.1 Historia

En el Smithsonian Institution de EEUU se expone un paquete de chicles "*Wrigley*", el primer producto etiquetado con un código de barras. La primera experiencia sobre códigos de barras data de 1973, cuando en EE.UU. se aprobó el UPC (Universal Product Code), un estándar que aún continúa vigente y que se refiere a EE.UU. y Canadá. Pero no fue hasta el año siguiente, en 1974, cuando el 26 de junio se inauguró el primer punto de venta con escáner de la historia en Trou (Ohio, EE.UU.), con lo que es en esta fecha cuando el código de barras comienza a actuar. Mientras, en Europa, un grupo de especialistas con representación de unos 12 países y diversos organismos de numeración (el CGC alemán, el francés GENDOC,...) trabajaron durante 3 ó 4 años hasta alumbrar el sistema de codificación comercial EAN, compuesto por una serie de herramientas estandarizadas.

La Asociación Española de Codificación Comercial (AECOC) se constituyó en septiembre de 1977. Anteriormente, en febrero de 1977, se creó en Europa EAN International (International Article Numering), un organismo encargado de establecer la normativa de codificación de productos en el ámbito internacional, al que AECOC se incorporó inmediatamente y en el que ejerce una participación muy activa desde entonces. En España, la primera empresa que incorporó el código de barras a sus productos fue 3M. Por su parte, el primer supermercado español con escáneres lo abrió la cadena "*Mercadona*" en 1982, y para ello el distribuidor tuvo que codificar el mismo prácticamente todos los productos.

Pese a que la AECOC fue fundada en 1977, el código de barras no irrumpe en nuestro país hasta el año 1981. Si bien la evolución de asociados al AECOC durante los primeros años fue lenta, a partir de 1983 la progresión ha sido espectacular hasta alcanzar los 24.000 asociados actuales. A las empresas de alimentación y droguería, que fueron las primeras en incorporarse a AECOC, se sumaron paulatinamente otros sectores: ferretería y bricolaje, deporte, editorial, material eléctrico, farmacéutico, sanitario…

La AEOC es el organismo que asigna el código de empresa en España, primer paso para que una compañía pueda disponer de códigos de barras para sus productos una vez que se asocia a esta entidad. Este número varía entre 7 y 10 dígitos, en función de las referencias que la empresa quiera incluir. Es decir, según la estructura de esta serie secuencial, se pueden codificar hasta 100, 1.000, 10.000 ó 100.000 referencias distintas, sin que exista un límite. De todas formas, los primeros dos dígitos son siempre fijos. Se trata del prefijo nacional que, para el caso de España, es el 84. Esto no significa necesariamente que el producto sea español. Sólo indica que el responsable de su puesta en el mercado, independientemente de su nacionalidad o ubicación territorial, utiliza el código asignado por la Asociación Española de Codificación Comercial. El siguiente paso para la empresa es completar la serie de números hasta llegar a 12 dígitos. Esta segunda secuencia, junto al dígito número trece (el de control, que se obtiene mediante un algoritmo matemático) constituye el código del producto en cuestión. La última parte del proceso es la impresión de los códigos y la adhesión a los productos, para lo cual se puede acudir a un proveedor especializado.

En resumen, lo que se consigue es que cada producto tenga su propio código de barras de manera única y exclusiva. El código de control, además, elimina cualquier error de impresión al interceptar una lectura errónea.

2.1.2.2 Características

El código de barras está compuesto por una disposición de barras y espacios en paralelo que contiene información codificada. Gracias a esto, se almacena información que puede ser reunida de manera rápida con una excelente precisión. Así pues, los códigos de barras representan un método sencillo y fácil de codificar información de texto a través de las barras y espacios que pueden ser leídos por dispositivos ópticos

que envían la información del producto a un ordenador de la misma forma que si la información hubiese sido tecleada. El código de barras no contiene la información propiamente dicha del producto como por ejemplo su precio, pero si contiene la clave para acceder a un registro de una base de datos donde realmente se encuentra la información.

Una de las limitaciones más importantes del código de barras es su no capacidad de lectura simultánea dado que solamente se puede identificar un objeto de cada vez. Este hecho limita la velocidad y eficiencia en la lectura de los productos. Otra limitación importante es la baja capacidad que posee a nivel de datos dado que solo es aplicable para el almacenamiento de un código único, pero no permite por ejemplo el almacenamiento de más datos como puede ser la fecha de expedición, de caducidad, el número de lote u otra información de interés. Además una vez impreso el código de barras es imposible rescribirlo y es necesario el cambio total de la etiqueta. También puede provocar lecturas erróneas si se produce algún daño en las barras en posición vertical, como por ejemplo la eliminación de una barra vertical completa. Si se da este caso, es imposible recuperar la información. En el caso de ser un daño horizontal no influye tanto ya que el lector hace una pasada por los diferentes puntos, leyendo correctamente en cualquier ubicación que esté bien.

Ilustración 2.-Se necesita tener visión directa entre el lector y el código de barras.

Otra limitación a añadir por parte de esta tecnología es la necesidad de tener visibilidad directa entre la etiqueta y el lector. A esto se añade que si el código de barras se encuentra sucio o roto su lectura se dificulta o imposibilita. Su ciclo de vida es corto debido a que la impresión no soporta determinadas condiciones de trabajo salvo que se proteja mecánicamente.

A pesar de estas limitaciones la mayoría de las innovaciones acontecidas en el código de barras se han centrado en la captura de la información y en la transmisión de estos datos, para obtener mayor conectividad a la red y facilidad de uso. Su uso se encuentra tan extendido debido a que su coste es prácticamente despreciable en muchas aplicaciones, ya que en la mayoría de los casos es impreso sobre el producto en la misma etiqueta que posee o en una etiqueta adhesiva.

2.1.2.3 Tipos

Los códigos de barras pueden imprimirse de muchas formas. Muchos de ellos resultan familiares porque son los utilizados en la vida cotidiana. Sin embargo, existen gran cantidad de formas utilizadas por algunas industrias como pueden ser la de salud o fabricación que poseen terminologías únicas.

La existencia de varios tipos de códigos de barras, se debe a que las simbologías están diseñadas para resolver problemas específicos. De acuerdo al tipo de necesidad de identificación interna del negocio o con los requisitos que se deben cumplir para poder comerciar según las normas del mercado, se debe optar por el sistema de codificación más adecuado. Es decir, existen diferentes simbologías para las diferentes aplicaciones, y cada una de ellas tiene características propias.

La selección de la simbología dependerá del tipo de aplicación donde va a emplearse el código de barras. El tipo de carácter, numérico o alfanumérico, la longitud de los caracteres, el espacio que debe ocupar el código o la seguridad, son algunos de los que determinarán la simbología a emplear. Las principales características que definen a una simbología de código de barras son las siguientes:

- Numéricas o alfanuméricas.
- De longitud fija o de longitud variable.

- Discretas o continuas.
- Número de anchos de elementos.
- Autoverificación.
- Quiet Zone (área blanca al principio y al final de un símbolo del código de barras).

Existen diferentes tipos de códigos de barras entre los que están:

Códigos de barras lineales. Son los más utilizados en aplicaciones de Auto-ID. Están formados por una impresión de barras oscuras y claras (generalmente blancas) alternadas y de amplitud variable. El otro componente de este sistema es el lector o scanner. La estructura básica del código de barras consta de los siguientes elementos visualizados en la siguiente.

- **Módulo:** Es la unidad mínima o básica de un código. Las barras y espacios están formados por un conjunto de módulos.
- **Barra:** El elemento oscuro dentro del código. Se hace corresponder con el valor binario 1.
- **Espacio:** El elemento claro dentro del código. Se hace corresponder con el valor binario 0.
- **Carácter:** Formado por barras y espacios. Normalmente se corresponde con un carácter alfanumérico.

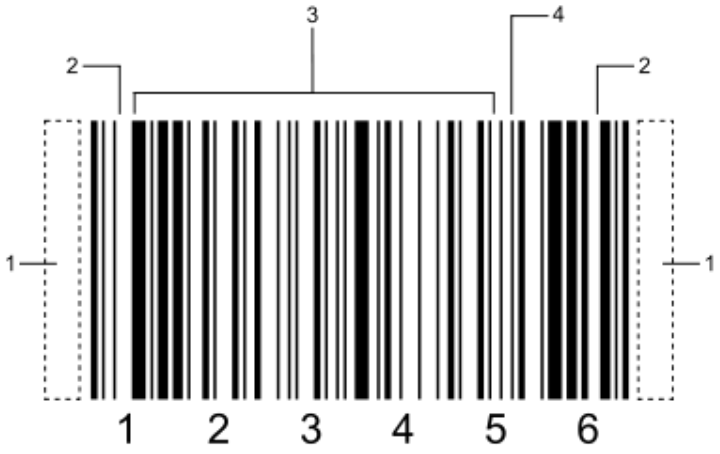


Ilustración 3.-Estructura básica código de barras lineal: 1. Quite Zone; 2.-Carácter de inicio (derecha)/ terminación (izquierda); 3.-Carácter de datos; 4.-Checksum o suma de verificación

Códigos de barras bidimensionales. Un código de barras bidimensional está formado por múltiples filas de códigos de barras de corta longitud, dispuestas de manera que asegure una correcta decodificación. Hay muchos sistemas, aunque el más utilizado es el PDF 417.

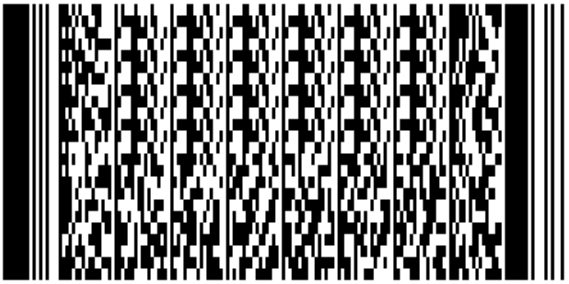


Ilustración 4.-Ejemplo de código de barras bidimensional

En este tipo de código de barras existe una redundancia mayor a la simple vertical que proporciona el código de barras lineal. Los esquemas de datos, así como la encriptación ayudan a incrementar la capacidad de los datos y su seguridad. Pero al ser una tecnología de visibilidad que contiene mayor información que el simple código lineal, la seguridad en cuanto a falsificación está en entredicho. Por ejemplo, un código PDF puede ser fotocopiado, escaneado o enviado por fax y posteriormente leído, pudiendo falsificar de manera simple y sencilla. En cuanto a su resistencia, la suciedad, cortes, etc. pueden llegar a hacer no legible el código.

Matrices de símbolos. Son el tercer tipo de códigos de barras. Están formadas por módulos discretos (típicamente círculos o cuadrados) colocados en una cuadrícula.

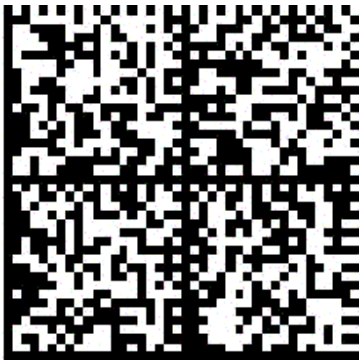


Ilustración 5.-Matrices de símbolos

Estos códigos comparten muchas características de los códigos lineales, pero tienen unos rasgos únicos que proporcionan un mejor comportamiento en ciertas aplicaciones.

En cuanto a la seguridad y capacidad de datos poseen las mismas características que sus compañeros de 2 dimensiones.

El coste resulta mayor que el de los lineales, dado que necesitan ser leídos por lectores CCD de dos dimensiones o CMOS más caros que los estándares.

2.1.2.3.1 Códigos de barras de una dimensión (lineales)

Universal Product Code (U.P.C.)

UPC es la simbología más utilizada en el comercio minorista de EE.UU., pudiendo codificar solo números.

El estándar UPC (denominado UPC-A) es un número de 12 dígitos. El primero es llamado "número del sistema". La mayoría de los productos tienen un "1" o un "7" en esta posición. Esto indica que el producto tiene un tamaño y peso determinado, y no un peso variable. Los dígitos del segundo al sexto representan el número del fabricante. Esta clave de 5 dígitos (adicionalmente al "número del sistema") es única para cada fabricante, y la asigna un organismo rector evitando códigos duplicados. Los caracteres del séptimo al onceavo son un código que el fabricante asigna a cada uno de sus productos, denominado "número del producto". El doceavo carácter es el "dígito verificador", resultando de un algoritmo que involucra a los 11 números previos. Se creó en 1973 y desde entonces se convirtió en el estándar de identificación de productos utilizado en la venta al detalle y en la industria alimentaria.

Ilustración 6.-Ejemplo de código de barras U.P.C.

Para productos pequeños se utiliza el código UPC-E

Ilustración 7.-Código UPC-E

European Article Numbering (E.A.N.)

El EAN es la versión propia del UPC europea, creado en 1976.

El sistema de codificación EAN es usado tanto en supermercados como en comercios. Es un estándar internacional, creado en Europa y de aceptación mundial. Identifica a los productos comerciales por intermedio del código de barras, indicando país-empresa-producto con una clave única internacional. Hoy en día es casi un requisito indispensable tanto para el mercado interno como para el internacional.

El EAN-13 es la versión más difundida del sistema EAN y consta de un código de 13 cifras (uno más que el UPC) en el que sus tres primeros dígitos identifican al país, los seis siguientes a la empresa productora, los tres números posteriores al artículo y, finalmente, un dígito verificador que proporciona seguridad al sistema. Este dígito extra se combina con uno o dos de los otros dígitos para representar un código de barras, indicando el origen de la mercancía. Para artículos de tamaño reducido se emplea el código EAN-8.

Ilustración 8.-Código EAN-13 y EAN-8 respectivamente

Código 39

Se desarrolló en el año 1974, debido que algunas industrias necesitaban codificar el alfabeto y los números en un código de barras. Es un estándar no utilizado en la industria alimentaria, sino que generalmente se utiliza en la identificación de inventarios y para propósitos de seguimiento. Esta simbología es actualmente la más usada para aplicaciones industriales y comerciales para uso interno ya que permite la codificación de caracteres numéricos, letras mayúsculas y algunos símbolos como “-“, “.”, “$”, “/”, “+”, “%” y " ". Se utilizan sólo dos grosores tanto para barras como para espacios, sin embargo el código 39 produce una barra relativamente larga y puede no ser adecuada si la longitud es un factor de consideración.

Ilustración 9.-Código 39

Code 93

El código de barras Code93 fue desarrollado en el año 1982 con la finalidad de complementar el estándar Code39. El Code93 es un código alfanumérico de alta densidad que soporta el juego de caracteres ASCII completo sin la ambigüedad de su antecesor, Code39. La versión estandar permite codificar 47 caracteres: A-Z, 0-9, espacio, "-", ".", " ", "$", "/", "+", "%" y cuatro caracteres especiales para soportar el código ASCII completo. El código de barras puede ser de longitud variable y necesita dos caracteres de checksum.

Ilustración 10.-Code 93

Código 128

Este código de barras fue creado en 1981 y se utiliza cuando es necesaria una selección de caracteres mayor de la que puede proporcionar el Código39. El Código 128 utiliza 4 diferentes grosores para las barras y los espacios y tiene una densidad muy alta, ocupando en promedio sólo el 60% del espacio requerido para codificar información similar en Código 39. Code 128 es un código de barras de alta densidad, usado ampliamente para la logística y paquetería. Puede codificar caracteres alfanuméricos o solo numéricos. Con este código es posible representar todos los caracteres de la tabla ASCII, incluyendo los caracteres de control.

Ilustración 11.-Código 128

Entrelazado 2 de 5

Se trata de otra simbología muy popular en la industria de envíos. El entrelazado 2 de 5 es ampliamente utilizado en la industria del almacenaje. Es una simbología compacta que puede encontrarse en las cajas de cartón corrugado que se utilizan para el envío a tiendas.

Se basa en la técnica de intercalar caracteres permitiendo un código numérico que utiliza dos grosores. El primer carácter se representa en barras, y el segundo por los espacios que se intercalan en las barras del primero. Es un código muy denso, aunque siempre debe haber una cantidad par de dígitos. La posibilidad de una lectura parcial es alta, especialmente si se utiliza un lector láser. Por lo tanto, generalmente se toman ciertas medidas de seguridad, como codificar un carácter de verificación al final del símbolo.

Ilustración 12.-. Entrelazado 2 de 5

Codabar

El Codabar aparece en 1971 y encuentra su mayor aplicación en los bancos de sangre, donde un medio de identificación y verificación automática eran indispensables.

Es una simbología de longitud variable que codifica solo números. Utiliza dos tipos de grosores para barras y espacios y su densidad es similar a la del Código 39.

Ilustración 13.-Codabar

Posnet

Tan solo utilizada por el Servicio Postal de EE.UU., esta simbología, que apareció en el año 1980, codifica los códigos postales para un procesamiento más rápido de entrega de correo.

Ilustración 14.-Código Posnet

2.1.2.3.2 Códigos de barras de dos dimensiones o matriciales

En estos códigos la información no se reduce sólo al código del artículo, sino que pueden almacenar gran cantidad datos. Los datos se codifican en altura y longitud del símbolo La principal ventaja de utilizar los códigos de 2 dimensiones es que el código contiene una gran cantidad de información que puede ser leída de manera rápida y fiable, sin necesidad de acceder a una base de datos que almacene dicha información, cosa que si sucede en los códigos de 1 dimensión.

Los códigos de 2D deben ser considerados como un complemento a la tecnología tradicional de códigos de 1D, no como su reemplazo; y las ventajas deben ser comparadas en contra del incremento en costo.

PDF 417

Conocido como un código de dos dimensiones, es una simbología de alta densidad no lineal que recuerda un rompecabezas. La diferencia entre éste y los otros tipos de código de barras, es que el PDF417 es en realidad un Portable Data File (Archivo de Información Portátil, PDF), es decir, no se requiere consultar a un archivo. Éste contiene toda la información, ya que tiene una capacidad de hasta 1800 caracteres numéricos, alfanuméricos y especiales. Un documento como este es interesante por varias razones, ya que es un espacio suficiente para incluir información como, por ejemplo: nombre, foto, historial del comportamiento y alguna otra información pertinente. Algo importante a destacar es que el tamaño del ancho de las barras y espacios repercute en un mayor espacio de impresión del código en cuestión y viceversa.

Este tipo de códigos de barras tiene diversas aplicaciones: industria, sistemas de paquetería, compañías de seguros (validación de pólizas), instituciones gubernamentales (aduanas), bancos (reemplazo de tarjetas y certificación de documentos), identificación personal, registros públicos de la propiedad, testimonios notariales, permisos de conducción, industria electrónica…etc.

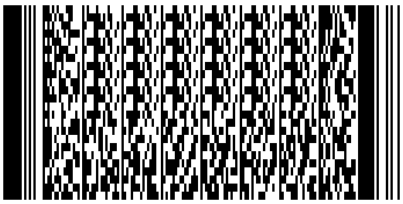


Ilustración 15.-PDF417

Maxicode

Es una simbología de alta densidad creada por UPS (United Parcel Service). En la actualidad esta simbología es de dominio público y está especificada bajo las normas ANSI (MH10.8.3M-1996). Se utiliza para el procesamiento de información a alta velocidad.

La estructura del Maxicode consiste de un array de 866 hexágonos utilizados para el almacenamiento de datos en forma binaria. Estos datos son almacenados en forma pseudo-aleatoria. Posee un blanco o bull utilizado para localizar a la etiqueta en cualquier orientación. Es posible codificar hasta 100 caracteres en un espacio de una pulgada cuadrada. Este símbolo puede ser decodificado sin importar su orientación con respecto al lector óptico.

La simbología utiliza el algoritmo de Reed-Solomon para corrección de errores. Esto permite la recuperación de la información contenida en la etiqueta con daños de hasta un 25 por ciento.

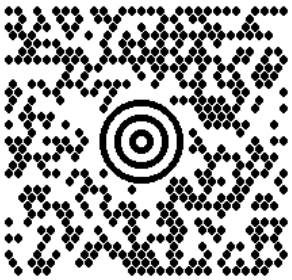


Ilustración 16.-MaxiCode

Datamatrix

Desarrollado en 1989 por International Data Matrix Inc. La versión de dominio público es la ECC 200, desarrollada también por International Data Matrix en 1995. Entre sus aplicaciones cabe destacar la codificación de la dirección postal en un símbolo bidimensional, marcado de componentes para control de calidad, etiquetado de deshechos peligrosos para control y almacenamiento a largo plazo, cupones de lotería, etc.

El símbolo Datamatrix está compuesto de módulos de celdas cuadradas definidas dentro de un perímetro marcado. Es posible codificar hasta 3116 caracteres ASCII y en la micropercusión superan los 100 caracteres. Cada símbolo consiste en zonas de datos que forman módulos cuadrados en una secuencia regular. Los símbolos más grandes contienen varios módulos y cada zona de datos está delimitada por una línea continua en 2 caras y discontinua en otras 2. Cada código individual está rodeado de una zona lisa que haga las veces de margen.

Cada código tiene un número determinado de filas y columnas. La mayoría de los códigos Datamatrix son cuadrados y van desde 10×10 hasta 144×144 puntos. De todos modos también es posible encontrar códigos Datamatrix de forma rectangular con tamaños que van desde los 8×18 a los 16×48. Todos los códigos pueden ser reconocidos desde la esquina superior derecha cuando son iluminados (binario 0).

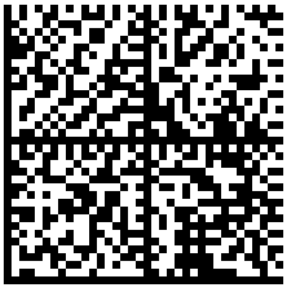


Ilustración 17.-Cuatro matrices integran este DataMatrix

Código QR

Un código QR (Quick Response Barcode) es un sistema para almacenar información en una matriz de puntos o un código de barras bidimensional creado por la compañía japonesa Denso-Wave en 1994; se caracterizan por los tres cuadrados que se encuentran en las esquinas y que permiten detectar la posición del código al lector. La sigla "QR" se derivó de la frase inglesa "Quick Response" pues el creador aspiraba a que el código permitiera que su contenido se leyera a alta velocidad. Los códigos QR son muy comunes en Japón y de hecho son el código bidimensional más popular en ese país.

Ilustración 18.-Los tres cuadrados de las esquinas permiten detectar al lector la posición del código QR.

2.1.2.4 Lectores de Códigos de Barras

Los lectores están compuestos por un "sensor" y un descodificador de código. Hay dos tipos de sensores para lectores de códigos de barras: (Mayné, 2009)

Láser (Light Amplified by Stimulated Emission of Radiation)
CCD (*Charged Coupled Device* - Dispositivo de Carga Acoplada).

Los lectores con sensor láser son más rápidos que los sensores CCD y además permiten hacer lecturas de hasta más de 10 metros de distancia. Gracias a la alta velocidad que permiten los sensores por láser, se puede "barrer" el código varias veces, para evitar errores.

Hay escáner de mano y fijos, como los que se utilizan en las cajas de los supermercados.

Tiene varios medios de conexión: USB, Puerto serie, wifi, bluetooth incluso directamente al puerto del teclado por medio de un adaptador, cuando se pasa un código de barras por el escáner es como si se hubiese escrito en el teclado el número del código de barras.

Un escáner para lectura de códigos de barras básico consiste en el escáner propiamente dicho, un decodificador y un cable que actúa como interfaz entre el decodificador y el terminal o la computadora.

La función del escáner es leer el símbolo del código de barras y proporcionar una salida eléctrica a la computadora, correspondiente a las barras y espacios del código de barras. Sin embargo, es el decodificador el que reconoce la simbología del código de barras, analiza el contenido del código de barras leído y transmite dichos datos a la computadora en un formato de datos tradicional.

Un escáner puede tener el decodificador incorporado en el mango o puede tratarse de un escáner sin decodificador que requiere una caja separada, llamada interfaz o emulador. Los escáneres sin decodificador también se utilizan cuando se establecen conexiones con escáneres portátiles tipo "batch" (por lotes) y el proceso de decodificación se realiza mediante el Terminal propiamente dicho.

Los lectores con sensores CCD se basan en tomar una imagen de la barra, con un conjunto de LEDs iluminan la barra y la luz reflejada carga eléctricamente el sensor, la distancia máxima de lectura es de 15 cm. Tanto el lector láser como el lector CCD permiten leer el código del derecho como del revés, ya que muchas veces no se puede dar la vuelta al código por estar pegado a una gran caja.

Modo de lectura

Los códigos de barras se leen pasando un pequeño punto de luz sobre el símbolo del código de barras impreso. Aunque sólo se vea una fina línea roja emitida desde el escáner láser, lo que sucede es que las barras oscuras absorben la fuente de luz del escáner y la misma se refleja en los espacios luminosos. Un dispositivo del scanner toma la luz reflejada y la convierte en una señal eléctrica.

El láser del escáner (fuente de luz) comienza a leer el código de barras en un espacio blanco (la zona fija) antes de la primera barra y continúa pasando hasta la última línea, para finalizar en el espacio blanco que sigue a ésta. Debido a que el código no se puede leer si se pasa el scanner fuera de la zona del símbolo, las alturas de las barras se eligen de manera tal de permitir que la zona de lectura se mantenga dentro del área del código de barras. Mientras más larga sea la información a codificar, más largo será el código de barras necesario. A medida que la longitud se incrementa, también lo hace la altura de las barras y los espacios a leer.

En la figura que sigue se muestra la dirección de lectura del código y la señal eléctrica entregada por el sensor.

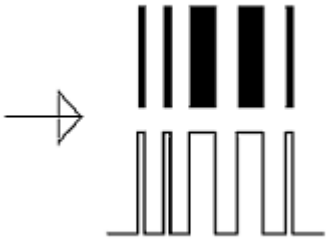


Ilustración 19.-Dirección lectura del código

Tipos de lectores de Códigos de Barras

Lectores manuales CCD (hasta 30 cm).
Lectores manuales láser (hasta 10 m).
Lectores láser omnidireccional.
Lectores láser automáticos (industriales).

Ilustración 20.-Lector lápiz; Lector por ranura; Lector láser; Lector omnidireccional

2.1.3 Botones de memoria de contacto

Los botones de memoria de contacto son un tipo de tecnología de Auto-ID que requiere contacto físico con el botón para poder leer los datos contenidos en la etiqueta. Este tipo de tecnología no ha tenido una aceptación muy extendida en comparación con la inversión que es necesario realizar para su implantación y el desarrollo que ha presentado por dicha tecnología Una de las posibles causas de esta poca expansión de los botones de memoria, puede ser debida a la falta de estándares sobre esta tecnología.

Ilustración 21.-Botones de memoria de contacto

Entre las características más importantes de este sistema destacan que los botones de memoria son aptos para ser escritos y leídos tantas veces como sea necesario, son robustos, soportan entornos hostiles como los que se dan en ambientes industriales donde pueden encontrarse vibraciones o ambientes sucios. También es importante destacar que los datos incluidos en la memoria se pueden cifrar como medida de seguridad y la capacidad de almacenamiento puede alcanzar los 8 MB de información ().

Por otra parte, las memorias de contacto presentan limitaciones, como puede ser que la distancia de lectura es nula dado que se necesita el contacto físico entre el botón y la etiqueta. Este contacto limita en parte la eficiencia de la lectura puesto que una obstrucción del botón puede provocar el error en la lectura. El número de unidades leídas simultáneamente es al igual que los códigos de barras de uno al mismo tiempo.

2.1.4 Identificación por radiofrecuencia (RFID)

2.1.4.1 ¿Qué es RFID?

Las siglas RFID significan Identificación por Radiofrecuencia. Se trata de un sistema de almacenamiento y recuperación de datos inalámbrico. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto o persona (similar a un número de serie único) mediante ondas de radio.

Un sistema RFID consta principalmente de tres componentes, un lector de RFID, un tag RFID y un subsistema de procesamiento de datos denominado middleware.

El lector se compone de una antena, un transceptor y un decodificador. Cuando el lector capta una señal de un tag, envía señales y extrae la información requerida pasándola al subsistema de procesamiento de datos. Si la etiqueta es pasiva, el lector puede transmitir energía para poder leerla.

El tag RFID está compuesto por una antena, un transductor y un chip. A través de la antena se transmite la información de identificación de la etiqueta. El chip posee la capacidad de almacenar el número de identificación y en algunos casos datos adicionales.

2.1.4.2 Historia del RFID

RFID o Identificación por radio frecuencia es una tecnología que nació aproximadamente hace 50 años en el ámbito militar.

Si se remonta a los inicios de la radiofrecuencia, en 1864 James Clerk Maxwell predijo la existencia de ondas electromagnéticas y fue Heinrich Hertz quien en 1888 demostraría la existencia de ondas electromagnéticas mediante la construcción de un aparato que producía y detectaba ondas en la región UHF.

Pero el desarrollo de la tecnología de identificación por radiofrecuencia no surgiría hasta la Segunda Guerra Mundial cuando los alemanes, americanos, japoneses y británicos utilizaban el radar descubierto en 1935 para localizar los aviones que se aproximaban desde kilómetros de distancia. El radar poseía un gran inconveniente y

era la imposibilidad de identificar qué aviones eran enemigos o por el contrario pertenecían al escuadrón y regresaban después de realizar una misión.

Los alemanes descubrieron que si los pilotos volteaban los aviones al regresar a la base, la señal que retornaba reflectada se modificaba por lo que permitía diferenciar los aviones alemanes de los aliados. Este sistema pude considerarse como el primer sistema RFID pasivo.

Los británicos por su parte, bajo las órdenes del ingeniero británico Watson, desarrollaron el primer identificador activo. El sistema consistía en instalar una antena en el fuselaje de los aviones aliados de manera que respondieran correctamente a una señal de interrogación que se les enviaba, y de este modo podrían distinguir entre un avión 'amigo' de un avión 'enemigo'. Las siglas IFF hacen referencia a Identify: Friend or Foe, lo cual significa Identificación: Amigo o Enemigo. Aunque estos sistemas sirvieron de gran ayuda durante la Segunda Guerra Mundial no ofrecían cobertura a altas velocidades ni para el tráfico denso de aviones. No obstante, a pesar de este hecho, los sistemas actuales de control de avión están basados en este sistema.

Los avances en el radar y en los sistemas de comunicaciones de radiofrecuencia continuaron durante los años 50 y 60. Científicos de EE.UU., Europa y Japón presentaron informes en los que explicaban como la energía de radiofrecuencia podía ser utilizada para la identificación de objetos remotos. Las empresas empezaron a comercializar sistemas antirrobo que utilizaban ondas de radio para diferenciar si un artículo había sido o no pagado. Las etiquetas de vigilancia electrónica de artículos, que hoy en día siguen siendo utilizadas, constan de 1bit. El bit puede estar en estado on/off. Si una persona paga por el artículo, el bit se pasa al estado off, y la persona puede salir de la tienda. Pero si la persona no paga e intenta salir de la tienda, los lectores de la tienda detectan la etiqueta y se activa la alarma.

En 1977 el gobierno de Estados Unidos montó un sistema de radiofrecuencia para el manejo de puertas en las centrales nucleares, que se abrían al paso de los camiones que se encontraban equipados con una antena. En este mismo año, los laboratorios científicos de Los Álamos en Estados Unidos, transfirieron la tecnología RFID desarrollada por las agencias gubernamentales y el ejército al uso público. Empezaron a desarrollarse las primeras aplicaciones comerciales como la identificación de vagones de tren, los peajes automáticos o los sistemas control de acceso sin llave. Se desarrolló el control del ganado que había sido vacunado insertando bajo la piel del animal una etiqueta RFID pasiva que informaba si el animal había sido vacunado o no.

A principios de la década de los 90 la empresa Wal−Mart fue la gran impulsora de la tecnología RFID. Utilizando recursos de radiofrecuencia, se pretendía obtener una auto−identificación de cualquiera de sus productos. Con el estándar inicial, esta tarea era imposible dada su baja velocidad de transferencia. De ahí que la evolución y mejora del estándar corrija notablemente estos puntos. El chip RFID ha pasado de ser del tamaño de una tarjeta de crédito, a ser menor a un sello postal en ocasiones.

Sus investigaciones fueron rápidamente atractivas para otras empresas, lo que en 1999 llevó a la formación del Auto−ID Center (Automatic IDentification) partiendo de un consorcio de empresas y científicos. La idea principal era de formar una red de productos (Internet of Objects) que hoy en día se ha generalizado a escala mundial, permitiéndose así la posibilidad de conocer si el producto está en la cadena de producción, en algún contenedor de transporte, o si está ya por ejemplo en venta.

En Europa, el proyecto lanzado en 2005 por Correos de España, Q-RFID, liderado por AIDA Centre SL, ha contribuido a incorporar las últimas tecnologías de control por radiofrecuencia para permitir la trazabilidad de la correspondencia a lo largo de todo el proceso postal. QRFID ha resultado uno de los más importantes proyectos de RFID de Europa, suponiendo una gran contribución al desarrollo e implantación de la tecnología. Aunque el proyecto ha finalizado en 2007, el éxito alcanzado garantiza la continuidad del mismo.

Como ya ha ocurrido y seguirá ocurriendo, distintos organismos se han lanzado en la creación de sus propios estándares, de forma que hoy en día es difícil pensar en RFID como un único estándar, a pesar de que cada vez se acercan más las posturas hacia la creación de un estándar mundial: El EPCGlobal Gen2. Los diferentes estándares serán descritos en apartados posteriores.

A través de estos años de desarrollo e investigación desde su inicio hasta la actualidad el sistema RFID a alcanzado un desarrollo tanto en tamaño como en coste que permite ser utilizado en múltiples aplicaciones y su uso se ha generalizado a cualquier empresa que quiera utilizarlo.

En la actualidad se está comenzando a implementar el sistema RFID junto con sistemas biométricos para mejorar la seguridad de las aplicaciones y conseguir por otra parte comodidad y facilidad de uso por parte del usuario.

2.1.4.2.1 Primeras patentes del sistema RFID

Mario W. Cardullo proclama haber recibido la primera patente americana de un tag RFID con memoria reescribible el 23 de enero de 1973. Ese mismo año, Charles Walton, un empresario californiano, recibió la patente de un transponder pasivo utilizado para abrir una puerta sin necesidad de llave. Un transponder incrustado en una tarjeta enviaba una señal a un lector situado cerca de la puerta. Cuando el lector detectaba que el número de identificación almacenado en el tag RFID era válido, éste abría la puerta. Walton licenció la tecnología a Schlage, un fabricante de cierres, y a otras empresas. (Sabater Suau)

El Gobierno de EE.UU. también trabajó en sistemas RFID. En los años 70, el Departamento de Energía encargó a Los Álamos National Laboratory el desarrollo de un sistema para la traza de materiales nucleares. Un grupo de científicos resolvió el problema instalando transponders en los camiones y lectores en las salidas. La antena de la puerta de salida despertaría al transponder del camión, que respondería con su ID y otros datos (como la ID del conductor). Este sistema fue comercializado a mediados de los 80 cuando los científicos de Los Álamos que formaron parte del proyecto lo dejaron para formar una empresa dedicada a sistemas de pago de peaje automatizados. Actualmente, estos sistemas son ampliamente utilizados en carreteras, puentes y túneles de todo el mundo. A petición del Departamento de Agricultura, Los Álamos desarrolló unos tags RFID pasivos para seguimiento del ganado. Al administrase hormonas y medicinas a las vacas enfermas, surgió el problema de distinguir a qué vacas se les había suministrado una dosis, ya que a muchas vacas se les suministraba dos dosis de manera incorrecta. Los Álamos desarrolló un sistema RFID pasivo que utiliza ondas radio a la frecuencia de 125 kHz. Un transponder encapsulado se inyecta bajo la piel de la vaca. El sistema funciona absorbiendo la energía del lector y devolviendo al lector la señal reflectada modulada, técnica que se conoce como backscatter. Este sistema se sigue aplicando actualmente en millones de animales. Los transponders de baja frecuencia también se implementan en tarjetas y se utilizan para controlar el acceso a los edificios. Las empresas comercializaron los sistemas de 125 kHz y luego subieron en el rango frecuencial hasta llegar a alta frecuencia (13.56 MHz), cuya principal ventaja es la de proporcionar velocidades de transferencia de datos más altas y un mayor radio de alcance.

Las empresas, principalmente las europeas, empezaron a utilizar estos sistemas para la traza de contenedores reutilizables y de otros bienes. Hoy en día, los sistemas RFID a

13,56 MHz son utilizados en sistemas de control de acceso, en sistemas de pago y en dispositivos antirrobo de automóviles (un lector situado en la columna de dirección del automóvil lee el tag RFID pasivo que se encuentra en la llave; si el número de ID no es el correcto, el coche no arranca).

A principios de los 90, ingenieros de IBM desarrollaron y patentaron un sistema RFID UHF que ofrecía mayor velocidad de transferencia de datos y un mayor rango de lectura (hasta 65 metros en buenas condiciones). IBM experimentó esta tecnología junto con Wal-Mart, pero nunca la comercializó. A mediados de los 90, al verse afectada por problemas financieros, IBM vendió su patente a Intermec, un proveedor de códigos de barras. Los sistemas RFID de Intermec han sido instalados en numerosas aplicaciones, desde en la traza de bienes en almacenes, hasta en aplicaciones farmacéuticas. Pero el uso de esta tecnología resultaba muy caro, debido al poco volumen de ventas y a la falta de estándares.

Los sistemas RFID UHF despertaron interés en 1999, cuando el Uniform Code Council, EAN Internacional, Procter & Gamble y Gillette se unieron para constituir el Auto-ID Center en el Massachussets Institute of Technology. Dos profesores, David Broca y Sanjay Sarma, habían estado investigando la posibilidad de colocar tags RFID de bajo coste en todos los productos fabricados, a fin de poder seguirlos a través de la cadena de distribución. Su idea consistía en que el tag constara solamente de un número de serie, para que mantuviera un coste bajo (un microchip sencillo que almacenara poca información tendría un menor precio de fabricación que uno complejo de más memoria). De esta forma, los datos asociados con el número de serie del tag serían almacenados en una base de datos accesible a través de Internet. Esto supuso un gran avance en el sector empresarial, ya que a partir de entonces el fabricante podía notificar a los compradores cuando el envío salía de su almacén y, por otro lado, el comprador podía notificar al fabricante la recepción de la mercancía de manera automática.

Entre 1999 y 2003, el Auto-ID Center contó con el soporte de más de cien empresas, del Departamento de Defensa de los EE.UU. y de muchos vendedores de llaves RFID. Se fundaron laboratorios de investigación en Australia, Reino Unido, Suiza, Japón y China. El Auto-ID Center desarrolló dos protocolos de interfaz aérea (Class 1 y Class 0), el sistema numérico EPC (Electronic Product Code) y una arquitectura de red para controlar los datos de los tags RFID en Internet. La tecnología se licenció al Uniform Code Council en 2003, que, a su vez, creó EPCglobal como una joint venture (alianza comercial) junto a EAN Internacional con objeto de comercializar con tecnología EPC.

El Auto-ID Center cerró sus puertas en octubre de 2003 y sus actividades de investigación pasaron a manos de Auto-ID Labs. A día de hoy, algunos de los mayores vendedores del mundo (Albertsons, Metro, Target, Tesco, Wal-Mart) y el Departamento de Defensa de los EE.UU. utilizan la tecnología EPC para realizar la traza de artículos a través de sus cadenas de distribución. Numerosos sectores de la industria (farmacéutica, automovilística, defensa, textil…) están empezando a adoptar esta tecnología.

En diciembre de 2004, el EPCglobal elaboró un segundo estándar, denominado Gen2, ampliamente adoptado.

2.1.4.2.2 El internet de las cosas

En el año 1988 el jefe de investigación de Xerox, Mark Weiser, tuvo la visión de que las tecnologías debían convivir con las personas en el mundo real, no en un mundo virtual. Así, se formuló la idea de Internet de los objetos o de las cosas, IdO o IoT, por sus siglas en inglés.

Como afirma la ponente parlamentaria sobre la internet de los objetos, Maria Badia (2010) este término se refiere a una nueva aplicación de las tecnologías de internet, que se está desarrollando tan rápidamente como lo ha hecho la red en los últimos cuarenta años. Y se prevé que, en diez o quince años, se encuentre en la vida diaria. Utiliza un chip, capaz de contener amplísima información sobre el objeto o la persona donde se ha depositado, que luego transmite esos datos mediante la tecnología de identificación por radiofrecuencia (RFID).

El sistema funcionaría del siguiente modo, el sistema RFID envía el código EPC a través de internet a una base de datos de Object Name Service (ONS) que funciona de igual forma que lo hace los DNS de Internet pero en lugar de identificar una dirección, identifica un producto. A este servidor, pueden acceder las empresas autorizadas a buscar información sobre un determinado producto. El servidor ONS iguala el número EPC a la dirección del servidor donde está guardada la información del producto. Todo este sistema es lo que forma el denominado internet de las cosas.

Este servidor utiliza PML o Physical Markup Language (Lenguaje de marcado de productos) para almacenar toda la información de los productos de los fabricantes. El sistema ONS conecta el EPC con su archivo asociado en PML de forma automática, de tal forma que al introducir un determinado EPC, el servicio remite el archivo PML. Este lenguaje, el PML, está basado en el lenguaje XML y se utiliza para describir objetos físicos.

2.1.4.3 Código EPC

El Código Electrónico de Producto (Código EPC) es un número único diseñado para identificar de manera exclusiva cualquier objeto a nivel mundial, número que además, se encuentra almacenado en un tag de RFID. Este código nace como consecuencia de tres claras necesidades impuestas por la economía globalizada que son:

- La necesidad de codificar artículos unitarios como únicos.
- La necesidad de tener un sistema de codificación globalizado.
- La necesidad de evitar el trabajo humano para alimentar el ordenador.

En la actualidad y como se ha visto en apartados anteriores existen gran cantidad de sistemas de codificación como pueden ser el EAN-13 o el DataMatrix entre otros. Cada uno de ellos responde a diferentes necesidades pero tienen como principal desventaja el hecho de que cuando el producto debe pasar por una cadena de suministro el aumento de los costes es espectacular. Es por este motivo que las asociaciones europea y americana (EAN y UPC respectivamente) se unificaron y crearon EPCglobal para poner unificar la codificación de los productos a nivel global creando de esta forma el código EPC.

Su simpleza y su carácter compacto contrastan con el número tan grande de identificadores que es capaz de generar. Además su esquema lo hace compatible con algunas normas y estándares:

- GTIN (Global Trade Identity Number): Es el identificador único y global del EAN-UCC para identificar productor y servicios.
- GRAI (Global Returnable Asset Identifer): Es un identificador utilizado para numerar los materiales retornables tales como tambores o cilindros de gas.
- GIAI (Global Individual Asset Identifier): En determinados negocios se utiliza para identificar elementos inamovibles e inventarios fijos.
- GLN (Global Location Number): Se utiliza cuando se quiere representar entidades legales o socios comerciales entre otros.

2.1.4.3.1 Estructura del código EPC

La estructura del código EPC es similar a la estructura del código EAN-13, es decir, tiene un identificador de cabecera, un código de empresa y un código de producto como el EAN-13 pero con una serie de diferencias que se describen a continuación:

- ✓ Ya no hay diferencias entre países o zonas de influencias; el sistema de codificación es igual para todos los países del mundo.
- ✓ La codificación está basada en la numeración hexadecimal, por lo que multiplica las posibilidades y es perfectamente inteligible en el lenguaje máquina de los ordenadores.
- ✓ Está compuesto por 24 dígitos en lugar del los 13 del código Ean
- ✓ Los últimos 9 números hacen de numerador, de tal forma que es posible numerar más de 68 billones de un mismo producto sin repetir el código

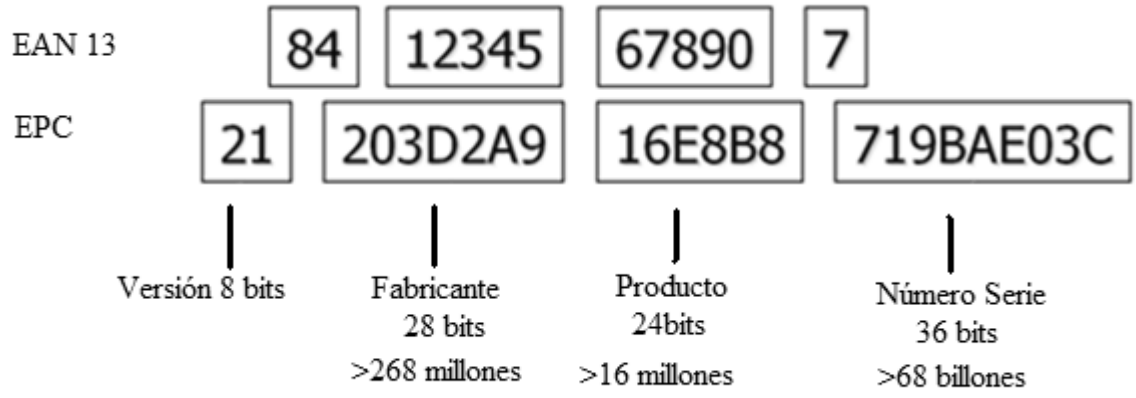


Ilustración 22.-Diferencia entre el código EAN-13 y el código EPC

La nueva forma de codificación es ideal para utilizarla con chips RFID al venir perfectamente preparados para almacenar al código EPC de 96 bits. No obstante, el número del código EPC se puede representar con barras, pero su enorme tamaño lo

hace impracticable para la mayoría de productos que existen actualmente en el mercado y que ya tienen impreso su Ean-13.

2.1.5 Comparativa entre las distintas tecnologías

Se realizará en el siguiente apartado una comparativa de las distintas tecnologías vistas anteriormente para diferenciar de manera más clara sus diferencias, ventajas y desventajas.

En primer lugar se hará un estudio comparativo general de las tecnologías vistas en apartados anteriores para a continuación realizar una comparación exhaustiva entre la tecnología RFID y el código de barras.

2.1.5.1 General

A continuación se muestra de manera general en la tabla2.1 las diferentes características de las tecnologías en un determinado campo.

	Código de barras	Memoria de contacto	RFID pasivo	RFID activo
Modificación de datos	No modificable	Modificable	Modificable	Modificable
Seguridad de datos	Mínima	Alta	Variable	Alta
Capacidad de datos	Lineales de 8 a 30 caracteres y los 2D hasta 7200 caracteres	8Mb	64Kb	8Mb
Coste	Bajo	Alto (>1€)	Medio(15-30 cént/tag)	Alto(10-100€/tag)
Estándares	Estable	Propietario. No estándar	Evoluciona hacia el estándar	Evoluciona hacia el estándar
Ciclo de vida	Corto	Largo	Indefinido	Depende de la batería (3-5 años)
Distancia de lectura	Visión directa, hasta 1,5 m.	Requiere contacto físico	No requiere visión directa. Desde pocos cm hasta 10 m.	No requiere visión directa. Hasta 100 m. o más
Número de lecturas simultáneas	1	1	Múltiples	Múltiples
Posibles interferencias	Cualquier tipo de modificación sufrida en las barras (suciedad, etc.)	Bloqueo del contacto	Ambientes o campos con emisiones radioeléctricas	La interferencia es muy limitada debido a la potencia elevada de la transmisión

Tabla 1.-Comparativa general entre las distintas tecnologías de Auto-ID

2.1.5.2 Código de barras Vs RFID

Por la enorme relevancia del código de barras en nuestra vida actual y el gran impacto que su sustitución por la tecnología RFID puede significar, se resumen a continuación las principales diferencias entre ambas tecnologías para facilitar la comprensión de las dificultades de la sustitución de los códigos de barras por RFID y las ventajas que conlleva:

La tecnología RFID supera en la mayoría de los campos al tradicional código de barras, pero sin embargo en la actualidad el más utilizado es éste último. A continuación se resumen las principales ventajas del sistema RFID frente al código de barras.

El sistema RFID a diferencia del código de barras no necesita tener contacto visual con el lector para poder leer las etiquetas. Además la distancia entre las etiquetas y el lector puede ser desde un par de centímetros hasta cientos de metros dependiendo del tipo de tecnología RFID utilizada.

Otro factor importante es el hecho de que gracias al sistema RFID el producto se puede identificar como único, esto quiero decir que productos iguales se pueden diferenciar por una clave que contiene la etiqueta RFID. El código de barras sin embargo es utilizado el mismo para productos iguales. Por ejemplo dos brik de leche llevan el mismo código de barras, la misma identificación por consiguiente. Si estos brik tuvieran etiquetas RFID se podrían gestionar como productos individuales. Además gracias al RFID cabe la posibilidad de leer múltiples tags simultáneamente hecho que no ocurre con los códigos de barras que deben ser leídos uno por uno.

Por otra parte las etiquetas RFID pueden almacenar mucha más información que los códigos de barras y en determinadas etiquetas de lectura/escritura puede ser modificada dado que poseen una memoria direccionable que permite la modificación de los datos infinidad de veces durante la vida útil de la etiqueta. En el caso del código de barras si éste sufriera algún daño, debido al desgaste o la suciedad no pueden ser reescrito de nuevo, es necesario realizar una nueva impresión. Los lectores RFID son unidades sin partes móviles, lo que garantiza un correcto funcionamiento sin límite de uso y sin que haya que hacer algún tipo de mantenimiento. También se pueden instalar a la intemperie sin que las inclemencias del tiempo, como altas y bajas temperaturas ambientales, los dañen. La distancia de lectura, dependerá del tipo de lector.

La tecnología RFID permite tener mayor seguridad en cuanto a clonación o falsificación que el código de barras además de que las etiquetas son más resistentes debido a que normalmente forma parte del producto o se coloca bajo una superficie protectora que soporta mejor la humedad y la temperatura.

El único factor que parece favorable al código de barras es el coste dado que puede llegar a ser insignificante debido a que en ocasiones se imprime sobre el mismo producto. En la actualidad, aunque los precios han bajado la tecnología RFID sigue suponiendo un desembolso considerable de dinero por parte de la empresa que lo quiere implantar. Es por este hecho que en la actualidad el RFID no llegará a reemplazar por completo el código de barras sino que convivirán.

	Código de barras	Sistema RFID
Ventajas	✓ Muy barato su precio en ocasiones puede considerarse despreciable ✓ Instalación sencilla y económica. ✓ Fácilmente integrable en el proceso de producción y posteriores.	✓ No requiere visión directa del código. ✓ Capacidad de identificar productos de manera individual. ✓ Lectura simultánea de múltiples unidades a la vez. ✓ Modificable. Se puede reescribir sobre la etiqueta si es de lectura/escritura ✓ Gran capacidad de almacenamiento de información ✓ Mayor seguridad frente a falsificación. ✓ Utilización de las etiquetas en ambientes adversos. ✓ Puede reemplazar o coexistir con los sistemas actuales.

Tabla 2.-Tabla resumen de las principales características del sistema RFID frente al código de barras

2.1.5.3 ¿Dominará el sistema RFID el campo de la auto-identificación?

En este apartado se describirán las distintas aplicaciones que poseen las tecnologías de auto-identificación estudiadas y el inmenso campo que abre la tecnología RFID.

El código de barras dado su mínimo precio se posiciona como un método muy competitivo en los casos en que se etiqueten productos a nivel comercial e industrial, en los que se necesite etiquetar directamente el producto, sobre manera si éste es metálico. También resulta competitivo en los casos en los que se necesite identificar unidades materiales fuera de la empresa. Por ejemplo, se han desarrollado lectores de códigos de barras en teléfonos móviles, PDAs, etc. que permiten al personal móvil, técnicos de reparaciones o al personal de seguridad identificar su zona de paso. Aunque la tecnología activa RFID ofrece las mismas capacidades, esta es más compleja y costosa de implementar. El uso de los lectores de códigos de barras es más efectivo en relación al coste en estos casos, porque no es necesaria la capacidad de datos que proporcionan las etiquetas activas.

Los botones de memoria de contacto resultan muy eficaces cuando se trata de leer elementos que han estado en movimiento o poseen una alta vibración o ruido porque trabajan perfectamente en entornos con radiación electromagnética en contra de las etiquetas RFID, y para trazar elementos químicos volátiles gracias a su resistencia a la corrosión.

Por su parte la tecnología RFID ha evolucionado mucho en los últimos años. Gracias a esta tecnología se puede llegar a gestionar gran cantidad de información en tiempo real lo que abre un gran campo de aplicación en el futuro.

La identificación de objetos a través de RFID activas o semiactivas (que permiten obtener lecturas a gran distancia, con gran velocidad y sin necesidad de visualización directa) es la solución más eficaz para la identificación de objetos aunque su costo aún es demasiado caro para implantar en determinadas aplicaciones.

Se está desarrollando en la actualidad, la tecnología RFID pasiva, sobre todo en UHF (más barata que las activas, alrededor de 20 céntimos) que permite compensar el coste de la RFID activa aunque su rango de alcance sea menor.

A través de esta tecnología de auto-identificación se consigue disminuir los posibles errores humanos, por ejemplo en actividades tales como la realización de stoks o la

identificación de objetos realizándose además de una manera más rápida que si la lectura se realizara manualmente.

La trazabilidad de datos en tiempo real y de forma serializada (cada producto posee un número de serie distinto) abre un gran campo en la identificación no sólo ya del tipo del producto sino de ese producto en particular proporcionando un nivel de detalle de información de la cadena de suministro muy superior al que se está manejando actualmente.

Se pueden realizar comunicaciones máquina-máquina de manera que el software y las máquinas pueden tomar decisiones de manera automatizada incrementando por tanto la velocidad del proceso y evitando de nuevo posibles errores humanos.

Según IdTechEx (Puigbò) a principios de del año 2009 se llevaban fabricados y vendidos 3.752 millones de tags RFID desde el comienzo de esta tecnología hace unos 60 años. El 46%, es decir, 1.726 millones, se habían fabricado en los dos últimos años. El mercado de la RFID no ha tenido el crecimiento espectacular que se vaticinaba hace unos meses. Sin embargo, estos datos confirman que se trata de un mercado claramente en su fase de despegue.

Para añadir funcionalidad a las etiquetas RFID se están incluyendo una clase de sensores de bajo coste que añaden una inteligencia adicional a la etiqueta.

Según IdtechEx (Puigbò) las aplicaciones más importantes de las etiquetas de RFID, además de las ya mencionadas (logística de productos de consumo, trazabilidad de productos), son en bibliotecas, aeropuertos y defensa. Naturalmente, un mundo totalmente aparte son las “smart cards” que se utilizan, por ejemplo, en el transporte urbano y uno de los ejemplos más recientes es el del metro de Moscú que supondrá un consumo de 30 millones de tarjetas al mes. Otras aplicaciones de interés son pasaportes, identificación de animales, vehículos, documentos y personas. En España, hay empresas que usan la RFID internamente y hay numerosos proyectos en marcha en el sector del automóvil, alimentación y farmacéutico, entre otros. La organización EPCglobal cuenta ya con más de 1.100 miembros, de los cuales casi 500 son usuarios finales de EE.UU., que como en tantos otros campos, lidera la economía mundial. Los numerosos grupos de trabajo realizan una actividad frenética para integrar las necesidades de los nuevos sectores industriales que se están sumando a EPC (aeronáutica, electrónica de consumo, ocio y entretenimiento, química, automóvil, etc.), acabar todos los estándares técnicos (como la etiqueta para el transporte) y establecer las recomendaciones de uso, entre otras actividades.

2.1.6 Arquitectura del sistema RFID

Un sistema RFID se puede dividir en una capa física, es decir, la que realmente lleva a cabo la transmisión de los datos por radiofrecuencia y una capa de tecnologías de la información cuyo objetivo no es otro que convertir los datos recogidos por la capa física en información útil para el proceso que corresponda. En los siguientes apartados se describirán los distintos elementos pertenecientes a la capa física tales como las etiquetas RFID o los lectores. Dentro de la capa de gestión de la información se profundizará en el middleware como elemento indispensable para realizar la conexión entre el hardware de RFID y los sistemas de información existentes en la empresa.

2.1.6.1 Capa física

2.1.6.1.1 Etiquetas o tag RFID

El tag o etiqueta RFID también conocido como transponder (derivado de los términos transmisor y receptor) esta compuesto por una antena, un transductor radio, un material encapsulado y en el caso de tags activos, una batería. El propósito de la antena es permitirle al chip, el cual contiene la información, transmitir la información de identificación de la etiqueta. El chip posee una memoria interna con una capacidad que depende del modelo y varía de una decena a millares de bytes. Existen distintos tipos de memoria y de antena que se irán describiendo en apartados posteriores.

2.1.6.1.1.1 Tipos de etiqueta según fuente de energía

La clasificación más importante la podemos realizar de acuerdo al origen de la energía, batería interna o fuente de alimentación. Podemos identificar básicamente tres grandes categorías: etiquetas pasivas, semi-pasivas y activas.

Las etiquetas pasivas son las más ampliamente utilizadas actualmente. La energía la toman de la lectora. Las etiquetas son inactivas hasta que la señal de interrogación de la lectora las despierta. Son baratas pero sólo permiten un alcance corto.

Las semi-pasivas poseen batería en la etiqueta pero no pueden iniciar la comunicación hasta que se lo pida la lectora, sirven como sensores, recogen información del entorno. Son más caras y permiten mayores distancias entre lectora y etiqueta. La energía la toman de su batería y de la lectora. Las etiquetas activas por el contrario, integran batería y pueden iniciar la comunicación.

2.1.6.1.1.1.1 Etiqueta pasiva

Los tags pasivos no poseen alimentación eléctrica. La señal que les llega de los lectores que inducen una corriente eléctrica pequeña y suficiente para operar el circuito integrado CMOS del tag, de forma que puede generar y transmitir una respuesta. La mayoría de tags pasivos utiliza backscatter sobre la portadora recibida; esto es, la antena ha de estar diseñada para obtener la energía necesaria para funcionar a la vez que para transmitir la respuesta por backscatter. Esta respuesta puede ser cualquier tipo de información, no sólo un código identificador.

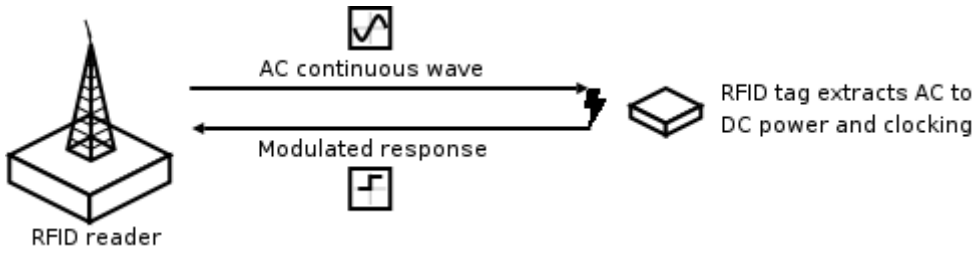


Ilustración 23.-Esquema backscatter para tags RFID

Puesto que dependen de la energía electromagnética de radiofrecuencia tanto para la energía como para la comunicación, los tags pasivos pueden sufrir restricciones en el rango de lectura-escritura. El rango de lectura de los tags pasivos es mucho menor en comparación con los tags activos.

Al no tener autonomía energética, las etiquetas pasivas son más pequeñas que las otras por lo que pueden ser incluidas en una pegatina e incluso en algunos casos insertarse debajo de la piel.

El tag RFID pasivo consta de un microchip conectado a una antena. El microchip puede encontrarse encapsulado de diferentes formas. Puede montarse en un substrato para crear un tag, o emparedado entre capas adhesivas y una etiqueta de papel para crear un label RFID imprimible, o smart label. Los tags también pueden integrarse en tarjetas de plástico, como por ejemplo la tarjeta ciudadana de Gijón, en llaves y en encapsulados especiales para resistir al frio, al calor o a determinados productos químicos. El tipo de encapsulamiento utilizado dependerá de la aplicación. Se debe tener en cuenta que el encapsulado del tag aumenta significativamente su precio.

2.1.6.1.1.1.2 Etiqueta activa

A diferencia de los tags pasivos, los activos poseen su propia fuente autónoma de energía, que utilizan para dar corriente a sus circuitos integrados y propagar su señal al lector. Estos tags son mucho más fiables (tienen menos errores) que los pasivos debido a su capacidad de establecer sesiones con el lector. Gracias a su fuente de energía son capaces de transmitir señales más potentes que las de los tags pasivos, lo que les lleva a ser más eficientes en entornos dificultosos para la radiofrecuencia como el agua (incluyendo humanos y ganado, formados en su mayoría por agua), metal (contenedores, vehículos). También son efectivos a distancias mayores pudiendo generar respuestas claras a partir de recepciones débiles (lo contrario que los tags pasivos). Por contra, suelen ser mayores y más caros, y su vida útil es en general mucho más corta.

Ilustración 24.-Etiqueta activa

Algunos tags activos tienen rangos efectivos de cientos de metros y una vida útil de sus baterías de hasta 10 años. Algunos de ellos integran sensores de registro de temperatura y otras variables que pueden usarse para monitorizar entornos de alimentación o productos farmacéuticos. Otros sensores asociados con RFID incluyen humedad, vibración, luz, radiación, temperatura y componentes atmosféricos como el etileno. Los tags, además de mucho más rango, tienen capacidades de almacenamiento mayores.

2.1.6.1.1.1.3 Etiqueta semi-activa o semi-pasiva

Este tipo de etiquetas activan la circuitería del chip a través de una batería al igual que las etiquetas activas. Sin embargo al contrario que éstas, la energía que es generada para activar la comunicación con el lector es la que se recoge de las ondas de éste mismo, al igual que lo hacen las etiquetas pasivas. Por eso se denominan etiquetas semi-activas o semi-pasivas pues realizan funciones de ambas clases. Además de poseer características de ambas tecnologías también comparten ventajas y desventajas de ambas.

Al utilizar batería para activar la circuitería del chip, las etiquetas resultan ser de un tamaño mayor a las pasivas y su precio es más elevado que éstas. Por otra parte, si se compara con las etiquetas activas, las semi es más pequeña y barata que ésta. Como ventaja cabe destacar que los rangos de comunicación son mejores que en las pasivas, la fiabilidad es comparable con las etiquetas RFID activas y el tiempo de vida es mayor que éstas.

2.1.6.1.1.2 Tipos de etiqueta según tipo memoria del chip

Las memorias se pueden clasificar atendiendo a si su memoria es de sólo lectura o además se puede escribir en ellas:

Sólo lectura: En las memorias de sólo lectura el código de identificación que posee, es único y es personalizado durante el proceso de fabricación de la etiqueta. En este proceso se escribe el código de identificación del producto serializado y único y una vez escrito este código no se podrá modificar en ningún momento. Las memorias de sólo lectura poseen una capacidad baja dado que solamente almacenan el código de identificación.

De lectura y escritura: La información de identificación puede ser modificada por el lector. Además de que la información que ya posee la etiqueta pueda ser modificada después de haber escrito la información por primera vez también existe la posibilidad de poder almacenar más información en la etiqueta. La capacidad de almacenamiento en este tipo de etiquetas por tanto es mayor, dado que se puede llegar a almacenar más información útil sobre el producto.

Anticolisión: Este tipo de etiquetas son etiquetas especiales dado que se tratan de tags que permiten que un lector identifique varias etiquetas de manera simultánea.

2.1.6.1.1.3 Tipos de etiqueta según clase

EPC global como órgano de estandarización para la RFID en su uso con EPC ha organizado las etiquetas en 6 clases. Se podría llegar a coger estas categorías aunque no fueran con contenido EPC.

Clase 0: solo lectura (el número EPC se codifica en la etiqueta durante el proceso de fabricación).
Clase 1: escritura una sola vez y lecturas indefinidas (se fabrican sin número y se incorpora a la etiqueta más tarde)
Clase 2: lectura y escritura.
Clase 3: capacidades de la clase 2 más la fuente de alimentación que proporciona un incremento en el rango y funcionalidades avanzadas.
Clase 4: capacidades de la clase 3 mas una comunicación activa con la posibilidad de comunicar con otras etiquetas activas.
Clase 5: capacidades de la clase 4 más la posibilidad de poder comunicar también a etiquetas pasivas.

2.1.6.1.1.4 Partes de la etiqueta

Chip RFID

Un elemento de elevada importancia en la composición de la etiqueta RFID es su chip RFID. El chip del identificador RFID contiene toda la circuitería necesaria para aprovechar la energía que se recibe a través de la antena o antenas del identificador y para modular la respuesta al lector de acuerdo al protocolo de comunicación establecido. En algunos casos, los identificadores disponen de chips que permiten almacenar datos, registrar mediciones para comunicarlas al lector, etc.

Antena

La antena es un elemento muy importante en el ámbito de la comunicación de datos entre la etiqueta y el lector. Se ha de tener en cuenta que de su diseño y ubicación

dependerán en gran medida factores tan importantes como la zona de cobertura, el alcance o la precisión en la comunicación.

Así pues, por ejemplo el diseño de una antena de polarización lineal ofrecerá la posibilidad al sistema de tener un mayor alcance de lectura que la que dispondría si tuviera una antena de polarización circular. Sin embargo la antena de polarización lineal no ofrecerá mejores resultados en cuando a la precisión de lectura en el caso de que la orientación de la antena de la etiqueta pueda variar durante el proceso.

La antena que incorporan los identificadores para ser capaces de transmitir los datos almacenados en el microchip puede ser de dos tipos:

- Un elemento inductivo (bobina).
- Un dipolo.

Existen dos mecanismos por los cuales es posible transferir la potencia de la antena del lector a la antena de la etiqueta, para que ésta transmita su información: acoplamiento inductivo y propagación por ondas electromagnéticas. Estos dos tipos de acoplamiento dependen de si se trabaja en campo cercano o en campo lejano. En la tabla 2.3 se resumen las principales características de ambos modos.

Propagación/Acoplamiento Inductivo	Propagación por ondas electromagnéticas
Trabaja en el campo cercano: Cobertura baja	Trabaja en el campo lejano: Cobertura mayor
Suele trabajar a bajas frecuencias	Suele trabajar a altas frecuencias
Hay que considerar la orientación de la antena	La orientación de la antena es indiferente
Es muy sensible a las interferencias electromagnéticas	Necesita regulación

Tabla 3.-Principales características de los modos de propagación

El límite teórico entre campo lejano y campo cercano depende de la frecuencia utilizada, ya que de hecho es proporcional a $\lambda/2\pi$, donde λ es la longitud de onda. Esto implica por ejemplo unos 5 cm para un sistema AF y 3,5 m para un sistema UHF, valores que se reducen cuando se tienen en cuenta otros factores.

Tipos de acoplamiento

En este apartado se va a describir brevemente los dos mecanismos por los cuales la etiqueta o tag es capaz de recibir energía del lector.

Acoplamiento inductivo

Este método se basa en el acoplamiento magnético entre el interrogador y el transpondedor, funcionamiento similar al de un transformador. La antena del lector genera un campo magnético que induce una corriente en la antena de la etiqueta, formada normalmente por una bobina y un condensador. La corriente inducida en el elemento acoplado (bobina) carga el condensador y éste proporciona el voltaje necesario para la transmisión.

Los sistemas que utilizan este principio de funcionamiento deben trabajar siempre en el campo cercano, que suele ser una distancia aproximadamente equivalente al diámetro de la antena. Para distancias superiores la fuerza del campo de la señal transmitida decrece con el inverso del cubo de la distancia o incluso con el inverso de la distancia elevada a su cuarta potencia (1/d^3 1/d^4), dependiendo de la orientación de la etiqueta respecto a la antena del lector, lo que dificulta en extremo una correcta recepción de la señal. Este fuerte debilitamiento de la señal puede ser positivo para aquellas aplicaciones donde se desee acotar la zona de cobertura del lector.

Normalmente este modo de funcionamiento se da en sistemas que trabajan a bajas frecuencias (BF y AF). Como el área de cobertura es pequeña, suele utilizarse con etiquetas pasivas, ya que éstas carecen de baterías de alimentación.

Por otro lado, cabe resaltar que la sensibilidad a las interferencias electromagnéticas es mayor en este tipo de sistemas, mientras que su coeficiente de penetración en materiales no conductivos es bueno.

Algunas de las aplicaciones que más utilizan los sistemas RFID inductivos son: las etiquetas inductivas de 1 bit para vigilancia electrónica de artículos (EAS), los controles de acceso y seguridad, sistemas antirrobo y identificación de animales.

Propagación por ondas electromagnéticas

En el campo lejano la señal electromagnética puede considerarse como una señal de radio. Cuando se trabaja en estas condiciones el acoplamiento se produce a través de la recepción de ondas electromagnéticas planas.

En los sistemas basados en campos electromagnéticos, el interrogador o lector transmite la energía a través de ondas electromagnéticas. Los transpondedores situados dentro de la zona de cobertura se ven inmersos en el campo generado y recogen parte de la energía según pasa. La cantidad de energía disponible en un punto concreto está relacionada con la distancia al transmisor (antena) y es proporcional al inverso del cuadrado de la distancia (1/d^2).

Este tipo de propagación se utiliza a muy altas frecuencias: UHF y microondas. Ofrece una cobertura alta, entre 2 y 15 metros, pero normalmente necesitan una batería adicional, ya que la potencia recibida del lector no es suficiente para alimentar la transmisión del transpondedor. Por este motivo, con este sistema suelen utilizarse etiquetas activas.

Por otro lado, la alta cobertura proporcionada hace necesaria una regulación, ya que se trata de una zona del espectro que es necesario gestionar para evitar interferencias sobre otros dispositivos que trabajen a la misma frecuencia.

Los transpondedores que funcionan en el campo cercano requieren una antena grande para recoger la energía procedente del campo magnético generado por el lector. Este tipo de antenas consta de un conductor con muchas vueltas que permiten acumular la energía. En cambio, según aumenta la frecuencia, el número de vueltas que necesita la antena para transmitir se reduce, por lo que la utilización de este modelo de propagación es más adecuada para UHF y microondas.

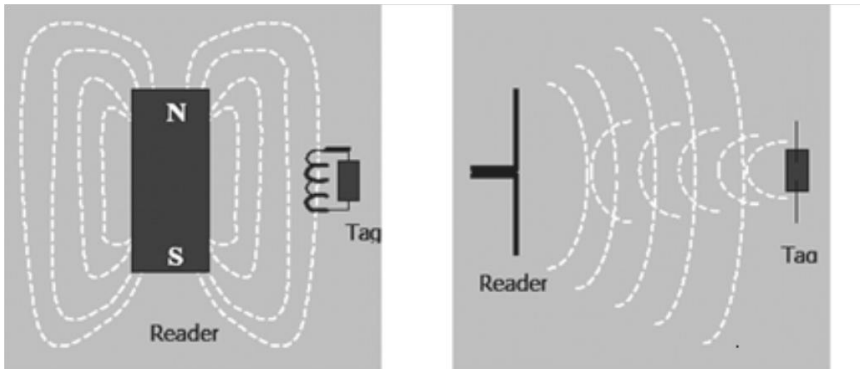


Ilustración 25.-Campo cercano y lejano respectivamente

Sustrato

Es el material que mantiene el chip y la antena juntos y protegidos. La mayoría es un film plástico. Tanto el chip como la antena quedan adjuntados a él.

2.1.6.1.2 Lector RFID

Un lector RFID es el dispositivo que proporciona energía a las etiquetas, lee los datos que le llegan de vuelta y los envía al sistema de información. Asimismo, también gestiona la secuencia de comunicaciones con el lector.

Con el fin de cumplir tales funciones, está equipado con un módulo de radiofrecuencia (transmisor y receptor), una unidad de control y una antena. Además, el lector incorpora un interfaz a un PC, host o controlador, a través de un enlace local o remoto: RS232, RS485, Ethernet, WLAN (RF, WiFi, Bluetooth, etc.), que permite enviar los datos del transpondedor al sistema de información (Portillo, y otros).

Ilustración 26.-Lector RFID portátil (PDA UHF GUN)

El lector puede actuar de tres modos:

- ✓ Interrogando su zona de cobertura continuamente, si se espera la presencia de múltiples etiquetas pasando de forma continua.
- ✓ Interrogando periódicamente, para detectar nuevas presencias de etiquetas.
- ✓ Interrogando de forma puntual, por ejemplo cuando un sensor detecte la presencia de una nueva etiqueta.

Un lector RFID está compuesto por un módulo de radiofrecuencia, una unidad de control y una antena. A continuación se describe cada componente:

El **módulo de radiofrecuencia**, que consta básicamente de un transmisor que genera la señal de radiofrecuencia y un receptor que recibe, también vía radiofrecuencia, los datos enviados por las etiquetas. Sus funciones por tanto son:

Generar la señal de radiofrecuencia para activar el transpondedor y proporcionarle energía.
Modular la transmisión de la señal para enviar los datos al transpondedor.
Recibir y demodular las señales enviadas por el transpondedor.

La **unidad de control**, constituida básicamente por un microprocesador. En ocasiones, para aliviar al microprocesador de determinados cálculos, la unidad de control incorpora un circuito integrado ASIC (Application Specific Integrated Circuit), adaptado a los requerimientos deseados para la aplicación.

La unidad de control se encarga de realizar las siguientes funciones:

Codificar y decodificar los datos procedentes de los transpondedores.
Verificar la integridad de los datos y almacenarlos.
Gestionar el acceso al medio: activar las etiquetas, inicializar la sesión, autenticar y autorizar la transmisión, detectar y corregir errores, gestionar el proceso de multilectura (anticolisión), cifrar y descifrar los datos, etc.
Comunicarse con el sistema de información, ejecutando las órdenes recibidas y transmitiéndole la información obtenida de las etiquetas.

Una de las funciones más críticas que debe realizar la unidad de control es gestionar el acceso al medio. Cuando se transmite información mediante una tecnología que no requiere contacto físico, existe la posibilidad de que aparezcan interferencias que provoquen cambios indeseados a los datos transmitidos y, en consecuencia, errores durante la transmisión. Para evitar este problema se utilizan procedimientos de comprobación (checksum). Los más comunes son la comprobación de bits de paridad, comprobación de redundancia longitudinal (LRC, Longitudinal Redundancy Check) y comprobación de redundancia cíclica (CRC, Cyclic Redundancy Check).

El número de etiquetas que un lector puede identificar en un instante de tiempo depende de la frecuencia de trabajo y del protocolo utilizado. Por ejemplo, en la banda de Alta Frecuencia suele ser de 50 tags por segundo, mientras que en la banda de Ultra Alta Frecuencia puede alcanzar las 200 tags por segundo.

La **antena** del lector es el elemento que habilita la comunicación entre el lector y el transpondedor.

Las antenas están disponibles en una gran variedad de formas y tamaños. Su diseño puede llegar a ser crítico, dependiendo del tipo de aplicación para la que se desarrolle. Este diseño puede variar desde pequeños dispositivos de mano hasta grandes antenas independientes. Por ejemplo, las antenas pueden montarse en el marco de puertas de acceso para controlar el personal que pasa o sobre una cabina de peaje para monitorizar el tráfico que circula.

El elemento más característico de la antena del lector es la frecuencia de operación a la que trabaja el sistema. Sin embargo, existen otra serie de parámetros físicos que es necesario considerar: impedancia, máxima potencia permitida, ganancia, patrón de polarización (polarización X-Y o circular). Estos son los elementos clave que crean el campo de radiofrecuencia, pero a su vez están influenciados por otros parámetros, como la eficiencia de la antena o el tipo de acoplamiento con la antena de la etiqueta. En general, las posibilidades que brinda el tipo de antena, su conexión al lector y su ubicación son innumerables. Cabe destacar que algunos lectores (principalmente aquellos que trabajan en campo cercano, como los lectores de mano), incorporan la antena integrada en el lector, lo que reduce enormemente esta flexibilidad.

El principal aspecto a considerar a la hora de elegir una antena es el área de cobertura requerido para la aplicación, de modo que sea lo suficientemente grande para detectar las etiquetas, pero lo suficientemente pequeño para evitar lecturas no válidas que pueden afectar y confundir al sistema.

Otro aspecto que puede afectar a la cobertura es la orientación de la antena del lector con respecto a la etiqueta, que influye sobre la cantidad de potencia transferida al tag, afectando en ocasiones de forma significativa a la lectura.

A pesar de que las etiquetas pueden leerse en todas las orientaciones, en general el campo generado por la antena del lector tiene una dirección determinada. Este hecho influye especialmente en AF y UHF, pudiendo reducirse la cobertura al 50% o incluso imposibilitando la lectura de la etiqueta. Por ello, resulta conveniente buscar el acoplamiento óptimo entre ambas antenas, y si la orientación de la etiqueta no puede controlarse se debe buscar una compensación mediante un adecuado diseño de la antena.

Todos estos aspectos hay que tenerlos en cuenta antes de adquirir el lector, ya que en general todas las antenas RFID se presentan como productos finales, por lo que es necesario analizar previamente sus características. Sin embargo, la mayoría son sintonizables de modo que puedan ajustarse a la frecuencia de operación seleccionada para el sistema. Esto las hace susceptibles a multitud de factores externos, como son:

- ✓ Variaciones RF.
- ✓ Pérdidas por proximidad de metales.
- ✓ Variaciones del entorno.
- ✓ Efectos armónicos.
- ✓ Interferencias con otras fuentes de RF.
- ✓ Reflexiones de la señal.

El problema de desintonización de la antena, como consecuencia del efecto de estos factores, puede corregirse mediante la introducción de circuitos dinámicos autosintonizadores, que realimentan continuamente la antena para que ésta esté siempre bien sintonizada.

Una vez que una etiqueta es detectada y seleccionada, el lector puede realizar operaciones sobre ella, es decir, leer su información o escribir en ella. Después de finalizar la operación, el lector descarta la etiqueta para proceder a interrogar a la siguiente. Existen algoritmos como el “Protocolo Orden-Respuesta”, en el que el lector ordena a un transpondedor que cese su transmisión, cuando reconoce que ya ha recibido la información. Otro método alternativo, más seguro pero más lento y

costoso, se denomina “Sondeo Selectivo”, donde el lector busca específicamente las etiquetas que tienen una determinada identificación y las interroga por turnos.

2.1.6.2 Capa gestión de la información

2.1.6.2.1 Middleware

El middleware es el software que se ocupa de la conexión entre el hardware de RFID y los sistemas de información existentes en la empresa. Entre sus funciones cabe destacar la gestión de los lectores, el filtrado de los datos y el control de la infraestructura.

Las funciones básicas del middleware son la gestión a nivel de control y configuración toda la red de hardware de lectores y etiquetas, recolectar y filtrar datos de las lecturas, y traspasar estos datos de manera eficiente a los sistemas de gestión.

A continuación se van a enumerar las funcionalidades de los middleware de la manera más general.

Adquisición de datos: El middleware se encarga de la adquisición, agrupación y filtrado de los datos procedentes de múltiples lectores RFID en un sistema complejo.

Encaminamiento de los datos: El middleware permite la integración de las redes de elementos y sistemas RFID en los sistemas de la empresa. Dirige los datos al sistema apropiado dentro de la organización empresarial

Gestión de procesos: El middleware se puede utilizar para disparar eventos en función de las reglas de la organización empresarial donde opera como pueden ser envíos no autorizados, pérdidas de stock, etc.

Gestión de dispositivos: Una de sus funciones también es la de monitorizar y coordinar los lectores RFID, así como verificar su estado y posibilita su gestión remota.

2.1.6.2.2 Ordenadores

Desde un equipo ubicado junto al lector que haga una gestión sencilla y localizada de los datos hasta multitud de ellos que pueden formar una red que aglutine una cadena completa de suministro y a las varias empresas que la compongan apoyándose en el intercambio electrónico de datos (EDI)

2.1.6.2.3 Redes de comunicación

Al igual que lo anterior, en función de la aplicación pueden ir de lo más sencillo a la integración de varias redes de diferentes empresas o incluso a internet

2.1.6.2.4 Software de gestión de la información

Software de gestión de la información (puede ser desde un completo sistema ERP a una simple base de datos que permita el aprovechamiento de toda la información generada)

2.1.6.3 Programadores RFID

Los programadores son los dispositivos que permiten escribir información sobre la etiqueta RFID. La programación se realiza una vez en las etiquetas de sólo lectura o varias veces si la etiqueta es de lectura/escritura. Es un proceso que generalmente se suele llevar a cabo antes de que el producto entre en las distintas fases de producción.

El programador puede operar en un radio de cobertura que normalmente es menor que el rango propio de un lector, ya que la potencia necesaria para escribir es mayor. En ocasiones puede ser necesario utilizar distancias próximas al contacto directo.

Por otra parte, el diseño de los programadores solamente permite una lectura una única escritura cada vez. Esto puede resultar dificultoso cuando se quiere escribir la misma información en muchas etiquetas. En ocasiones la reprogramación se puede realizar permaneciendo la etiqueta sobre el artículo cuya información porta. Este hecho, resulta muy beneficioso si se trata de un fichero de datos interactivo, que va cambiando dentro del mismo proceso de producción. Así pues, los datos se pueden ir modificando según el artículo vaya pasando las diferentes fases de producción. De este modo se consigue aumentar las ventajas de flexibilidad del sistema RFID al no tener que quitar la etiqueta del artículo para poder escribir la nueva información.

La combinación de las funciones de un lector con las de un programador permite modificar y recuperar datos que porta el tag en cualquier momento sin comprometer la línea de producción.

Un tipo especial de programador es la impresora RFID. Existen impresoras que tienen la capacidad de lectura/escritura, que permiten programar las etiquetas a la vez que se imprime con tinta de forma visible. Para ello, antes de realizar la escritura se deben introducir los datos deseados en la impresora. Una vez estén escritos, un lector a la salida comprueba la fiabilidad de los datos. Este tipo de impresión debe realizarse sobre unas etiquetas especiales hechas de materiales flexibles que permiten la impresión en su exterior.

Ilustración 27.-Impresora RFID

2.1.7 Principios de funcionamiento del sistema RFID

2.1.7.1 Comunicación entre lector y etiqueta RFID

Durante la comunicación entre el lector y la etiqueta se produce una transmisión de información y de energía (en el caso de las etiquetas pasivas, necesaria para activar su circuitería). Los datos se envían a través del proceso de modulación en el que se modifica la frecuencia o la amplitud de la onda para realizar la transmisión de los datos. En el caso que la modulación sea FM se modifica la frecuencia (menor frecuencia equivale a cero y mayor frecuencia equivale a uno). En el caso de que la modulación realizada sea AM, lo que se modifica es la altura de la onda (menor altura equivale a cero y mayor altura equivale a uno). Si la modulación que se realiza es PM se altera la polaridad de la onda.

El intercambio de información entre el lector y el tag se puede realizar de dos formas distintas dependiendo de la frecuencia de trabajo y la distancia existente entre las antenas de ambos.

En aplicaciones donde se trabaja con baja frecuencia se trabaja con el campo cercano, que como se ha visto en apartados anteriores no es más que el acoplamiento magnético entre la antena emisora y receptora. El acoplamiento es omnidireccional y da a la antena receptora la energía necesaria para activar la circuitería del tag. La antena reacciona modificando la impedancia que presenta al campo magnético lo que puede ser detectado e interpretado por la fuente emisora. Así, mediante esta variación del campo magnético que las acopla según un determinado protocolo se puede intercambiar información.

Cuando las aplicaciones trabajan a frecuencias mayores se realiza la comunicación mediante el denominado campo lejano donde se consigue un incremento del alcance del sistema. Como ya se ha visto en apartados anteriores, las ondas electromagnéticas se separan de la antena y avanzan en el medio hasta alcanzar la antena receptora. De esta manera la antena receptora alimenta la circuitería del tag.

Es importante destacar que para que el sistema funcione correctamente es aconsejable que la presencia de varias etiquetas en las inmediaciones de un lector no entorpezcan las lecturas. Por ello se diseñan protocolos anticolisión que permiten un orden en la respuesta de las etiquetas a la antena interrogadora y con ello una lectura eficaz de varias etiquetas de forma simultánea.

2.1.7.2 Frecuencias utilizadas

Uno de los aspectos que cobran mayor importancia en la conexión entre la etiqueta y el lector RFID es la frecuencia a la que operan. La frecuencia de operación puede variar dependientdo de la aplicación, estándares y regulaciones.

Atendiendo a la frecuencia de radio que usan los sistemas RFID pueden operar a frecuencia baja, frecuencia alta, frecuencia ultra-alta y frecuencia microondas. Cada frecuencia posee su sector de aplicación aunque hay aplicaciones que pueden ser desarrolladas por sistemas de diferente frecuencia.

En general la frecuencia define la tasa de transferencia de datos entre la etiqueta y el lector. A bajas frecuencias la tasa de transferencia es más baja. Las condiciones ambientales también juegan un papel significativo en la determinación correcta de las frecuencias teniendo en cuenta que las etiquetas RFID deben ir adheridas a los objetos que se quiera identificar o a la presencia de ondas de radio producidas por otros dispositivos que estén funcionando en el mismo ámbito que los objetos que se quieren identificar tales como hornos microondas o cables telefónicos por ejemplo, que pueden llegar a crear interferencia en las bandas UHF y microondas respectivamente.

2.1.7.2.1 Frecuencia Baja (9-135kHz)

La principal ventaja de este tipo de frecuencia es que es aceptada en todo el mundo, funciona con metales y se encuentra ampliamente difundida.

La distancia de lectura es menor a los 1,5 metros por lo que su uso más habitual está en la identificación de animales, sistemas de control de acceso o seguridad de automóviles.

Como principales desventajas destaca que la velocidad de lectura es lenta, el tamaño de etiqueta es grande y se produce una mala lectura ante la presencia de interferencias.

2.1.7.2.2 Frecuencia Alta (13,56 MHz)

Este tipo de frecuencia también se encuentra aceptado en todo el mundo. Es capaz de funcionar en entornos hostiles. A diferencia de la frecuencia anterior no funciona cerca de los metales. Se utiliza principalmente en seguimiento a nivel de artículo (trazabilidad), movimiento de equipajes en los aviones, etc.

El alcance de lectura esta por debajo de los 1,5 metros y como desventaja cabe destacar que la velocidad de lectura de los datos es lenta.

2.1.7.2.3 Frecuencia Ultra-Alta (433 MHz-860-960 MHz)

La frecuencia Ultra-Alta (UHF) no se encuentra aceptado en todo el mundo, aún no se encuentra listo para ser utilizado en Japón. Su uso comercial está en aumento dada sus ventajas, el tamaño de la etiqueta es pequeño y posee un rango de alcance elevado mayor de 1,5 metros.

Como principales desventajas destaca que no funciona en entornos húmedos y se desintonizan cuando las etiquetas están próximas físicamente.

Entre las aplicaciones destaca el seguimiento de trailers y camiones o de palets y contenedores.

2.1.7.2.4 Frecuencia de Microondas (2.45 GHz y 5.8 GHz)

Este tipo de frecuencias son las más utilizadas por parte de los tags activos. Ofrecen largas distancias de lectura y altas transmisiones de velocidad. Además funciona bien frente a las interferencias electromagnéticas

Frecuencias altas usualmente significan antenas de menor longitud, por lo que el tamaño del tag es más pequeño pero posee mayores regulaciones y restricciones en su uso y frecuentemente su coste es alto.

Se utiliza frecuentemente para el seguimiento de contenedores marítimos o peajes electrónicos.

Se debe tener en cuenta, que las bandas de frecuencia no han podido unificarse a nivel global. En EE.UU por ejemplo, las bandas de frecuencia asignadas para su utilización libre en RFID UHF son distintas de las de Europa y Asia

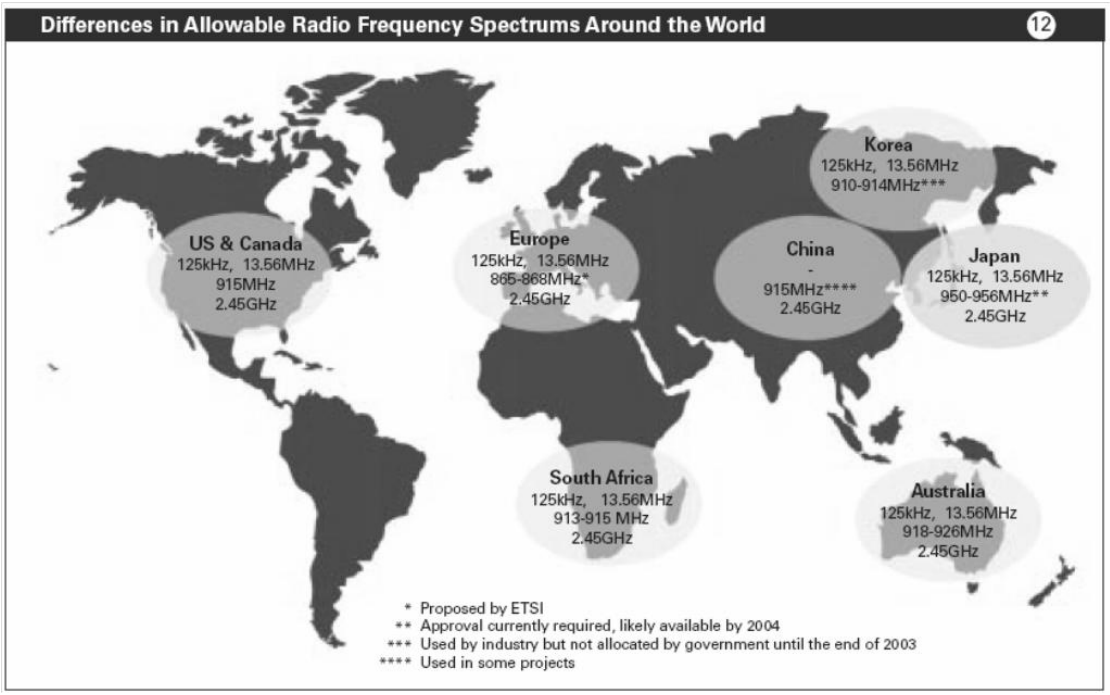


Ilustración 28.-Frecuencias utilizadas en cada una de las bandas por los diferentes continentes o país

2.1.7.3 Velocidad

La velocidad de lectura de los datos depende principalmente de la frecuencia portadora. En términos generales, cuanta más alta sea dicha frecuencia más alta será la velocidad de transferencia.

Un aspecto a considerar es la velocidad con que las etiquetas se mueven dentro de la zona de lectura. El tiempo que tarda una etiqueta en atravesar una zona de lectura debe ser superior al tiempo de lectura de la propia etiqueta, o no dará tiempo al lector para que pueda realizar adecuadamente la lectura. Este problema puede agravarse si son varias las etiquetas que el interrogador debe detectar, ya que cuando varios tags intentan transmitir sus datos a un mismo lector, el tiempo de lectura se multiplica por el número de tags.

Para etiquetas que poseen una alta capacidad de almacenamiento de datos, cuando se trata de leer toda la información almacenada en la etiqueta los tiempos de lectura serán en consecuencia elevados. En este sentido, la opción que poseen algunas etiquetas para realizar lecturas selectivas, por bloques o por sectores, puede ser muy beneficiosa para reducir considerablemente el tiempo de lectura.

A baja frecuencia (<135 KHz) una unidad lectora estándar tardará aproximadamente 0,012 segundos en capturar la información de una etiqueta, permitiendo una velocidad de 3 m/s. Para velocidades más rápidas se necesitarían antenas más grandes.

2.1.8 Estándares RFID

La estandarización permite la interoperabilidad entre aplicaciones y dispositivos. De esta manera las diferentes aplicaciones y dispositivos aún siendo de elaborados por diferentes fabricantes no interfieren unos con otros en sus funciones.

En un principio, previo al desarrollo los estándares que se describirán a continuación, las compañías desarrollaban sistemas propietarios lo que hacia que por ejemplo lectores de un fabricante en concreto solo podían habitualmente leer etiquetas de ese mismo fabricante. Este hecho impedía a esta tecnología crecer a nivel global entre las empresas y por ello se comenzó a plantear la estandarización del RFID para favorecer la interoperabilidad.

Los estándares de RFID abordan cuatro áreas fundamentales:

- ✓ **Protocolo en el interfaz aéreo***:* especifica el modo en el que etiquetas RFID y lectores se comunican mediante radiofrecuencia.
- ✓ **Contenido de los datos***:* especifica el formato y semántica de los datos que se comunican entre etiquetas y lectores.
- ✓ **Certificación:** pruebas que los productos deben cumplir para garantizar que cumplen los estándares y pueden interoperar con otros dispositivos de distintos fabricantes.
- ✓ **Aplicaciones:** usos de los sistemas RFID.

Como en otras áreas tecnológicas, la estandarización en el campo de RFID se caracteriza por la existencia de varios grupos de especificaciones competidoras. Por una parte está ISO con la serie 18000-6C, y por otra EPCglobal con EPC Gen 2.

2.1.8.1 Estándar ISO

El desarrollo de estándares es responsabilidad del comité técnico de la Organización Internacional de Normalización (ISO- International Organization for Standardization) compuesta por representantes de los Organismos de Normalización Nacionales, como la DIN en Alemania, el AENOR de España, el ANSI en Estados Unidos, etc. Si bien la ISO es una organización no gubernamental muchos de sus miembros son representantes de los gobiernos de los países miembros.

ISO supera las necesidades de los sectores públicos y privados, concentrándose en la creación de estándares y construcción de consensos universales para la aceptación de estos estándares. Desde sus inicios en 1947 ha publicado más de 13.000 estándares internacionales para los diferentes tipos de industrias.

Entre los estándares ISO que hacen referencia a la tecnología RFID cabe destacar:

ISO/IEC 10536

Para tarjetas de identificación inteligentes a 13,56 MHz. Describe las características físicas de dichas etiquetas, dimensiones de éstas, localizaciones de las aéreas de interrogación, las señales electrónicas y los procedimientos de reset, las respuestas de reset y el protocolo de transmisión de información.

ISO/IEC 14443

Desarrollado para tarjetas de identificación inteligentes con rango superior a un metro, utilizando la frecuencia 13,56 MHz. Describe las características físicas, el interfaz aéreo que utilizan, la inicialización y anticolisión, y el protocolo de transmisión de datos.

ISO/IEC 15693

Se desarrollan las características físicas, la interfaz aérea y los protocolos de transmisión y anticolisión para tarjetas sin contacto con circuitos integrados en la banda HF (13,56 MHz).

ISO/IEC 15962 RFID

Dirigido al procedimiento que el sistema RFID utiliza para intercambiar información de la gestión a nivel unidad. Establece un formato de datos uniforme y correcto, una estructura de comandos, y el procesamiento de los errores.

ISO/IEC 15963

Este estándar se dirige al sistema de numeración, el proceso de registro y uso de la etiqueta RFID. Se diseñó para el control de calidad durante el proceso de fabricación. También está dirigido a la trazabilidad de las etiquetas RFID durante este proceso, su ciclo de vida y control para anticolisión de varios tags en la zona de interrogación.

ISO/IEC 18000

Diseñado para la creación de una interoperabilidad global, donde se define la comunicación entre las etiquetas RFID y los lectores RFID. Incluye las distintas frecuencias de trabajo.

La norma ISO 18000 define la interfaz aérea, los mecanismos de detección de colisión y el protocolo de comunicación para una etiqueta en diferentes bandas de frecuencia. La norma se divide en siete partes: la primera parte describe la arquitectura, mientras de la segunda hasta la sexta se especifican las características de radiocomunicaciones para las diferentes bandas de frecuencias, así:

Parte 2: etiquetas que operan en bajas frecuencias (F<135 KHz).
Parte 3.1: etiquetas que operan en altas frecuencias (F=13,56 MHz).
Parte 3.2: sistemas RFID que operan en altas frecuencias (F=13,56 MHz), con anchos de banda superiores a 848 kb.
Parte 4: sistemas RFID que operan a ultra-altas frecuencias (F=2,45 GHz); esta parte se divide en dos modos: modo 1: sistema back-scattering pasivo, y modo 2: sistema de alta tasa de datos, mayor alcance y con etiquetas activas.
Parte 5: sistemas RFID que operan a extremadamente altas frecuencias (F=5,8 GHz); en la actualidad, esta parte está en investigación.
Parte 6: define un sistema de back-scattering pasivo alrededor de 900 MHz (la banda sólo es parcialmente disponible en Europa).
Parte 7: especifica un sistema RFID con tags activos en la banda de 433 MHz.

2.1.8.2 Estándar EPCglobal

EPCglobal nació en Octubre de 2003 como el sucesor del "MIT Auto-ID Center, creador de la tecnología EPC (Electronic Product Code) o la tecnología del código de producto. Este código único permite que cada producto tenga su propio código individualmente algo que como se ha visto en apartados anteriores el EAN-13 no es capaz de conseguir.

Ilustración 29.-Logotipo de EPCglobal.

El GS1 EPCglobal se crea como resultado de la unión entre la organización EAN Europea y la organización UPC Americana, resultando un solo organismo global para regulación del RFID con el código EPC.

La junta de gobierno de EPC global esta compuesta por representantes de EPCglobal, GS1, Auto-ID labs, Cisco Systems, KHL/Exel Supply Chain, Haier Group Company, Johnson&Johnson, Kimberly-Clark Corporation, LG Electronics, Lockheed Martin Corporation, METRO AG, Novartis Pharma AG, Office of the Secretary of Defense, Procter & Gamble, Sony Corporation, The Dow Chemical company y Wal-Mart Stores. Inc.

Cabe destacar que estas especificaciones se refieren al nivel físico (interfaz radio que permita leer la información en cualquier lugar del mundo) y de codificación (Código Electrónico de Producto unívoco).

Protocolo	Frecuencia	Tipo de etiqueta
Clase 0	UHF	Sólo lectura
Clase 0 Plus	UHF	Lectura-Escritura
Clase 1	HF/UHF	Una escritura-Múltiples lecturas
Clase 1 Generación 2	UHF	Una (normalmente muchas escrituras en los dispositivos comerciales) escritura-Múltiples lecturas
Clase 2	UHF	Lectura-Escritura

Tabla 4.- Protocolos EPC

2.1.8.3 EPC Gen2

El estándar Gen2 se originó en una reunión del MIT (Massachussets Institute of Technologies o Auto ID-Center) el 2 de octubre de 2002. El Centro esperó para añadir al protocolo existente de Gen1 Class 1 (que en ese momento se encontraba en estado de borrador) una serie de características de Matrics (ahora Symbol). Además, directores de Auto ID-Center, Matrics, Alien, ThingMagic, etc. intercambiaron ideas en Newsport que les llevo a un nuevo diseño de tag EPC y a la evolución de la tecnología EPC (2005).

Debido al retraso que tenía la Gen1, se decidió utilizar esas nuevas ideas para iniciar el trabajo para la Gen2, poniéndose una fecha para que pudiera estar disponible en el mercado a finales de 2005. Para esta nueva generación se marcó como objetivo la mejora de la versión existente, la unificación y la globalización. Cuando Auto-ID Center pasó a ser EPCglobal también se transpasaron los procesos de desarrollo. Así, durante el 2004 bajo la dirección de EPCglobal, un creciente grupo de usuarios, fabricantes y vendedores desarrollaron la especificación final para la nueva Gen2 de tags. Esta fue ratificada a final del año, empezando el trabajo para desarrollar productos comerciales.

El nuevo estándar EPC Gen2 fue se ha creado a partir de las mejores características de la Gen1, tanto de la Class 1 como de la Class 0, y de los protocolos ISO (ISO 18000 series) con el compromiso de mejorar el estándar actual. El estándar ha sido desarrollado con la colaboración de los fabricantes líderes de RFID y de usuarios e instituciones de estandarización, todo ello bajo la coordinación y supervisión de EPCglobal. El nuevo estándar para UHF se ha realizado con los siguientes objetivos:

- Establecer una única especificación UHF, a fin de unificar las existentes como EPC Class 1, EPC Class 0 e ISO 18000-6, parte a y b.
- Diseño para un desarrollo mundial, dirigido a las diferentes regulaciones de diferentes regiones.
- Influenciar y mejorar las especificaciones UHF existentes, además de anticipar posibles aplicaciones futuras (como incluir funcionalidades para etiquetas que contengan sensores).

El estándar Gen2 promete mejoras en diferentes aspectos respecto a la Gen1:

- ✓ Global y abierto: Gen2 incorpora las frecuencias y características para un uso mundial.
- ✓ Incremento del ratio de lectura (velocidad): promete unas 8 veces más que la Gen1. Esto es especialmente importante en países donde el ancho de banda es muy limitado, que pueden llegar a tener velocidades un 30% inferiores que EE.UU.
- ✓ Tamaño: se espera que el tamaño de los chips se puedan reducir en un 20% respecto al tamaño actual.
- ✓ Alta fiabilidad en la comunicación.
- ✓ Mejores algoritmos de lectura que reducirán las lecturas duplicadas.
- ✓ Modo para lectura en entornos de ata densidad de lectores (Dense-Interrogator channelized signaling, normalmente llamado Dense Reader Mode).
- ✓ Seguridad: mejorada con un password encriptado de 32 bits y la posibilidad para "matar" permanentemente el tag.
- ✓ Incremento de la capacidad de escritura gracias a la mejora de los esquemas de escritura.
- ✓ Memoria: es opcional el poder añadir memoria adicional a la requerida para el EPC. Uso para que los clientes finales puedan añadir información específica.

La tecnología está en constante evolución y Gen2 marca un punto de inflexión para el desarrollo de aplicaciones en la cadena de distribución. La mayoría de los agentes implicados en la tecnología RFID han dado soporte a la nueva generación, más que en la Gen1.

El estándar se recoge en un documento de ingeniería de 94 páginas titulado "EPC Radio Frequency IdentityProtocols/Class 1 Generation – 2 UHF RFID Protocol for communications at 860-960 MHz", que fue ratificado en Diciembre de 2004. Dicho estándar especifica las características de los tags, así como el protocolo de comunicación, para garantizar la interoperabilidad con los lectores EPC.

El estándar especifica el comportamiento básico requerido para un entendimiento común, en él hay comandos obligatorios, opcionales y personalizados. Por este motivo se debe entender algo muy importante, y es la diferencia entre lo que se especifica y el rango de comandos o funcionalidades que puede proveer el producto de Gen2. Esto

obliga a buscar realmente la mejor solución para un entorno real, que puede tener comandos opcionales o personalizados, por lo que se debe de tener en cuenta que todos los productos lo soporten. Si no es así, se encontrarán productos certificados en Gen2 pero que según que comando no podrá hacer.

La especificación de EPCglobal UHF Gen2 describe un nuevo protocolo para la interfaz aérea. Este es similar, pero no completamente igual, a los protocolos existentes de la ISO (Organización Internacional de Estandarización), en la ISO 18000 series, parte 6a y 6b. Los ISO ha incorporado la Gen2 dentro de la ISO como ISO 18000-6 Part C, después de que EPCglobal sometiera a la ISO para su aprobación. La pregunta que se plantea es porque se creó un estándar nuevo (aunque sea lo mejor de los existentes) para el EPC. La respuesta es que la ISO 18000 sólo se centra en el protocolo de interfaz aérea, mientras que el EPC define el contenido de los datos, la implementación física de los lectores, redes, etc. porque se ha creado para la cadena de suministro global, aunque pueda soportar otras aplicaciones para otros sectores. Esta característica conlleva a definir un nuevo sistema global.

La especificación Gen2 tiene varios puntos clave:

- ✓ Las etiquetas RFID pueden comunicarse en cualquier frecuencia entre 860-960 MHz, este requerimiento también afecta a los lectores RFID.
- ✓ Los tags son capaces de entender tres esquemas de modulación diferentes:
    - DB-ASK (Double Sideband-Amplitude Shift Keying)
    - SS-ASK (Single Sideband-Amplitude Shift Keying)
    - PR-ASK (Phase-Reversal Amplitude Shift Keying)
- ✓ Los tags pueden transmitir a cuatro velocidades diferentes: 80 Kbps, 160 Kbps, 320 Kbps o 640 Kbps. Los lectores determinan que velocidad usan. (Hay que recordar que la Gen1 proporcionaba velocidades entre 80Kbps y 140 Kbps.)
- ✓ Los tags Gen2 aportan EPC (Electronic Product Code) de 256 bits, mientas que la Gen1 soportaba hasta 96 bits.
- ✓ El estándar Gen2 incluye un método para soportar múltiples lectores y reducir la interferencia entre ellos (Dense-Interrogator Channelized Signaling). Este modo se utiliza en zonas donde múltiples lectores funcionan

al mismo tiempo. Es importante saber que este modo es opcional para los lectores, según la especificación. El comportamiento en el entorno real depende de muchos factores, incluyendo interferencias externas de otros dispositivos, como teléfonos inalámbricos UHF, equipamiento industrial o equipos inalámbricos de redes LAN. Con estos puntos clave se puede obtener la conclusión que la especificación de Gen2 ofrece multitud de posibilidades, de ahí que en el EPC US Conferencia le pusieran el nombre de chinese menu, por su gran variedad de combinaciones.

En el entorno del RFID/EPC se ha hablado mucho sobre la propiedad intelectual de varias patentes que diferentes empresas tienen en sus manos, sobre todo las que hacen respecto a Intermec, que lanzó un programa de licenciamiento rápido. Para cumplir con la especificación de EPCglobal (con los comandos obligatorios) no hace falta ninguna propiedad intelectual de Intermec. Cabe destacar que estas patentes permiten sistemas más robustos que trabajan mejor en los entornos reales. Por este motivo cada empresa proveedora debe negociar directamente con Intermec. También hay otras empresas con patentes relacionadas con la tecnología RFID, y su caso se resuelve de la misma forma, hay que negociar royalties con ellas a cambio de su utilización.

2.1.8.3.1 Mejoras que aporta el Gen2

La aportación más importante que proporcionada por Gen2 es la de tener un único protocolo global, ya que la primera generación tenía dos, para la Class 1 y la Class 0. Esta diferencia aporta un gran avance, porque tener más de un protocolo crea confusión sobre la tecnología a los usuarios finales que deben implantarla. Además los vendedores no saben en que protocolo deben basar sus productos. La Gen2 elimina cualquier confusión y permite bajar los precios de la tecnología. A continuación se detallan las mejoras que introduce la Gen2 respecto a sus antecesores.

2.1.8.3.1.1 Velocidad o transmisión de datos

Con la Gen2 hay una máxima velocidad de 640 Kbps, mientras en la Gen1 se disponía de 80 Kbps en Class 0 y 140 kbps en la Class 1, esto supone 8 veces más de velocidad.

Esta mejora supone un avance muy importante para las empresas porque al incrementar la velocidad se incrementa los tags leídos por segundo, no haciendo falta disminuir la velocidad de sus operaciones para funcionar. Un ejemplo claro es que las cintas transportadoras no necesitarán disminuir la velocidad para que se pueda leer el tag[12], también en las grúas o toros que no deberán pasar tan lentamente. Hay que tener en cuenta que es impensable rebajar la velocidad de los procesos para adaptarlos al EPC porque se perdería productividad.

La capacidad de lectura también se ve incrementada gracias a este factor de mejora. La Gen2 permite escribir 16 bits cada 20 milisegundos[13]. Si se escribe el código EPC de 96 bits más la cabecera, en menos de 140 ms se ha completado el proceso. Esto permite una capacidad de 7 tags por segundo aproximadamente. Este parámetro también es importante para la velocidad de los procesos.

Con las especificaciones en mano se puede calcular aproximadamente que, en condiciones ideales, con la Gen2 se podrían leer unos 1.700 tags por segundo en EE.UU. y unos 600 en Europa (por restricciones en potencia y ancho de banda). Estas velocidades podrían permitir identificar objetos de una cinta transportadora con una velocidad máxima de 200 metros por minuto y que un toro pasara por un portal lector a una velocidad de 13 Km/h.

2.1.8.3.1.2 Flexibilidad de la velocidad

Al igual que cuando se habla con gente en una habitación cerrada, donde se produce ruido que puede molestar a otras conversaciones, a los tags y lectores les sucede lo mismo: pueden hablar rápido y entenderse el uno con el otro si hay tranquilidad en el entorno, sino deben hablar más despacio para entenderse. La primera generación operaba generalmente a una velocidad de comunicación fija, apropiada a las condiciones típicas, para que tuvieran buen comportamiento en la mayoría de aplicaciones. La Gen2 proporciona cuatro velocidades de comunicación diferentes (entre 80, 160, 320 y 640 Kbps), dotando al estándar de una enorme flexibilidad para operar en varios entornos de trabajo. Esta flexibilidad tiene un elevado impacto para obtener una alta fiabilidad en sistemas RFID.

2.1.8.3.1.3 Comando Select

El protocolo de Gen1 clase permite al lector identificar algunos tags mediante sus bits de datos. Así, si el código de fabricante en el EPC era 12345, una tienda podía buscar las cajas o paletas mediante estos bits correspondientes a la empresa, y solo contaría las suyas. Esta característica se diseño para proporcionar mayor rapidez a los inventarios de tags. La Gen2 ofrece una versión con mayor flexibilidad de esta característica. El lector puede antes del inventario seleccionar mediante el comando select, el filtro de búsqueda por diferentes bits como EPC, ID, memoria de usuario, etc. Esta flexibilidad es muy importante para el incremento de la eficiencia de lectura. Por ejemplo, un lector se puede configurar para que ignore los tags para etiquetar cajas y solo lea los de palet. Esta característica reduce la información a procesar en el sistema lector. La Gen2 soporta varios comandos select para operaciones más complejas. Si suponemos que un vendedor quiere identificar todos los tetra briks de zumo de naranja que han caducado. El lector seleccionara todos los tags de tetra briks de zumo de naranja mediante los apropiados comandos select, primero con un select identificando parte del código EPC, y en un segundo select haciendo un filtraje de la memoria de usuario donde se ubica la fecha de caducidad.

2.1.8.3.1.4 Dense-Interrogator Channelized Signaling

Conocido también con los nombres de Dense Reader Mode o Dense Reader Operations, (según fabricantes). Las transmisiones entre lectores y tags se gestionan en tiempo o espectro de frecuencias para evitar su interferencia.

La Gen2 permite tres modos diferentes de operar: single reader mode (un solo lector), multiple reader mode (múltiples lectores) y dense reader mode (con alta densidad de lectores). Estos tres modos tienen como objetivo minimizar las interferencias entre lectores y evitar las colisiones. Un detalle muy importante a tener en cuenta, es que este parámetro es diferente según las regulaciones locales (FCC, EU CEPT, etc.), ya que los anchos de banda destinados son muy diferentes, en Europa es de 2 Mhz, mientras que en EE.UU. es de 26 Mhz. En Europa en el modo single reader, primero transmite el lector y éste escucha la respuesta del tag. Estas dos comunicaciones están separadas temporalmente. Cuando se trabaja en modo múltiple o denso, la transmisión y respuesta se separan mediante diferentes canales en frecuencia, se dispone de 10 canales en el espectro RFID UHF. En América (FCC) se separan las transmisiones en canales de frecuencia, además se utiliza frecuency hopping (salto de frecuencias) entre sus 50 canales posibles

2.1.8.3.1.5 Fiabilidad

No todas las aplicaciones requieren de la alta velocidad que proporciona la Gen2, muchos usuarios necesitan están realmente seguros que todos los tags son identificados correctamente. Las lecturas falsas pueden crear problemas a sistemas de inventario, que incorpora o actualiza una caja o paleta que realmente no existe. En la Gen1 Class 0 había lecturas falsas donde el lector identificaba tags que realmente no existían, según estudios basados en pruebas pilotos se tenían unas 677 de cada 515.000, un 1,3 por mil. Gen2 utiliza varias técnicas para reducir estas falsas lecturas. La primera, cuando un lector de Gen2 envía un comando query, el tag debe responder como máximo con un retraso de 4 ms. Si un tag responde fuera de este tiempo, el lector ignora el tag. Si el tag responde dentro del tiempo establecido, se inicia el dialogo. El tag envía primero un preámbulo (una onda única que no varía). Si el lector ve y valida el preámbulo, entonces lee las ondas radio para transformarlo a bits de datos. El lector verifica que los bits formen una estructura de código EPC válido. Si es cierta continua, sino abre comunicación con otro tag. El tag de Gen2 ha sido diseñado para decirle al lector cuantos bits le ha enviado, así el lector compara este dato con los que ha recibido realmente. Si coinciden se comprueba el CRC (Cyclic Redundancy

Check), de 16 bits de tamaño (también usado en la Class 1 Gen1), para asegurar que se había recibido al completo y sin ningún bit corrupto.

2.1.8.3.1.6 Sesiones

El protocolo de Gen1 tiene una debilidad en el momento que un lector cuenta los tags de su campo de lectura, ya que se puede ver interferido en el transcurso de su inventario por otro lector. En la Gen1 cuando un lector lee un tag, pone a este en modo sleep, así cuando se quiere hacer otro inventario se hace un wake up. Este modo de trabajo hace que no pueda haber inventarios simultáneos sin interferirse. Por ejemplo, un lector fijo de una estantería empieza a contabilizar los tags al mismo tiempo que los pone en modo sleep. En la mitad del inventario aparece un lector de mano que para empezar a contar pone los tags en modo wake up. El lector fijo tendrá que volver a contar todos los tags porque los tags que había contado, ahora son para contar otra vez. La Gen2 se anticipa a situaciones donde hay varios lectores simultáneamente que quieren realizar inventarios, comunicándose con un mismo tag. El objetivo es poder permitir a los lectores contar en paralelo sin interferencias entre ellos. El propósito es distinto al Dense Reader Mode y a la simetría AB (un lector diferente podría cambiarle el flag y volver a tener el mismo problema que con los comandos sleep y wake up). Hay 4 sesiones lógicas (S0, S1, S2 y S3) con simetría AB para cada sesión, que evitan que entre ellas no se puedan interferir. El sistema se puede configurar para que los lectores utilicen la sesión según el tipo, y así se podría determinar que los lectores fijos utilizaran la S0, los de las carretillas la S1 y los móviles la S2. El punto de cómo los lectores asignaran la sesión no está muy claro, pero se prevé que sean los propios usuarios finales quienes lo hagan. En algunas aplicaciones no es importante que un segundo lector no lea un tag o lo haga dos veces (porque la aplicación posterior gestiona el sistema), pero a veces se necesita saber qué lector en particular ha leído un determinado tag, sobretodo para saber la ubicación. Además, esta característica mejora el rendimiento de lectura.

2.1.8.3.1.7 Passwords más largos

El protocolo de Gen1 permite enviar el comando de kill para desactivar el tag permanentemente para proteger la privacidad, para realizar dicha acción es necesario en la Class 1 que el lector envíe 8 bits de código para que el tag responda y realice el proceso. Estos 8 bits solo permiten 256 números únicos. La razón de que sean pocos bits es para reducir sus costes. La Class 0 tiene utiliza 24 bits, que es mejor pero no ofrece la protección correcta a los usuarios finales. El protocolo de Gen2 tiene un password de 32 bits, que es usado para el código kill al igual que para bloquear y desbloquear los campos de la memoria del tag. Esto significa más de 4 billones de posibles opciones, que garantizan que sólo con el permiso del propietario del tag se pueda modificar la información contenida en su memoria.

2.2 Problemática de la tecnología RFID

En este apartado se analiza la problemática que puede venir asociada con los sistemas RFID, desde un punto de vista tanto técnico, social, económico como de salud.

En primer lugar se analizará la situación actual del RFID desde un punto de vista técnico, profundizando en los aspectos que pueden afectar a su fiabilidad, rango de alcance describiendo las posibles soluciones para cada tipo de problema.

También se detallará la problemática del sistema en cuanto al coste de sus componentes e instalación y el gran impacto social que está generando su introducción. Se describirán las principales trabas sociales a la implantación de este dispositivo así como diversos grupos en contra de su uso.

Desde un punto de vista médico, se describirán estudios realizados sobre la incidencia de la implantación de un chip bajo la piel que tiene en el organismo.

2.2.1 Fiabilidad

La capacidad de los sistemas de RFID para realizar su labor de una manera confiable en un entorno cambiante se denomina fiabilidad del sistema. Hay cantidad de factores que pueden influir en el desempeño de los sistemas de RFID (interferencias electromagnéticas producidas por las máquinas, mano de obra, la humedad, etc.).

La fiabilidad se puede ver afectada por:

- ✓ Distancia entre lector y etiqueta
- ✓ Orientación entre tag y antena
- ✓ Interferencias
- ✓ Materiales (metales, líquidos...)

2.2.1.1 Distancia

La distancia a la antena es una de los principales condicionantes para la lectura de un identificador. De hecho, la energía disponible por la antena del identificador para su activación y la que llega devuelta a la antena del lector disminuyen con la distancia elevada a la sexta potencia en el caso del campo lejano.

Por esta razón la lectura a distancia ha sido una de las dificultades del RFID hasta que el estándar EPC Gen 2 basado en UHF consiguió distancias grandes de lectura (<2m) con identificadores de coste muy reducido. A día de hoy, pueden leerse identificadores tipo etiqueta de bajo coste en campo abierto a distancias de 8-10m con fiabilidad. Este avance se ha debido no al incremento de potencias de emisión que están reguladas y limitadas por la normativa sino a una mejora constante de la eficiencia de los chips de los identificadores que consiguen activarse efectivamente con niveles de energía inferiores y, por otra parte, a un aumento de la sensibilidad de los lectores y su robustez frente a interferencias lo que les permite trabajar con señales más débiles.

La gráfica siguiente muestra la curva de disminución de fiabilidad típica de lectura de un identificador con la distancia a la antena. (Identificador sobre metal).

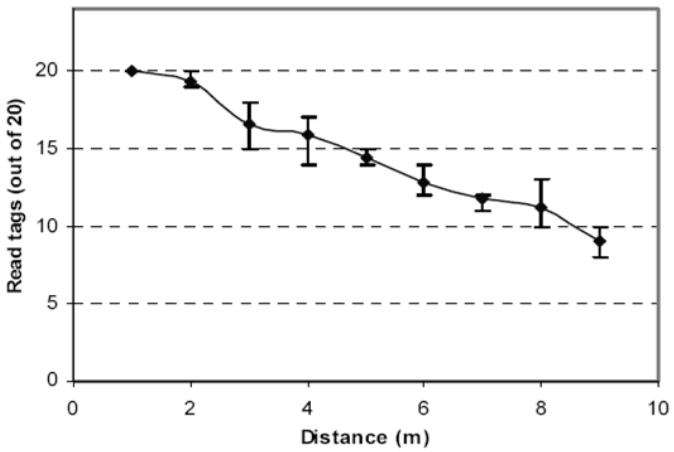


Tabla 5.-Fiabilidad de lectura Vs Distancia antena

2.2.1.2 Orientación entre tag y antena

La orientación de la antena del lector con respecto a la etiqueta, que influye sobre la cantidad de potencia transferida al tag, afectando en ocasiones de forma significativa a la lectura.

A pesar de que las etiquetas pueden leerse en todas las orientaciones, en general el campo generado por la antena del lector tiene una dirección determinada. Este hecho influye especialmente en AF y UHF, pudiendo reducirse la cobertura al 50% o incluso imposibilitando la lectura de la etiqueta. Por ello, resulta conveniente buscar el acoplamiento óptimo entre ambas antenas, y si la orientación de la etiqueta no puede controlarse se debe buscar una compensación mediante un adecuado diseño de la antena.

2.2.1.3 Interferencias

Debido a que la tecnología RFID no es una tecnología basada en un campo visual como es el sistema de códigos de barras, muchos procesos podrán ser automatizados y perfeccionados, como los procesos de seguimiento de medicamentes en hospitales, seguimiento de pacientes, identificación de personas, etc y de este modo ser acelerados. Sin embargo, existen dispositivos, entornos y elementos que pueden crear interferencias en las señales de radiofrecuencia.

La EMI (interferencia electromagnética) es básicamente un ruido que dificulta la correcta recepción de una señal proveniente de un tag UHF. Puede ser causado por una gran variedad de máquinas. Los motores emiten EMI y pueden necesitar ser aislados para prevenir interferencias con los sistemas RFID. Los transportadores con cintas de nylon pueden causar interferencias, como también lo hacen muchos robots en las cadenas de fabricación.

La interferencia también puede ser causada por otros sistemas basados en radiofrecuencia que operen en el almacén o por otras áreas en las que se utilice RFID. Por ejemplo, algunas redes locales wireless utilizan una frecuencia UHF. Éstas interfieren con los sistemas RFID UHF y necesitan ser actualizadas al estándar 802.11.

Los teléfonos inalámbricos, los ordenadores wireless y otros dispositivos también pueden interferir con los sistemas RFID (Sabater Suau).

La RFID activa tiene muy pocas barreras, sin embargo, la RFID pasiva en algunos entornos que se vean afectados por emisiones radioeléctricas pueden entorpecer a su correcto funcionamiento.

Existe una gran diferencia entre interferencia e interferencia mutua (Fennig, 2005). Generalmente, la interferencia mutua puede ser controlada si se entienden los parámetros sintonizables de cada lector en el mercado, se seleccionan las antenas adecuadas, y se realizan ajustes a la infraestructura física, y/o se agregan sistemas electrónicos que pueden activar un lector cuando es necesario e inhabilitarlo cuando ya no se lo necesita. La interferencia entre lectores es improbable, pero no elimina la necesidad de comprender el entorno desde la perspectiva del diseño RF.

Aquellas personas que no conocen estos problemas y sus soluciones suelen pensar que la culpa del bajo desempeño es la “inmadurez de la tecnología”. A través de una mayor comprensión de los principios físicos de RFID, puede realizarse a un piloto o la instalación de RFID con confianza y capturar el valor de la recopilación automática de datos a lo largo de la cadena de abastecimiento.

2.2.1.3.1 Interferencia

La interferencia ocurre cuando una antena recibe señales de la misma frecuencia desde dos o más fuentes. Debido a lo cual la tarea del lector se ve dificultada al tener que diferenciar entre señales que compiten entre ellas y llevan a una alta tasa de errores bit, y bajas tasas de datos.

2.2.1.3.2 Interferencia mutua

La interferencia mutua ocurre cuando las etiquetas son detectadas por dos o más lectores responsables de monitorear áreas físicas distintas. Esto da origen a confusión cuando los datos deben relacionarse, por ejemplo, a una puerta de acceso específica. En general, la interferencia mutua es causada por excesiva intensidad de la señal, una mala sintonización de las antenas de interrogación y una mala configuración del lector.

Usualmente, es inaceptable que la misma etiqueta sea leída por varias puertas de acceso, y el sistema debe diseñarse para eliminar este problema.

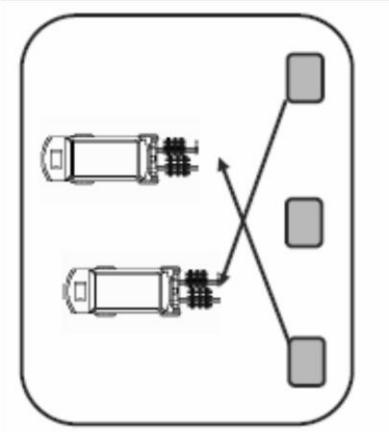


Ilustración 30.-Interferencia mutua.

Los lectores RFID ofrecen la posibilidad de sintonizarlos, es decir, de ser programados con diferentes niveles de flexibilidad. Se puede llegar a disminuir la interferencia mutua a través de diferentes acciones que serán planteadas en el apartado posterior. Como resumen se puede concluir que si se mejora la sintonizabilidad de los lectores y se consigue elegir una infraestructura adecuada el problema de la interferencia mutua queda disminuída al mínimo.

2.2.1.3.3 Soluciones para la interferencia mutua

La potencia de salida del lector determina la máxima distancia a la que se puede leer una etiqueta y la cantidad de material que puede ser penetrada por la señal de comunicación del lector. A menudo, los lectores proporcionan la habilidad de ajustar la potencia de salida, lo que permite sintonizar la modulación del campo emitido por las antenas de interrogación y evitar que interfiera con los sistemas adyacentes. Desafortunadamente, algunos materiales requieren una señal muy intensa para penetrar un *pallet* y leer las cajas que se encuentran en su interior. En ese caso, debe utilizarse algún otro método para modular el campo y, al mismo tiempo, evitar la interferencia mutua del lector.

La configuración adicional de los parámetros del lector puede tener un papel importante para minimizar los efectos de la interferencia mutua. Es importante entender estos parámetros porque puede ser posible eliminar la interferencia mutua a través de la sintonización del sistema, en lugar de agregar costos que surjan de la incorporación de infraestructura física.

En ocasiones es necesario instalar una infraestructura física para aislar a los demás lectores existente en el caso en el que se quiera una señal muy intensa y la sintonización del lector y los parámetros de configuración de la antena de éste no pueden eliminar el ruido causado por la interferencia mutua Un ejemplo de infraestructura física que realice esta función es la instalación de una pantalla conductora entre ambos lectores. En el caso de que la frecuencia sea UHF es suficiente con un filtro de malla para detener el campo eléctrico y aislar el sistema.

El método de activación del lector es más costoso, usualmente se utiliza un activador, por ejemplo un rayo de luz infrarroja, para detectar un movimiento a través de la puerta de acceso. Cuando se detecta un movimiento, el lector es activado por un lapso de tiempo y los datos de la etiqueta son capturados. Este método elimina la radiación innecesaria del entorno interrumpiendo la intensidad del campo cuando ya no es necesaria.

2.2.1.3.4 Soluciones para la interferencia

La solución estadounidense a la interferencia no es otra que evitar la colisión. Los reglamentos del FCC (Comisión Federal de Comunicaciones) establecen el uso obligatorio del salto de frecuencia, es decir, una técnica similar a la modulación en espectro ensanchado (FHSS por sus siglas en inglés) que debe ser implementada en la banda 902-928 MHz para el caso de los niveles máximos de potencia de transmisión permitidos. Utilizando el salto de frecuencia, los dispositivos deben "saltar" de canal en canal en forma pseudo -aleatoria, para reducir la probabilidad de transmitir en la misma frecuencia utilizada por otro dispositivo para recibir señales. Esta técnica elimina virtualmente la posibilidad de interferencia entre lectores, con una posibilidad de solo 0,04 de que exista interferencia entre dos sistemas de lectores UHF en los Estados Unidos.

Para evitar las colisiones, en Europa, el Instituto Europeo de Estándares de Telecomunicaciones (ETSI), encargado de regular la tecnología RFID, ordena un ciclo de tareas del 10% en la banda RFID Europea, es decir, el transmisor de un lector individual no puede estar activo más de un 10% del tiempo. Lo cual provoca problemas en las principales aplicaciones de esta tecnología.

Más recientemente, el ETSI propuso técnicas de frecuencia ágil que utilizan el protocolo 'escuchar antes de hablar', mediante el cual un receptor debe escuchar un canal dado antes de utilizarlo para transmitir. Aunque la amplitud de cada canal es menor a la de los Estados Unidos (200 kHz contra 500 kHz), el límite de potencia permitido es ahora de 3.2W EIRP, significativamente más alto que el anterior estándar ETSI, lo que convierte a la agilidad de frecuencia en una mejora importante comparada con el ciclo de tareas, y dará como resultado un uso mucho más eficiente de la banda RFID en toda Europa.

2.2.1.3.5 Medición de la interferencia

Aunque las interferencias debidas a otros sistemas de lectores son estadísticamente improbables, las señales espurias, armónicas, de frecuencias más bajas transmitidas en una mayor potencia pueden tener un impacto de importancia que podría provocar la desensibilización del receptor y la distorsión inter-modulación. Por consiguiente, es aconsejable la realización de un análisis espectral en la localización de RFID para detectar posibles fuentes de interferencia.

La interferencia entre lectores es improbable, pero no elimina la necesidad de comprender el entorno desde la perspectiva del diseño RFID.

Un analizador de espectro posibilita la medición de RF en tiempo real. Debido a que estos instrumentos son generalmente muy caros y a que se trata de instrumentos científicos complejos, la mayoría de los usuarios finales contratan a expertos para llevar a cabo análisis espectrales como parte de la evaluación de la localización. En lugar instalar un analizador de espectro en un punto único y buscar interferencias durante unos pocos minutos, es mejor un Análisis Completo del Ciclo Faraday, un análisis de espectro que se extiende durante varios ciclos comerciales (42-72 horas) que proporciona una perspectiva de la actividad RF durante las 24 horas.

Consideraciones acerca de la disposición espacial

Uno de los mayores enemigos del sistema RFID como se ha visto anteriormente es el ruido electromagnético presente en el ambiente y que por desgracia es habitual en los entornos de trabajo de donde se implanta este sistema. Una vez implantado, se producirá también el fenómeno contrario: interferencias en el otro sentido.

Luego el papel de los instaladores de soluciones RFID en empresas deberá ser en primer lugar el de hacer un estudio completo electromagnético del lugar donde se quiera implantar, con el fin de identificar las principales fuentes de radiación electromagnética, y decidir muchos elementos de la aplicación (tamaño de tags, alcance, tipos de reader, etc.).

Se debe tener claro dónde colocar los lectores: Lo más habitual es que los readers estén presentes en los accesos de mercancías hacia el almacén, o a la salida de una

cadena productiva. Además, muchas veces es interesante tener los readers cerca de un punto de acceso Ethernet, para poder centralizar todas las lecturas de todos los tags. De hecho también se implementan algunos readers con conectividad Wíreless, aumentando así la independencia entre elementos de la solución.

Será importante testear la situación de RF en el lugar de trabajo, asegurándose bien de las frecuencias que interfieren y la potencia con la que lo hacen. Cuanto más robustas sean las señales interferentes en una banda determinada, más complicado será establecer correctamente la aplicación RFID.

2.2.1.3.6 Anticolisión

El software anti-colisión se utiliza cuando múltiples tags actúan en el campo de radiofrecuencia del lector y deben ser identificados simultáneamente. Este comportamiento es típico en la mayoría de aplicaciones de la cadena de suministros. Es el caso de realizar un inventario de un supermercado ciento incluso miles de objetos pueden estar en el campo de lectura, que puede ser de varios metros de radio.

Las funciones anti-colisión requieren cooperación entre el tag y el lector para disminuir el riesgo de que muchos tags respondan a la vez. En algunos casos el algoritmo puede ser simple en el que cada tag espera una cantidad de tiempo aleatorio antes de responder la petición del lector.

2.2.1.4 Materiales

Las sustancias imantadas afectan a la transmisión distorsionando las ondas de radio. Los líquidos, como soluciones limpiadoras y aceites, absorben la energía de las ondas de radio y el metal puede reflejar las ondas hertzianas. Por tanto los materiales presentan una problemática en la identificiación mediante RFID

La atenuación en RFID normalmente se refiere a la reducción de energía emitida por el lector o a la energía reflejada que vuelve del tag. Si se recibe menor energía en el tag, éste debe estar más próximo al lector para que pueda ser leído. La energía emitida por el lector decrece con la distancia (proporcionalmente al inverso de la distancia al cuadrado). Los tags pasivos RFID UHF (que carecen de batería) devuelven la señal reflectada a muy bajos niveles de potencia. La señal reflectada de un tag decrece proporcionalmente al inverso de la distancia entre el lector y el tag a la cuarta. En otras palabras, la señal emitida por el lector se atenúa por naturaleza con la distancia, y la señal reflectada por un tag pasivo se atenúa a una tasa mucho mayor.

La atenuación de la señal también puede ser causada por la manera en que el sistema es instalado o por factores externos, como los objetos que son etiquetados. Algunos lectores disponen de más de una antena externa que emite ondas de radio. Éstas están conectadas al lector por cables coaxiales. Como la energía viaja desde el lector, a través del cable, hasta la antena lectora, la señal se atenúa. Así, colocar antenas demasiado alejadas del lector puede provocar un bajo rendimiento. El agua, el carbón y otros materiales absorben la energía UHF. Así, los productos con alto contenido en agua, como las frutas y algunas bebidas, o productos hechos de carbón, como las pilas, pueden atenuar la señal que llega a sus tags.

2.2.1.4.1 Absorción

La Absorción electromagnética en el material no puede ser excesiva. Algunos materiales absorben demasiada potencia que transmite el reader, de forma que la potencia reflejada por el tag es aún menor.

Cuando una onda de radio se tropieza contra un objeto, parte de su energía es absorbida por éste y se convierte en otro tipo de energía, mientras que otra parte se atenúa y sigue propagándose. La atenuación aumenta a medida que aumenta la

frecuencia o aumenta la distancia. Cuando una señal choca con un obstáculo, la atenuación producida depende directamente del tipo de material del que esté constituido el obstáculo.

En general los líquidos son materiales absorbentes de RF. Concretamente, absorben por completo toda la energía potencial que el tag necesita. Se reduce por tanto la fuerza de la señal incidente, lo que provoca que el tag no recibe alimentación suficiente. Por tanto, el backscatter en general no se produce correctamente, y por tanto la información nunca llega al reader. Pero por ejemplo el agua reacciona muy distinto a un producto a base de aceite de alguna clase. Por tanto es importante saber con seguridad la composición exacta.

Algún ejemplo del grado de atenuación de los distintos materiales se puede observar en la tabla de a continuación.

Material	Grado de atenuación	Ejemplo
Aire	Ninguno	Lectura de tag al aire libre
Plastico	Bajo	Lectura de tag de un objeto a través de su envoltorio de plástico
Vidrio	Bajo	Lectura de tag de un objeto encerrado en una vidriera
Seres vivos	Medio	Lectura de tag a través de la piel de un animal o persona
Agua	Medio	Lectura de tag en un ambiente húmedo
Metal	Muy alto	Lectura de un tag en el interior de un armario metálico

Tabla 6.-Grado de atenuación según el tipo de materia

2.2.1.4.2 Reflexión

En el lector, idealmente, se produce una señal que llega directamente al tag por medio de la transmisión a través de una antena. Pero el material que rodea tanto a un lector como a un tag pueden tener propiedades refractantes o reflectantes que pueden hacer llegar al tag una información errónea, siendo esta una versión ligeramente deformada de la señal que deberían recibir.

Los materiales que provocan reflexión son principalmene los materiales metálicos. La energía que proviene del lector no es capaz de ser absorbida por la etiqueta lo que puede producir la desintonización de la etiqueta.

2.2.1.4.3 Efectos dieléctricos

Se puede llegar a provocar una desintonización de la antena de la etiqueta debido a que la concentración de campo magnético cerca de un material de un material dieléctrico se puede multiplicar.

2.2.1.4.4 Efectos de propagaciones complejas

Los efectos de propagaciones complejas se producen a través de dos fenómenos físicos. Por una parte las ondas diferentes a la directa y por otra parte los múltiples caminos que causan las ondas estacionarias que pueden cancelar la propia onda directa.

Para lograr evitar estos efectos, se necesitan muchas horas de investigación y pruebas para lograr un desarrollo efectivo de las antenas para etiquetas RFID.

A continuación se muestra una tabla que resume los efectos de materiales sobre la comunicación RFID en general:

Composición del material	Efectos en la señal de RF
Cartón ondulado	Absorción (humedad)
Líquidos conductores	Absorción
Vidrio	Atenuación
Latas	Efectos de propagación múltiple + Reflexión
Seres vivos	Absorción+Desintonización+Reflexión
Metales	Reflexión
Plásticos	Desintonización (efecto dieléctrico)

Tabla 7.-Efecto de los diferentes materiales sobre la señal de RF

Las gamas de baja frecuencia son ideales para las aplicaciones en las que el tag necesite leerse a través de algún material o agua pero a corta distancia. A medida que se incrementa la frecuencia de las ondas de radio, estas empiezan a comportarse cada vez más como la luz: no pueden penetrar los objetos con tanta facilidad y tienden a verse reflejadas por muchos tipos de objetos, especialmente por los metales.

Las ondas de la banda UHF son absorbidas por el agua. Sigue siendo un gran reto para las aplicaciones UHF el leer etiquetas en el interior de pallets o cajas. Los líquidos, en general, absorben las señales de radio frecuencia. Además, hay que tener en cuenta que los materiales que presenten elevados niveles de humedad también lo harán. Por ejemplo, un embalaje de cartón húmedo se convertirá en un problema para el funcionamiento de un sistema RFID.

Los metales reflejan la radio frecuencia, una solución común que puede dar buenos resultados es proveer de un pequeño espacio entre el material metálico a identificar y la etiqueta o tag. La problemática de los metales es muy compleja, los metales muy próximos a las etiquetas pueden incluso desintonizar sus antenas imposibilitando su funcionamiento.

Incluso las fibras de carbono, absorben las ondas de radiofrecuencia. Con todo ello, nos quedan como materiales más benignos para las aplicaciones RFID el tejido, el cartón y el plástico (Montes)

2.2.2 Alcance

Con alcance se denomina la distancia máxima posible para que se desarrolle correctamente una comunicación fiable entre el lector y la etiqueta, es decir, la mayor distancia a la que el lector puede leer la etiqueta o escribir sobre ella. Se define entorno operativo como el radio de cobertura que abarca un lector de tal forma que la señal transmitida presente una atenuación menor a 90dB

El rango de alcance depende directamente de la frecuencia de operación. Como se verá en apartados posteriores el rango variará dependiendo del tipo de frecuencia que se esté utilizando. Además también se tiene que tener en cuenta si la etiqueta es

activa o pasiva y la orientación de la misma. A medida que la etiqueta se gira perpendicular al lector el rango disminuye.

Por lo general, las etiquetas RFID activas disponen de una cobertura mayor, ya que la energía necesaria para activar la circuitería interna del chip no se coge de la energía de la comunicación sino de la batería o fuente de alimentación interna. Por el contrario, para las etiquetas pasivas, parte de la energía de la comunicación es recogida para activar el chip y por ello disminuye la cobertura a la que puede leerse éste.

2.2.2.1 Cobertura de los sistemas de baja frecuencia

En los sistemas de baja frecuencia, al tratarse de un sistema inductivo, el campo magnético decrece de manera muy rápida con la distancia siendo el inverso del cubo de la distancia y también con las dimensiones de la antena.

En el caso de aplicaciones donde la cobertura de lectura deba ser limitada a un área pequeña el sistema de baja frecuencia presenta una clara ventaja sobre los demás. Las antenas utilizadas son pequeñas y complejas pero la tecnología se encuentra actualmente muy desarrollada.

El rango de alcance de las etiquetas pasivas es pequeño (como mucho medio metro) aunque este radio de alcance se puede ver modificado por la potencia en la antena.

2.2.2.2 Cobertura de los sistemas de alta frecuencia

Los sistemas de alta frecuencia alcanzan un rango de cobertura muy elevado, abarcando rangos de entre 1 y 2 metros en el sistema pasivo y hasta 15 metros o más para los sistemas activos.

2.2.2.3 Cobertura de los sistemas de ultra alta frecuencia

En cuanto a los sistemas de ultra alta frecuencia (UHF), los dispositivos pasivos pueden alcanzar una cobertura de alrededor de 3 o 4 metros mientras que los dispositivos activos, pueden llegar a alcanzar los 20 metros.

2.2.3 Seguridad

La seguridad en la transmisión de los datos mediante el sistema RFID es un aspecto muy importante que debe ser tratado con especial atención. La seguridad posee numerosas características que deben ser cumplidas para que un determinado sistema sea denominado "seguro". Así pues la confidencialidad es un aspecto muy importante, en el caso de los sistemas RFID a excepción de algunos sistemas de ISO 14443 la comunicación realizada entre el lector y etiqueta no se encuentra protegida y puede llegar a ser vulnerada. El canal entre el lector y la etiqueta puede tener un largo alcance por lo que puede ser escuchado por otro sujeto que se encuentre en la proximidad. El contenido de la etiqueta puede llegar a ser leído si no hay implementado un control de acceso a la misma.

Por otra parte un ataque posible a los sistemas es el rechazo de servicio dado que algunos de los sistemas RFID pueden ser perturbados de manera fácil por interferencias de frecuencia por lo que la propiedad de disponibilidad sería vulnerada.

La integridad de la información que se transmite mediante los dispositivos RFID no puede ser asegurada a excepción de la ISO 14443 que usa mensajes de códigos de autenticidad. El control de redundancia cíclica (CRC) es utilizado habitualmente sobre la interfaz de la comunicación pero solamente protege fallos aleatorios y no llega a corregirlos sólo reconocerlos. La memoria de la etiqueta (si es de escritura) puede llegar a ser manipulada si no se implementa un control de acceso, alguien puede cambiar los datos de una etiqueta siendo de esta forma los datos leídos no íntegros.

Otra propiedad muy importante de la seguridad es la autenticidad. En el momento que el EPC (Electronic Product Code) puede llegar a ser manipulado, cualquier etiqueta de lectura/escritura es susceptible de ser manipulada en su código. No ocurre lo mismo

con las de sólo lectura dado que sólo se pueden escribir en el momento de la creación de la etiqueta. La autenticidad por tanto en las etiquetas de lectura/escritura se puede ver vulnerada.

Por último y no menos importante el anonimato constituye un pilar fundamental de la seguridad. Cada código identificador (EPC) es como ya vimos en apartados anteriores único. Por tanto, la etiqueta puede servir como modo de rastreo de una persona o cosa que lleve la etiqueta.

2.2.3.1 Mecanismos de seguridad

Existen parámetros de cifrado, autentificación y autorización que se utilizan para aumentar la seguridad de la comunicación entre la etiqueta RFID y el lector. Para que esta comunicación se produzca de manera segura tanto el lector como el tag deben cooperar de manera conjunta y ejecutar el protocolo necesario para que la transmisión de datos se realice de manera correcta y segura. Así pues, los parámetros de cifrado, autentificación y autorización se utilizan cuando el intercambio de información entre el tag y el lector debe ser seguro. Para esto tanto el tag como el lector deben cooperar y ejecutar el protocolo necesario con el fin de conseguir el nivel deseado de seguridad en el transporte de los datos. Por ejemplo para prevenir que un lector no autorizado recupere datos de un tag determinado éste y el lector deben ejecutar un protocolo de autorización intercambiando un código secreto. Luego de que esta información compartida ha sido intercambiada y validada, el tag transmite datos al lector de forma segura.

2.2.3.1.1 Control de acceso a los datos

Algunas etiquetas RFID llevan implementados mecanismos de control de acceso para sus memorias de lectura/escritura. Estos mecanismos se producen entre el lector y la etiqueta RFID antes de entregarle al lector el permiso de acceso de lectura y escrituras en su memoria. Consiste en una autentificación del lector para que la etiqueta vea que el lector es legítimo y le entregue acceso a ella.

2.2.3.1.2 Cifrado y autentificación del mensaje

Algunos sistemas RFID (basados en ISO 14443 y MIFARE) pueden cifrar y autentificar el tráfico de datos con protocolos propios. De modo que alguien que escuche la conversación no sea capaz de descifrar lo que ésta conlleva.

2.2.4 Robo o pérdida de identificadores: Sustitución de identidad. Falsificación. Biométrica

2.2.4.1 Robo de identidad

La identificación de una persona puede basarse en algo que la persona pueda llevar como por ejemplo una tarjeta identificativa Esto no suele ser fiable, dado que las tarjetas pueden ser olvidadas, intercambiadas o robadas pudiendo así suplantar la identidad de la persona. El problema del robo de identidad ha aparecido en los últimos años. Éste consiste en la interceptación fraudulenta de datos y su posterior uso con fines distintos, al fin de personar a alguien que no es.

La defensa al robo de identidad es sin duda más importante en casos como el pasaporte electrónico, o las tarjetas de identificación en los empleados.

2.2.4.2 Falsificación

La falsificación de chips RFID es otra cuestión problemática en cuanto al sistema dado que es posible falsificar un chip RFID mediante diversas técnicas que serán explicadas en apartados posteriores.

En 2006, el investigador canadiense Jonathan Westhues anunció que había logrado clonar el implante subcutáneo RFID de Verichip Corporation, pese a lo cual la empresa seguía afirmando en su web que el chip tenía un identificador único y que el sistema era absolutamente seguro (Bengo).

Cloning:

Mediante esta técnica se escribe sobre un tag RFID los datos que posee otro tag RFID. Mediante la escucha entre la comunicación realizada entre un lector y una etiqueta se logra obtener los datos y copiar los originales en otra etiqueta. Se puede llegar a conseguir mediante esta técnica de ataque que un objeto o persona se pudiesen hacer pasar por otro dado que su etiqueta poseería los mismos datos que la etiqueta original. Este hecho se vuelve especialmente importante en caso como el e-passport o en tarjetas que permiten el control de acceso a determinadas áreas.

Spoofing

En esta técnica se escribe en una etiqueta en blanco los datos que identifican al producto. Se realiza reproduciendo tags a partir de los datos interceptados en una transmisión del tag original. De este modo los datos tendrán la misma estructura. Para lograr realizar spoofing la etiqueta debe tener la capacidad de escritura. Las etiquetas pasivas en su mayoría de sólo lectura sufren este riesgo de copia.

2.2.5 Coste del sistema

El coste de las etiquetas aún sabiendo que en los últimos años ha ido decrementándose de forma notable es aún importante y todavía no llega a los 4-5 céntimos que los expertos consideraban adecuados para que las empresas se plantearán las ventajas de su implantación. La diferencia de precio existente entre los tags RFID y su competidor en este caso el código de barras es muy elevado, ganando en esta lucha el código de barras dado que su precio es casi despreciable. Es por ello que muchas empresas se resisten todavía a su implantación. Sin embargo para técnicas de auto-identificación personal las ventajas frente a otros sistemas pueden llevar a la implementación de éste método en relación seguridad/precio.

Se debe tener en cuenta también, que el coste de la implantación de un sistema RFID no solamente depende del coste de las etiquetas sino también de la inversión que es preciso hacer en la compra de la infraestructura capaz de hacer que el sistema funcione, esto es lectores de tags RFID, sistemas de codificación y descodificación y el tratamiento de la información.

En este apartado se resumirá los costos de los principales componentes que hacen que un sistema RFID funcione correctamente. Se debe tener en cuenta que las necesidades de cada empresa son diferentes y que por tanto los costes variarán dependiendo de estas necesidades.

2.2.5.1 Etiquetas RFID

Las etiquetas RFID junto con los lectores son los principales componentes de un sistema RFID.

El coste de una etiqueta depende de diversos factores entre los que destacan el tipo de tag (si es pasivo o activo) y la frecuencia en la que trabaje.

Las etiquetas pasivas son más baratas que las activas (éstas llevan batería). El coste de una etiqueta pasiva oscila entre los 10-25 céntimos, los más sencillos producidos en gran volumen llegando a alcanzar algunos el valor de algunos euros en el caso que los tags se encuentren encapsulados en plástico o dentro de llaves para protegerlos de ambientes agresivos como puede ser el frío, calor o productos químicos.

Además de este precio las empresas deben considerar también los costes de testeo de los tags pasivos. En el año 2004 las tasas de error de los tags UHF EPC oscilaba entre el 0% y el 20% mientras que actualmente la tasa esta en torno al 0.2%-0.5%. Se debe además tener en cuenta que será necesario comprar algunos tags más de los imprescindibles para suplir posibles bajas debido a tags defectuosos.

En referencia a las etiquetas activas, como se ha dicho anteriormente, su precio es superior a los tags pasivos oscilando la cantidad entre 10 o 100 euros. La variación de esta cifra depende del tamaño de la batería de la etiqueta, de la cantidad de memoria del chip y del encapsulado que posea.

2.2.5.2 Lectores RFID

Los lectores RFID son el otro componente fundamental del sistema. El precio de este componente depende de sus características y de su funcionalidad. Hay que tener en cuenta que el precio de estos lectores no incluye el precio de la instalación de éstos ni del cableado hasta las áreas donde se instalan los lectores.

A modo de ejemplo los lectores UHF poseen un coste que va desde los 500 hasta los 3000 euros dependiendo de sus características.

2.2.5.3 Middleware y servidores

Como ya se ha descrito en apartados anteriores el middleware es el software que se ocupa de la conexión entre el hardware de RFID y los sistemas de información existentes en la empresa. Entre sus funciones cabe destacar la gestión de los lectores, el filtrado de los datos y el control de la infraestructura.

El coste del middleware es variable dependiendo de un vendedor o de otro y lo más habitual es que dependa de la complejidad de la aplicación y del número de dispositivos en los que será instalado entre otros.

2.2.5.4 Otros costes

Debido a la complejidad que supone la implantación de un sistema RFID, la mayor parte de las empresas tendrán que hacer uso de un integrador de sistemas para que instale los lectores y los tags en el mejor emplazamiento para que el sistema sea lo más eficaz posible. Se ha de tener en cuenta como se ha analizado en apartados anteriores los factores que afectan a la capacidad de lectura de los tags como puede ser la posición del tags, orientación, interferencias etc. Se debe asegurar también que la transferencia de los datos al middleware se realiza de manera correcta.

Por otra parte, la formación de los empleados de la empresa sobre el manejo del sistema es fundamental por lo que se debe tener en cuenta también el coste de formación de los trabajadores

2.2.6 Aceptación social: Violación de la privacidad.

2.2.6.1 Amenaza de la privacidad

Aunque el inicio del desarrollo de la tecnología RFID se remonte 50 años atrás, este tipo de tecnología aún se encuentra entre las tecnologías más desconocidas entre el público en general, aunque ya se esté utilizando en acciones tan cotidianas como pagar el transporte urbano o utilizarlo en el pasaporte.

Este desconocimiento de la tecnología unido a la falta de leyes que regulen el sistema de protección de la información son el caldo de cultivo apropiado para generar entre la población cierta desconfianza hacia las posibles amenazas que sobre su privacidad se ciernen.

En este apartado se analizará la amenaza a la privacidad de las personas desde un punto de vista de vulneración de la protección de datos y desde el punto de vista del seguimiento a una persona. Ambas características si se llevan a cabo violan la privacidad de las personas un derecho fundamental en la sociedad actual.

Es por ello, que se debe tener en cuenta estos hechos, para tratar de solventar estos posibles problemas implícitos en la tecnología RFID y tratar de potenciar las innumerables ventajas que puede llegar a poseer, ofreciendo grandes beneficios tanto a las empresas que hacen uso de ella como a los usuarios finales aunque la desconfianza actual sobre ella ofrezca cierta polémica entre este último sector.

En la actualidad, el sistema RFID cada vez se está imponiendo más y más en la sociedad debido a que los costes de producción de las etiquetas están disminuyendo por lo que su implantación tanto en el sector privado como en el sector público está progresando de manera exponencial. Es por ello que es necesario tener un conocimiento amplio sobre esta tecnología y poseer leyes que reduzcan al mínimo posible los problemas de amenaza de privacidad que puede conllevar su uso.

Revelación de datos personales

Una etiqueta RFID puede llegar a contener gran cantidad de información entre ella datos personales, como puede ser el caso por ejemplo de una tarjeta de acceso a un área restringida o un pasaporte. Esta información además se suele utilizar sin cifrar para no compartir con otros países algoritmos y claves por lo que la información se vuelve accesible a cualquier persona que posea un lector RFID.

Esta recopilación fraudulenta de datos personales si la autorización de la persona que porta la etiqueta con sus datos personales vulnera los principios de la Ley Orgánica de Protección de Datos.

La tecnología RFID estás sufriendo un progreso espectacular en la sociedad actual por lo el sistema legislativo, siempre más lento, está tardando en crear leyes que regulen este tipo de tecnologías.

Pero este tipo de problemas de amenaza en la protección de datos no sólo se puede aplicar a las etiquetas RFID sino a la totalidad de la infraestructura del sistema, incluyendo por tanto al lector RFID o la base de datos donde se encuentran almacenados los datos leídos de las etiquetas por el lector

Vigilancia

La vulnerabilidad de los derechos de privacidad de las personas se puede llevar a cabo no sólo mediante las lecturas ilegales de los datos personales contenidos en las etiquetas RFID sino también mediante el seguimiento de las personas que llevan una etiqueta RFID. Por el hecho de que cada etiqueta contiene un identificador único que lo distingue de todas las demás ésta puede ser usada como medio de vigilancia.

Esta desventaja está relacionada con el anonimato de las personas, ya que la vigilancia de las personas viola la privacidad de éstas. También se ha manifestado la preocupación por la posibilidad de una mayor vigilancia, especialmente en el lugar de trabajo, ya que podría derivar en una discriminación, exclusión, victimización y posible pérdida del empleo. Esta tecnología permite localizar en cada momento a individuos que lleven etiquetas RFID en su ropa, coche, tarjeta de acceso, etc., permitiendo una

vigilancia constante y pudiendo por lo tanto realizar técnicas de rastreo, lo que supone un paso más en la vulneración de su vida privada, coaccionándole en el ejercicio de sus libertades más básicas. Además esta tecnología tiene el añadido de que es casi imperceptible para el ojo humano, gracias a lo cual una persona podría llevar una etiqueta RFID en su ropa, por ejemplo, sin tener constancia de ello.

Los defensores de la privacidad están preocupados por la posible pérdida de anonimato de las personas. Temen que con el lector RFID, cualquier individuo u organización puede rastrear los movimientos de una persona y hacer esta información disponible a agencias de mercadeo o de gobierno. Algunas corporaciones han adoptado esta tecnología para facilitar la localización de empleados clave dentro de un local o campus extenso. Los defensores de la privacidad sugieren a los comerciantes que desactiven los transmisores de RFID tan pronto los clientes abandonen el local comercial. También recomiendan que los documentos que contengan RFID, como por ejemplo, los pasaportes, se guarden en un compartimiento hecho de un material que no permita que un lector RFID oculto tenga acceso a la información en el chip ().

“Existe una amenaza para las personas y nuestra sociedad", mantiene Ari Schwartz, Subdirector del Centro para la Democracia y la Tecnología, una agrupación defensora de los derechos civiles sin fines de lucro. Aquellas personas que corren riesgos de acoso, como víctimas de violencia doméstica o responsables del cumplimiento de la ley, podrían ser más vulnerables, afirma Ari. En cuanto a la sociedad, con el paso del tiempo, el uso de esta tecnología podría costar a los ciudadanos sus libertades civiles. Sin embargo, los defensores de RFID mantienen que todas las nuevas tecnologías tienen sus detractores. “Muchos de estos argumentos surgieron a partir de los códigos de barras”, remarca Mark Roberti, editor de la revista RFID Journal. “Debe de haber entre 30 y 40 millones de personas en EE. UU. que llevan transmisores RFID en su cuerpo o en su coche, y nunca se ha producido ni un solo caso de infracción de la privacidad”, sostiene.

Además, algunos expertos en seguridad informática afirman que el riesgo de ser espiado es mucho mayor a través de un teléfono móvil, que tiene una fuente de energía propia, a diferencia de la mayoría de los chips RFID, y puede rastrearse desde kilómetros de distancia, no sólo desde unos metros (O. Foley).

Creación de perfiles

Otra posible amenaza contra la privacidad de las personas es la elaboración indiscriminada de perfiles. Si bien este hecho, viene implícito a cualquier tipo de tecnología que permita obtener datos de carácter personal de forma masiva a través del sistema RFID se puede dar el caso de elaborar perfiles en lugares tales como en los supermercados.

Protección de la privacidad

A lo largo de la historia se han propuesto diferentes contramedidas para evitar la vulneración de la privacidad como se ha visto en los apartados anteriores.

La solución más simple es desactivar las etiquetas RFID bien permanentemente (utilizando técnicas como killing, clipping o RFID-Zapper) o temporalmente utilizando jaulas de Faraday o modos sleep/wake.

Killing

Esta técnica consiste en inhabilitar permanentemente o matar una etiqueta RFID con el comando kill. Actualmente se puede realizar sobre etiquetas EPC Clase-1 Gen-2. Cuando una etiqueta RFID EPC recibe un comando kill (matar) procedente de una lectora se consigue que se haga permanentemente no operativa. El comando kill se protege con un PIN (Personal Identifier Number) o contraseña, en las EPC Clase 0 es de 24 bits, en las EPC Clase 1 es de 8 bits y en las EPC tipo HF es de 24 bits.

Destrucción de la etiqueta. Clipping

A través de esta técnica se desactiva la etiqueta RFID rompiendo mecánicamente parte o toda la antena.

Destrucción de la etiqueta.RFID- Zapper:

Esta técnica consiste en destruir la etiqueta pasiva de manera que la etiqueta no pueda ser leída y por lo tanto la persona que porta el objeto no pueda ser identificada ni objeto de seguimiento. Para lograr la destrucción de la etiqueta RFID, es necesario tener ciertos conocimientos técnicos sobre la tecnología. Se puede conseguir exponiendo la antena en un microondas aunque de ésta forma se corre el riesgo de que el producto que porta el tag también acabe deteriorado. Para solucionar este problema se creó 'RFID Zapper' que utiliza microondas en una sola dosis generando un campo electromagnético fuerte que provoca la desactivación del tag, evitando de esta manera el deterioro del producto.

Prevención de lectura

Mediante esta técnica el tag no se desactiva ni destruye sino que lo que se realiza es una prevención de su lectura. La prevención de la lectura se puede conseguir mediante fundas protectoras como por ejemplo fundas para los e-passport, para las tarjetas de crédito etc.

Estas fundas actúan como una jaula de Faraday que bloquea la emisión de la antena del RFID protegiendo de esta forma su contenido de los campos electromagnéticos generados por un lector RFID.

2.2.6.2 Preocupación Religiosa

Algunos cristianos han salido contra el dispositivo RFID implantables, ya que hay una profecía Bíblica, donde todas las personas deben recibir la marca de la bestia "en su mano derecha o en sus frentes", que se describe en el Libro de Apocalipsis 13:16-18, a participar en la actividad económica bajo el gobierno del Anticristo. Esta preocupación se agrava por el hecho de que, según un reciente artículo de ABC News, ha habido informes de otros chips que se implantan en los pacientes en la mano derecha. Sin embargo, el chip también se ha visto que se implanta en el brazo o la mano izquierda,

así como otras áreas. A menudo se supone que los dieciséis dígitos en el chip den pie a una operación matemática de la que se obtenga 666, la Marca de la Bestia. La palabra griega Charagma (que significa marcar) describe la perforación mordedura de una serpiente, que es similar a usar una aguja para colocar el dispositivo bajo la piel.

Además, existen diversas religiones y sectas, que detestan la penetración en el cuerpo humano, al igual que con la cirugía o la implantación de dispositivos. Entonces, la implantación de un VeriChip (RFID implantable) viola las costumbres de esos grupos.

2.2.6.3 Asociaciones en contra del RFID

Desde la aparición de la tecnología RFID en el mercado, ésta se esta implantando en cantidad de procesos y aspectos de nuestra vida, haciendo que el RFID sea una realidad en las vidas de las personas. Es por ello, que muchas personas han empezado a alzar la voz en contra de lo que ellos piensan que es una vulnerabilidad de la intimidad

En 1999 se fundó la organización CASPIAN (Consumidores en Contra de la Invasión de la Privacidad y Enumeración por los Supermercados, por sus siglas en inglés) cuyo origen es popular y que pretende enfrentarse a los asuntos de privacidad de los consumidores.

Actualmente la organización está formada por casi diez mil miembros en los cincuenta estados de EE.UU. y en más de 30 países entre los que se encuentra España. La organización opera a través de internet y lográ sus campañas mediante las donaciones y el esfuerzo de sus miembros. La organización CASPIAN pretende frenar la implantación de los sistemas RFID hasta que la tecnología este lo suficientemente desarrollada para permitir una gestión de la privacidad de manera segura. Hay que destacar que la organización no pretende que la legislación prohíba el uso de las etiquetas RFID sino que los consumidores no las demanden hasta que los riesgos de vulnerabilidad de privacidad queden reducidos al mínimo.

Entre las empresas contra las que la organización ha luchado cabe destacar Benetton, Gillete, etc.

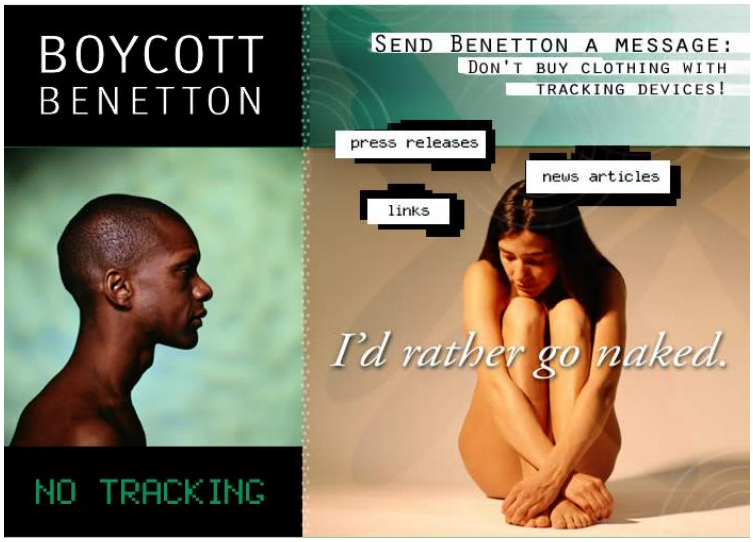


Ilustración 31.-Página en contra de la implantación del sistema RFID en la empresa textil Benetton.

Por su parte, las organizaciones que defienden el uso del sistema RFID afirman que las etiquetas solamente se pueden leer a unos pocos centímetros de distancia a lo que CASPIAN responde que gracias a los avances tecnológicos surgidos en los últimos años muy pronto este rango de lectura aumentará y será posible el seguimiento personal.

En 2006, CASPIAN publica el libro "Spychips" y en 2007 su versión en castellano "Chips Espías" donde los autores relatan los enfrentamientos que han tenido con numerosas empresas (Benetton, Tesco…).

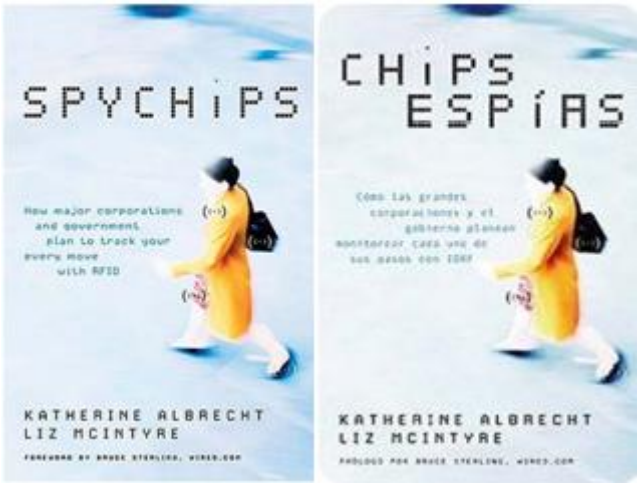


Ilustración 32.-Versión original y española del libro publicado en 2006 por la asociación CASPIAN

El libro contiene además investigaciones sobre el tema así como explicaciones exhaustivas de la tecnología RFID, su historia y el supuesto plan de las empresas para que los chips RFID se encuentren en todos los productos de tal forma que se pueda llegar a vigilar a un usuario sin su consentimiento.

El 20 de Marzo de 2008 se publica un documento titulado "Microchip-Induced Tumors in Laboratory Rodents and Dogs. A Review of the Literature 1990-2006" (Los microchips inducen tumores en roedores y perros de laboratorio) donde la

organización denuncia el comienzo por parte de las empresas de la implantación de los chips RFID bajo la piel de las personas como ya se está haciendo en las mascotas o el ganado.

2.2.7 Problemas para la salud. Cáncer

Según Wired News On-line, y la Associated Press, han surgido artículos de investigación en los últimos diez años, en los que se encuentra una conexión entre el implante de chips y la posible aparición de un cáncer. Cuando a los ratones les fueron inyectadas cápsulas de vidrio que contenían transpondedores RFID, como los desarrollados por PositiveID (VeriChip), se observó que "aparecia un desarrollo maligno, de crecimiento rápido y letal de cáncer, hasta en un 1% al 10% de los casos" en el lugar en que el microchip se inyecta o al que había emigrado. Sin embargo, dicen que el 10% se obtuvo con 'hemizygous', ratones con deficiencia de p53, la equivalencia de las personas que presentan el síndrome de Li-Fraumeni, y que las tasas de cerca de 1% son más típicas. El fabricante deVeriChip (actualmente PositiveID) respondió a este informe, que provocó una caida del 40 % de su valor en bolsa, al afirmar que de los roedores se proporcionaron también datos a la FDA, pero no guardan relación con el implante en los seres humanos o los animales domésticos; esto es fácilmente demostrable, pues son millones los gatos y perros qué, obligatoriamente por Ley en muchos países, no pueden venderse sin estar dotados de un microchip implantado, y no por ello desarrollan cáncer. Como lo demuestra la publicación de sólo dos casos aislados de cáncer detectados de la gran cantidad de perros y gatos sometidos a la implantación de chips. La aclaración a esta cuestión puede verse obstaculizada por el largo retraso en la aparición de efectos raros, como ya ha ocurrido en el caso de controversias con respecto a otros objetos extraños, como la acaecida con los implantes mamarios, o el riesgo de no profesionales al exponerse al amianto.

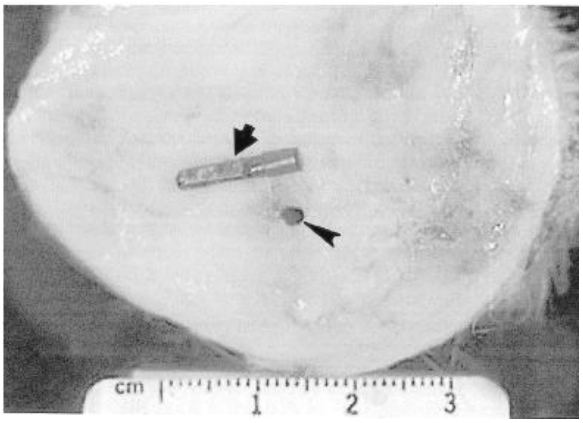


Ilustración 33.-Aspecto macroscópico de un microchip asociado a tumor. El chip (flecha) se ha retirado de la cavidad donde residía in-situ (punta de flecha). *"Experimental and Toxicologic Pathology52 (2001); 483-491"*

2.3 Identificación biométrica

En los últimos años han irrumpido en la escena de la autoidentificación las tecnologías biométricas.

Éstas emplean datos obtenidos de parametrizaciones de distintos elementos del cuerpo humano (iris, huella dactilar, palma de la mano), que se traducen en elementos identificadores únicos de un individuo.

Ilustración 34.-Análisis del iris como identificación biométrica

Los diferentes algoritmos de parametrización empleados por cada fabricante unidos a la naturaleza de los datos biométricos de origen, hacen enormemente difícil falsificar un elemento identificador de estas características.

Aunque existen dispositivos biométricos de muy diversos tipos son los basados en huella dactilar aquellos que más auge han tenido en los últimos años.

Para que estos sistemas se implanten y se utilicen de forma regular, es necesario que cuenten con la confianza de los usuarios. Ello implica que el sistema debe considerar aspectos como:

Probabilidad de fallos (falsos rechazos y falsas aceptaciones).

La probabilidad de falsa aceptación (FAR) (Torrealba) representa la probabilidad de que un individuo no autorizado pueda acceder y la probabilidad de falso

rechazo (FRR) incide en la frecuencia en que los usuarios legales son rechazados y por tanto deben repetir el intento de verificación. La FAR deber ser suficientemente baja, en un rango que suele establecerse, entre el 0,0001% y el 0,1%. Por ejemplo, en el 60% de las centrales nucleares de EE.UU se emplean lectores con la geometría de mano con una FAR de 0,1%. Se debe tener en cuenta que la tasa real de entradas no autorizadas es el producto de la FAR por la probabilidad de que un sujeto no autorizado alcance el dispositivo de control e intente el acceso.

Estabilidad, o robustez del sistema a cambios (normales) en la característica biométrica que mide. Se refiere, por ejemplo, a cambios en el timbre de voz por un catarro, o a cambios en las características de las manos o de la cara debidas por ejemplo a heridas, etc.

Comodidad y facilidad de uso del sistema por parte de los usuarios.
Invasividad.

Aceptación de los usuarios de que sus **datos biométricos no** serán **accesibles** por terceros.

Posibilidad de **engañar al sistema**, obteniendo autorización suplantando una identidad verdadera, es decir, suplantando una característica biométrica.

La tabla 4.2 resume de una forma cualitativa los parámetros que pueden resultar de interés en la aceptación, implantación y uso de los sistemas biométricos.

	Huella dactilar	Iris	Forma mano	Retina	Voz	Facial	Vein pattern
Seguridad	+++	++++	+++	++++	++	+++	++++
Velocidad	+++	+++	+++	+++	+++	+++	++++
Estabilidad	+++	+++	++	+	++	++	+++
Comodidad	+++	++	+++	+	+++	+++	+++
Aceptación	++	++	+++	++	+++	++	+++

Tabla 8.-Resumen de características de los diferentes sistemas biométricos

El funcionamiento de un sistema biométrico sigue fundamentalmente dos pasos que se describen a continuación: ()

El primer paso es el del registro de la persona en el sistema. Durante este proceso el sistema captura un rasgo característico del individuo como por ejemplo una huella digital. Mediante su procesamiento se crea un modelo de referencia que se almacena en una base de datos o en una tarjeta inteligente.

Aunque es poco probable obtener dos muestras iguales de un mismo individuo debido a entre otros factores diferencias ambientales u otras condiciones en el momento de la captura el sistema funciona correctamente debido a que la mayoría de los algoritmos de comparación cotejan los datos en base a determinados umbrales antes de ser aceptados o rechazados. Dependiendo de la tecnología biométrica utilizada y del proveedor se configura el falso rechazo o la falsa aceptación de forma diferente.

El segundo paso depende de si la función del sistema biométrico es la de verificar la identidad de la persona o la de identificar a la persona.

Si se trata de **verificar** la identidad de una persona ésta debe informar al sistema cuál es su identidad mediante la presentación de una tarjeta o mediante un código personal. El sistema captura el rasgo biométrico característico de la persona y lo procesa creando una representación electrónica que comparará con el modelo de referencia del individuo. Si ambos modelos parean la verificación es exitosa, en caso contrario es fallida.

En el caso de **identificación,** la persona no informa al sistema biométrico acerca de su identidad sino que es el sistema el que captura el rasgo característico del individuo y lo compara con un conjunto de modelos de referencia para determinar la identidad de la persona. A partir de este momento y dependiendo de la función del sistema la identificación, la identificación puede ser **positiva** cuando se busca que la identidad de la persona este registrada en el sistema o **negativa** si se busca que el rasgo biométrico no se encuentre registrado en la base de datos.

2.3.1 Seguridad

Dado que los sistemas biométricos analizan una característica propia del individuo, éste es el método más seguro de todos los sistemas de auto-identificación dado el carácter irremplazable e insustituible de los elementos de reconocimiento.

Dentro de los sistemas biométricos aquellos que se pueden considerar más seguros son los sistemas de auto-identificación mediante iris y retina dado que muy difícilmente infalsificables, y dado que los tejidos oculares albergan la característica de que se degeneran muy rápidamente una vez que el individuo ha fallecido la posible utilización de un ojo de una persona fallecida se hace prácticamente inviable y tienen las menores tasas de FAR y FRR.

Las nuevas tecnologías que están saliendo actualmente al mercado también ofrecen grandes tasas de seguridad como es el caso del reconocimiento facial y del mapa vascular que se explican más adelante.

2.3.2 Identificación biométrica con huellas dactilares

Los patrones de huellas digitales están divididos en 4 tipos principales, todos ellos matemáticamente detectables. Esta clasificación es útil al momento de la verificación en la identificación electrónica, ya que el sistema sólo busca en la base de datos del grupo correspondiente ().

Ilustración 35.-Patrones de huellas digitales

En la figura 4.8, aparecen puntos característicos que hay en un dedo, éstos se repiten indistintamente para formar entre 60 y 120 (por ejemplo 10 orquillas 12 empalmes 15 islotes, etc) A estos puntos también se llaman minutae, o minucias, término utilizado en la medicina forense que significa “punto característico”

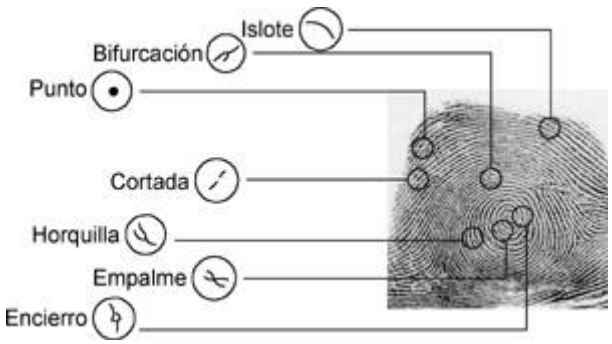


Ilustración 36.-Puntos característicos

Con este conjunto de puntos, el software biométrico de huella digital genera un modelo en dos dimensiones, según se muestra en el ejemplo, mismo que se almacena

en una base de datos, con la debida referencia de la persona que ha sido objeto del estudio. Para ello, la ubicación de cada punto característico o minucia se representa mediante una combinación de números (x, y) dentro de un plano cartesiano, los cuales sirven como base para crear un conjunto de vectores que se obtienen al unir las minucias entre sí mediante rectas cuyo ángulo y dirección generan el trazo de un prisma de configuración única e irrepetible. Para llevar a cabo el proceso inverso o verificación dactilar, se utilizan estos mismos vectores, no imágenes.

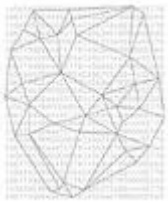
			
El dedo es leído por un captor de huellas.	El dedo es codificado por el captor.	Una plantilla es generada y la imagen es comprimida en formato WSQ (opcional).	El captor guarda y reconoce un conjunto de números que solo podrán ser reconocidos como una plantilla.

Ilustración 37.-Modelo de dos dimensiones generado por el software

Para la identificación de huellas, es conveniente contar con la traza digital completa, no obstante, pueden ser utilizarse fracciones de las mismas, con el inconveniente de que mientras más pequeño sea el marcado, menor es el margen de seguridad.

En el momento de la bioidentificación, el sistema debe asegurarse de que la persona es la que dice ser. Para ello chequea si los datos de la persona a identificar, corresponden con los guardados en una base de datos.

Este es el proceso de autenticación, es más técnico que el anterior, ya que incluye varias comparaciones con aquellas huellas que le sean similares, contenidas en muchas bases de datos, con el fin de poder diferenciarlas. Para ello compara la huella que la persona registra en un scaner óptico, con aquella registrada previamente. Cabe señalar que si el sistema usa las huellas digitales de los índices de ambas manos, ofrecerá un mayor margen de seguridad.

La identificación biométrica por medio de huellas digitales tiene un grado de seguridad tan alto debido a que nadie podría sustraer, copiar o reproducir los elementos usados

en ella, ya que son elementos inherentes a su portador, sin embargo puede estar sujeta a errores de falsa aceptación y falso rechazo.

Las aplicaciones se dan en dos ámbitos:

Criminal

Los archivos criminales compuestos por 10 huellas rodadas (Completas).

Civil

Maneja de 2 a 10 huellas y puede ser usado en:

- ✓ En el gobierno para Sistemas de registro de población, emisión de: credencial de identidad, seguro social, licencias; Migración, aduana y pasaportes; Licencias y control de vehículos; Registro y procesos electorales; Banca, Hacienda y Finanzas
- ✓ En la iniciativa privada permite el control de empleados, procesamiento de Nómina.
- ✓ Control de acceso a áreas restringidas.

En varios países, como Estados Unidos, Malasia, Nigeria, Libano, Hong Kong el sistema es un instrumento utilizado como una forma de pago, sustituyendo a la tarjeta de crédito o débito por el dedo de la persona, mismo que sería casi imposible de perder y difícil de robar o duplicar.

Como aplicación dentro del ámbito regional destaca la noticia publicada en la Voz de Asturias (García, 2010) donde se informa que el Principado ha puesto en marcha desde el 4 de mayo de 2010 el sistema de huella digital para controlar el horario del personal de los funcionarios de Justicia. Alrededor de 1.300 trabajadores de la administración pasan todos los días el control dactilar que permite a la consejería controlar, por un lado, que cumplan las horas y por otro, para mejorar la seguridad en los juzgados y los edificios adscritos a esta administración.

Ilustración 38.-Funcionario fichando en los juzgados de Oviedo. Foto: Armando Álvarez

No obstante, la seguridad atribuida a los sistemas de huella dactilar está muy lejos de ser cierta. Uno de los principales problemas es que de forma continua las personas dejan sus huellas dactilares marcadas en los diferentes sitios que tocan (mesas, bolígrafos, vasos, etc.). Su identidad queda por tanto "disponible" para ser reproducida y con la suficiente destreza utilizada para robársela falseando un lector de huella dactilar utilizando dedos de silicona. (Impact of Artificial "Gummy" fingers on fingerprint systems, 2002)

2.3.3 Identificación mediante el iris

El reconocimiento por iris (Marcelo Davila Vargas) se basa en los detalles que presenta la textura del iris, que por características inherentes a su morfología presenta grietas, criptas y estrías entre otros detalles. Esta textura formada durante la etapa embrionaria es estocástica y determina que el fenotipo de dos iris con el mismo genotipo conjunto tal como gemelos idénticos y siameses presenta detalles no correlacionados. Los patrones formados seguirán siendo los mismos durante toda la vida de la persona.

Ilustración 39.-Reconocimiento mediante iris

El desarrollo de la tecnología de identificación por reconocimiento de iris ha venido marcado por los siguientes hitos:

- **1936** - Oftalmólogo Frank Burch – Primero en ***proponer*** uso del iris.
- **1987** – Oftalmólogos Aran Safir y Leonar Flom ***patentan*** la idea de usar los iris para identificación.
- **1991 –** John Daugman escribe los ***algoritmos***.

- **1995** – IriScan hace un prototipo para el ***ejército*** americano.

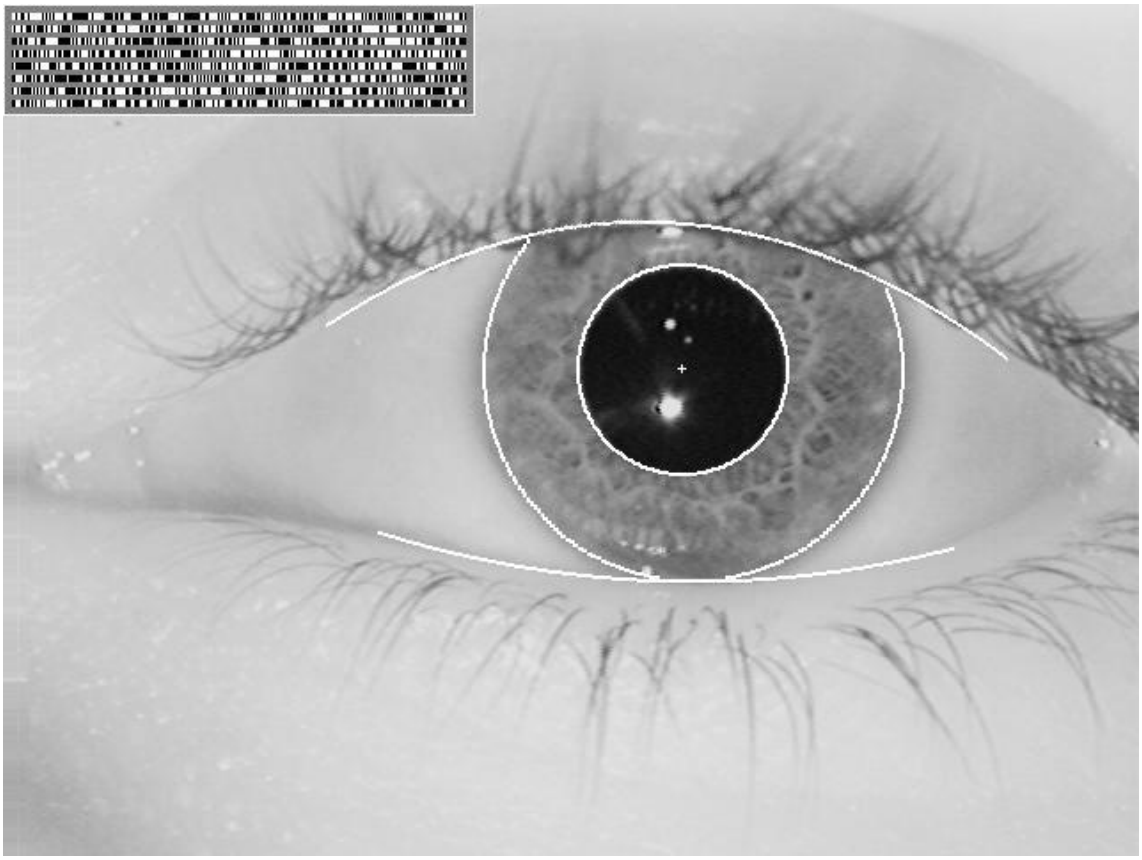


Ilustración 40.- Iriscode mostrado gráficamente junto al ojo correspondiente, de la web de John Daugman, Universidad de Cambridge. (Boulat, 2002)

En la actualidad se utiliza con frecuencia en instalaciones con altos requisitos de seguridad.

Es tal la información presente en el iris de un individuo que permite su identificación mediante procedimientos no invasivos y que se desarrollan a distancias prudenciales, sin restricciones ambientales y con patrones que son fáciles de capturar y codificar.

Además, los tejidos oculares albergan la característica de que se degeneran muy rápidamente una vez que el individuo ha fallecido por lo que la posible utilización de un ojo de una persona fallecida se hace prácticamente inviable.

Su éxito proviene del desarrollo por parte de John Daugman, (Dougman) que concibió un algoritmo matemático que permite con una gran eficiencia en la utilización de recursos de proceso caracterizar el iris de un individuo con un nivel de detalle suficiente para distinguirlo de cualquier otro.

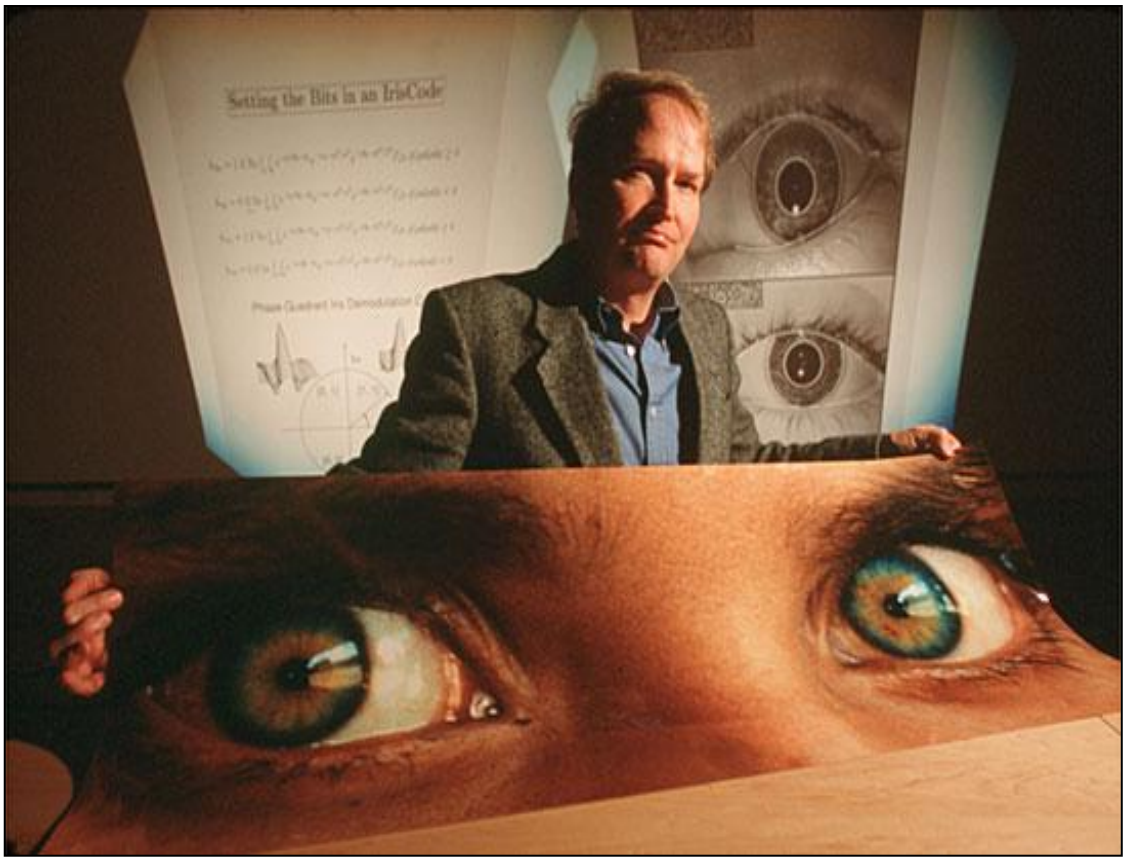


Ilustración 41.- Fotografía de John Daugman en su trabajo para National Geographic con objeto de la localización de la niña afgana de la portada de la revista en 1985.

Su tasa de falsa aceptación (FAR) es muy baja de 1/1200000 lo que hace al sistema ideal para aplicaciones de alta seguridad () y la eficiencia del algoritmo de Dougman permite una altísima velocidad de identificación.

2.3.4 Identificación biométrica por la forma de la mano

Estos sistemas obtienen una imagen del perfil de la mano completa, de dos dedos o de un solo dedo, con una cámara convencional o con una cámara infrarroja. Una vez tomada la imagen se extraen una serie de características de la mano y los dedos, como pueden ser longitudes, anchuras, alturas, posiciones relativas de dedos, articulaciones, disposición de venas, etc. Esas características se transforman en una serie de patrones numéricos, que luego se comparan con los patrones previamente almacenados.

Ilustración 42.-Lector biométrico según forma de la mano

Uno de los primeros usos de este sistema fue en los juegos olímpicos de 1996. También se está empezando a utilizar como alternativa al número de identificación personal en operaciones con tarjetas de crédito.

Los sistemas comerciales presentan tasas típicas de falso rechazo en torno al 0.1 % y de falsa aceptación en torno al 1%.

2.3.5 Patrones de Venas de la Retina

En esta técnica se examina el fondo del ojo y se detectan los patrones de venas que se extienden por la retina. Son también característicos y estables en cada individuo, y permiten diferenciar unos individuos de otros.

En los sistemas biométricos basados en patrones de vasos de la retina, el usuario mira a través de unos binoculares, realiza algunos ajustes, mira a un punto determinado y por último pulsa un botón. El sistema toma una imagen de la retina con una radiación infrarroja segura, de baja intensidad, detectando la estructura de vasos sanguíneos de la retina y transformándola en una serie de características numéricas para compararlas con las almacenadas (Portillo, 2003).

Como principal ventaja se puede citar su precisión y eficacia. Es el mejor método con menor tasa de FRR y FAR (Pérez Cortés). Los patrones de la retina son rasgos personales muy distintivos de cada individuo por lo que serán diferentes incluso en hermanos gemelos como ocurría con el iris del ojo. No obstante y aunque estos rasgos se mantengan normalmente durante toda la vida del individuo, se pueden ver afectados por enfermedades tales como el glaucoma o la diabetes.

El principal inconveniente de esta técnica estriba en lo invasiva que resulta para la persona pues debe posicionarse muy cerca del dispositivo, permanecer inmóvil y mirar de manera directa a la luz que escaneará la retina durante aproximadamente 10 o 15 segundos. Además el usuario deberá quitarse las gafas o las lentillas para que la lectura sea satisfactoria.

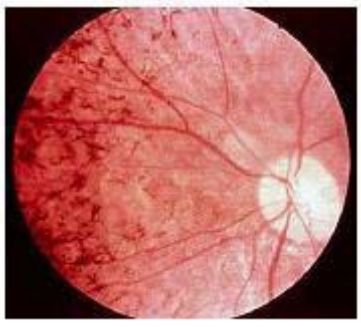


Ilustración 43.-Fondo del ojo

Su coste es elevado y su potencial peligrosidad compromete la necesidad de revisiones y mantenimientos periódicos no críticos en otros sistemas.

2.3.6 Reconocimiento por voz

En este sistema se adquiere la voz del usuario utilizando un micrófono, y seguidamente se analiza mediante un ordenador. Se buscan principalmente patrones de intensidad y frecuencia.

Existen dos tipos principales:

• De **texto dependiente**, en los que el reconocimiento se basa en un conjunto muy limitado de frases estándar.

• De **texto independiente**, en los que la variedad de frases es mucho más amplia. De hecho el sistema va proponiendo al usuario que diga varias palabras extraídas de un conjunto bastante grande.

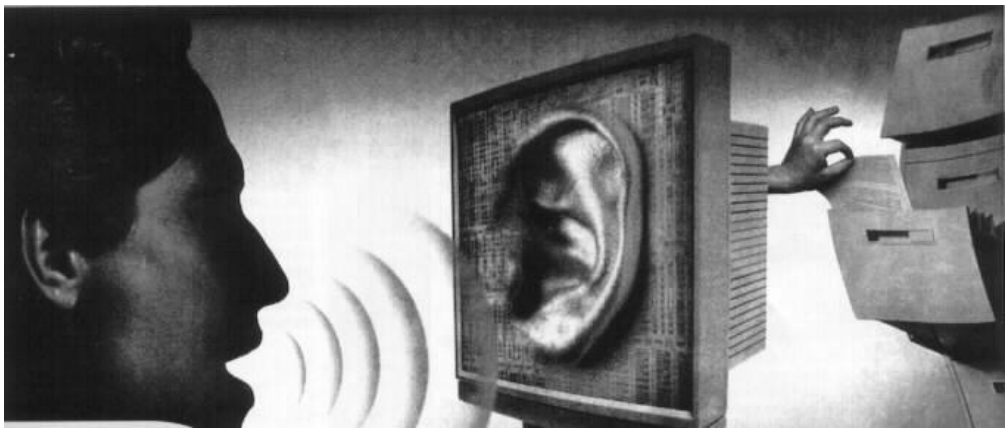


Ilustración 44.-Identificación mediante voz

Se trata de un sistema poco costoso de implementar, por lo que se encuentra muy extendido. Sin embargo, uno de los problemas que frenan su difusión es que se trata de una tecnología todavía propensa a errores. La probabilidad de falso rechazo está en torno al 3%, y la de falsa aceptación, en valores algo superiores al 1%.

2.3.7 Reconocimiento Facial

Este sistema de reconocimiento biométrico se basa en identificar las áreas de la cara menos susceptibles a mostrar cambios a corto plazo como puede ser los pómulos, boca o las cuencas de los ojos (Ross).

La detección se realiza mediante cámaras de video que no requieren contacto con el usuario el cual está familiarizado con esta tecnología y goza de gran aceptación. Por otra parte dado el carácter independiente del lector y el usuario éste puede ser utilizado sin el consentimiento del usuario aunque esto trae consigo implicaciones de privacidad.

Como principales desventajas se puede citar que el sistema es sensible a la iluminación donde se realiza la detección, se debe tener una buena visión de la cara en el campo de imagen. No obstante lo anterior existen dispositivos basados en captura infrarroja que presentan una menor sensibilidad a cambios de iluminación.

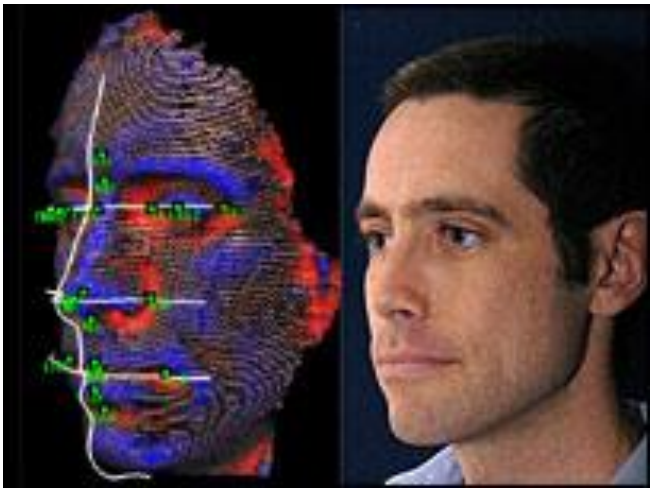


Ilustración 45.-Reconocimiento facial

Existen sistemas operativos en el mercado, que aseguran una probabilidad de reconocimiento correcto altísimo.

Algunas de las técnicas utilizadas en la auto-identificación biométrica son las siguientes:

Automatic face processing: Utiliza las distancias y proporciones entre los rasgos faciales comunes. Esta es la técnica más sencilla. Entre sus principales ventajas cabe

destacar su simplicidad y que el defecto de iluminación no le afecta en exceso. De reciente aparición, los dispositivos con doble cámara de infrarrojos permiten la parametrización en tres dimensiones del rostro del individuo consiguiendo una rapidez y precisión muy altas con costes muy asequibles (FAR:< 0.0001%).

Neural Network processing: Se utiliza una red neuronal para determinar si los rasgos faciales son lo bastante similares con los patrones de rasgos faciales almacenados en el sistema. Teóricamente posee una gran capacidad de adaptarse a los cambios.

Eigenfaces: Se utilizan imágenes en escala de grises que representan las características de un rostro.

Local Feature Analysis: Esta técnica hace uso de muchas pequeñas características del rostro y su situación local para construir un patrón.

2.3.8 Mapa vascular dactilar

La autentificación mediante el uso de los patrones de las venas de los dedos para uso de identificación personal es un método biométrico de reciente utilización (Finger Vein Authentication: White Paper).

Los patrones de las venas son diferentes para cada uno de los dedos de la mano y para cada persona y como están ocultos debajo de la superficie de la piel, la falsificación es prácticamente imposible.

El principio básico del sistema se basa en los rayos infrarrojos generados a partir de diodos emisores de luz. Los rayos infrarrojos penetran en el dedo y son absorbidos por la hemoglobina en la sangre. Las áreas en las que se absorben los rayos (es decir, las venas) aparecen como áreas oscuras de una imagen tomada por un cámara CCD situada en el lado opuesto del dedo. Mediante el procesamiento de imágenes se puede construir un patrón de venas de los dedos con la imagen de la cámara. Este patrón es comprimido y digitalizado para que pueda ser registrado como una plantilla de datos de autentificación biométrica de una persona.

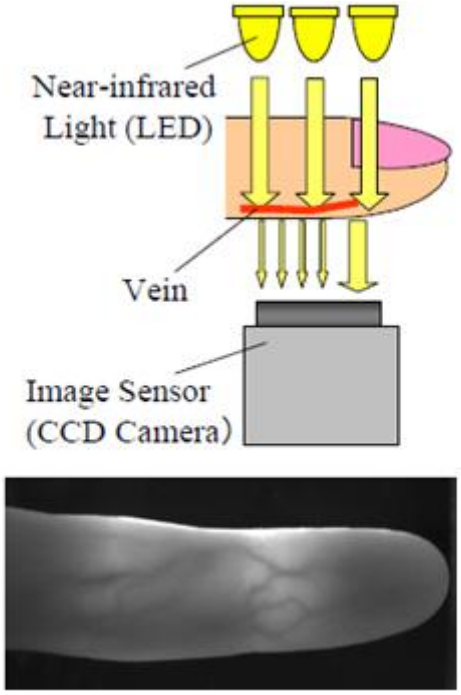


Ilustración 46.-Imagen obtenida mediante el procedimiento

Entre las características de este método destaca su alta precisión, la exactitud de la autentificación es menos del 0,01% para la FRR (Tasa de Falso Rechazo), y menos de la 0,0001% de las FAR (Tasa de Falsa Aceptación). Además el uso de la luz infrarroja asegura comodidad y limpieza para el usuario.

La facilidad de extracción de características de las venas de los dedos es relativamente estable y pueden ser fácilmente capturadas, lo que permite el uso de cámaras de baja resolución para tomar imágenes.

Además, la velocidad de la autentificación es rápida, menos de un segundo. Por otra parte, el dispositivo puede ser compacto, debido al pequeño tamaño de los dedos.

2.3.9 Mapa vascular de la palma de la mano

El sistema de identificación mediante las venas de la mano es al igual que el finger vein un sistema novedoso.

El sistema se basa en la autentificación del individuo utilizando los patrones de los vasos sanguíneos de la palma de la mano (Masaki Watanabe, 2005). En comparación con un dedo o el dorso de una mano, la palma tiene un sistema más amplio y complejo de patrones de venas lo que permite obtener gran cantidad de aspectos diferenciadores de un individuo a otro. Además es una zona que normalmente no posee vello y es menos susceptible de cambiar de color por lo que la fotografía del patrón vascular resulta más fácil.

La hemoglobina de los vasos sanguíneos absorben la luz con una longitud de onda de alrededor de 7.6x10-4mm dentro del área de infrarrojo. Cuando la imagen de rayos infrarrojos es capturada, sólo el patrón de vasos sanguíneos que contiene la hemoglobina desoxidada es visible como una serie de líneas oscuras. En base a esto el sistema traduce las líneas negras de la imagen de rayos infrarrojos como el patrón de vasos sanguíneos que luego hará coincidir con el patrón de vasos sanguíneos previamente registrado del individuo.

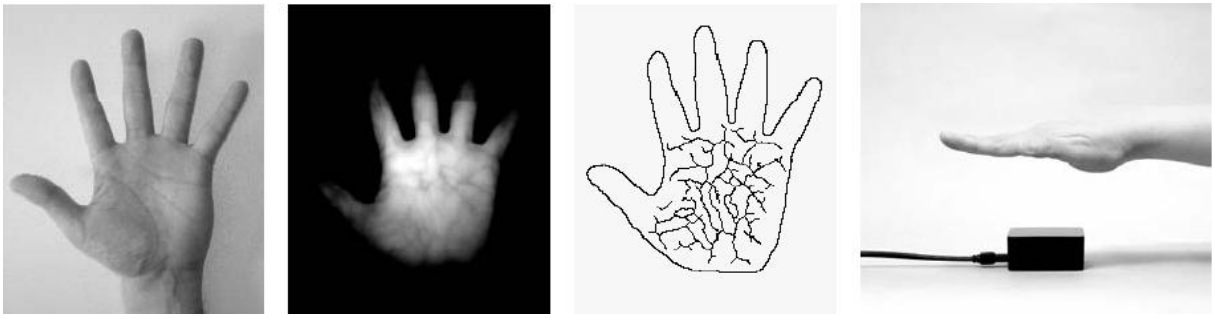


Ilustración 47.-Fotografía de la palma de la mano, imagen de rayos infrarrojos, patrón de venas y sensor respectivamente

El sensor es capaz de capturar la imagen de la palma de la mano independientemente de la posición y movimiento de la palma y permite su aplicación sin el contacto con el

usuario lo que lo caracteriza como un sistema higiénico y no invasivo de amplia aceptación por parte del usuario debido a estas características.

La información de las venas es prácticamente imposible de duplicar dado que permanecen en el interior de las manos del individuo. Además su nivel de precisión es elevado pues ofrece un falso rechazo (FRR) de 0,01% y una tasa de falsa aceptación (FAR) del 0,00008%.

2.4 Sistemas de auto-identificación aplicados a personas

A través de este apartado se pretende profundizar en las tecnologías de auto-identificación aplicadas a la identificación personal. Se realiza una descripción de las diferentes formas que tienen las personas de identificarse y se analiza las distintas tecnologías asociadas a este campo. Se realiza así mismo una comparativa entre todas ellas.

2.4.1 Identificación personal

De forma genérica, puede sintetizarse que existen tres formas de identificar a alguien:

- ✓ por lo que tiene (una ficha, una tarjeta, etc)
- ✓ por lo que sabe (una contraseña)
- ✓ por lo que es (un aspecto biométrico).

Dentro de la auto-identificación personal realizada mediante un elemento que la persona posee, éste puede tener alguna de las siguientes tecnologías:

- ✓ Código de barras
- ✓ Banda magnética
- ✓ Tarjeta chip
- ✓ Botones de memoria de contacto
- ✓ Tecnología RFID
- ✓ Identificación biométrica.

A continuación se analizarán las diversas tecnologías aplicadas a la identificación personal. Se explicarán la mayoría tomando como soporte una tarjeta, aunque algunas tecnologías.

2.4.2 Tecnologías de auto-identificación personal

2.4.2.1 Tarjeta de Código de barras

Las tarjetas de código de barras son de apariencia similar a la magnética, pero en lugar de la banda, llevan impreso un código de barras. La ventaja de esta tarjeta es que al pasarla por el lector, no existe rozamiento con un cabezal, sólo con un haz de luz que lee el código, por lo que su vida útil es levemente mayor.

El mayor inconveniente que poseen este tipo de tarjetas es que se se pueden rayar fácilmente alterando e incluso haciendo ilegible el código por lo que se obliga el recambio de la tarjeta.Al mismo tiempo la posibilidad de duplicación de la tarjeta por métodos de fácil acceso como la fotocopiadora, disminuyen notablemente su nivel de seguridad.

El costo de las tarjetas es similar al de las magnéticas. Los lectores que se utilizan en los equipos de Control de Acceso y Control de Tiempo y Asistencia pueden ser de diferentes calidades y prestaciones.

Los equipos más avanzados utilizan lectores que leen todos los códigos posibles, permitiendo el uso de tarjetas con códigos UPC, 2 de 5, 3 de 9, etc., en cambio los más económicos sólo leen uno de esos códigos, perdiendo versatilidad.

2.4.2.2 Tarjetas con contacto

Las tarjetas con contacto constituyen el medio más tradicional de identificación. Se basan en la utilización de tarjetas plásticas con tecnología de banda magnética o tarjeta de chip. Ambos elementos identificadores han de ser introducidos en un lector de tarjetas para que el fichaje del individuo se haga efectivo. Ha de existir contacto físico entre la tarjeta y el dispositivo lector.

2.4.2.2.1 Tarjeta de banda magnética

Las tarjetas magnéticas están formadas por un soporte de plástico y una banda magnética para almacenar los datos, cumpliendo la norma ISO 7811, que especifica el tamaño, el grosor, las pistas, etc. Aunque también existen otros formatos y soportes para bandas magnéticas no normalizadas, la descripción que se realizará de las tarjetas en este apartado se basa solamente a la ISO 7811 (Mayné, 2009)

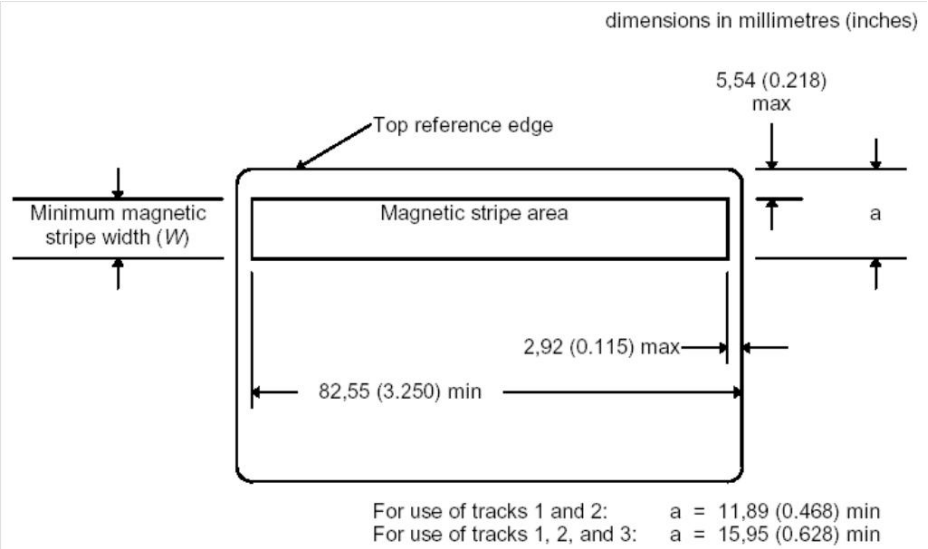


Ilustración 48.-Tamaño de la tarjeta magnética

Tipos de tarjetas magnéticas

Existen tres tipos de tarjetas, de una, dos, o tres pistas. Las características de todas ellas se muestran en la tabla 4.1

	Pista 1	Pista 2	Pista 3
Cantidad de datos	Máx 79 caract.	Máx 40 caract.	Máx. 107 caract.
Codificación de datos	6 bit alfanuméricos	4 bits BCD	4 bits BCD
Densidad de datos	8,3 bits/mm	3 bits/mm	8,3 bits/mm
Escritura	No permitida	No permitida	Permitida

Tabla 9.-Tipos de tarjeta magnética

Tipos de lectores de tarjetas magnéticas

Existe una gran variedad de lectores de tarjetas magnéticas. Si bien en relación al coste el lector resulta económico, posee el inconveniente de que el cabezal de lectura sufre cierto desgaste (ralladuras, suciedad...) con su uso y a medida que el cabezal se va dañando su superficie se vuelve más abrasiva y dañina para la banda magnética de la tarjeta con lo que el sistema termina degradándose hasta que el cambio resulta necesario.

Entre las ventajas de las tarjetas de banda magnética están su difusión, popularidad y bajo coste, pero en sí es, de todos los medios de identificación, el más vulnerable. Su banda magnética debe ser tratada con cierto cuidado, para evitar que se raye o sea expuesta a campos magnéticos que la borren. Por ese motivo no son recomendables para usar en ambientes industriales.

El tiempo de vida del sistema depende exclusivamente del ambiente, frecuencia de uso y el trato con el que se utilice. El promedio de vida útil está entre los 9 meses y 3 años aproximadamente.

Ilustración 49.-Tarjetas de banda magnética

2.4.2.2.2 Tarjetas de chip

Las tarjetas Chip se inventaron en Europa en 1970 y su uso principal fue la manera más fácil y económica de hacer la verificación de una transacción monetaria fuera de línea, debido al alto costo de las telecomunicaciones a través de Europa. En cambio en Estados Unidos la implantación de este tipo de tarjeta ha sido más lenta, debido a la gran implantación de tarjetas magnéticas y consecuentemente la gran cantidad de lectores instalados en el mercado. Las tarjetas Chip han mejorado en gran parte las aplicaciones de las tarjetas magnéticas. Permiten almacenar mayor información y mantienen mayor seguridad de la integridad de los datos.

Existen dos tipos de tarjetas chip:

Tarjetas Memoria
Tarjetas Memoria y Microcontrolador

Tarjetas Chip con Memoria

Las tarjetas con memoria pueden ser OTP (Grabable una sola vez) o Eeprom (regrabable muchísimas veces). Además pueden contener una circuitería lógica de seguridad o no. Esto quiere decir que el acceso a la memoria está controlada por una circuitería lógica de seguridad, que puede consistir en la protección de escritura o lectura de la memoria o en algunas partes de ella. Sin embargo, hay también algunas memorias con una circuitería lógica de seguridad más compleja, la encriptación de datos.

Tarjetas Chip con Memoria y Microcontrolador

Las tarjetas con memoria y un microprocesador, pueden almacenar cantidades masivas de información, además el microprocesador capacita a la tarjeta para tomar sus propias decisiones sin importar la información almacenada.

Las tarjetas chip están normalizadas bajo la ISO7816 tanto desde el punto de vista mecánico (los contactos), y la interfaz de comunicación. Existen una serie de receptáculos para la acomodación de las tarjetas para su lectura, que permiten mecánicamente conectar con cualquier tipo de tarjeta, tal como las que se muestran en la figura posterior.

Ilustración 50.-Distintos tipos de receptáculos para los chips

2.4.2.3 Tarjetas con tecnología RFID

Las tarjetas sin contacto constituyen un medio más avanzado de identificación. Generalmente el elemento identificador es una tarjeta plástica similar a las tarjetas de banda magnética, sin embargo, para realizar un fichaje no es necesario introducir la tarjeta en ningún lector. Basta con acercar la tarjeta a la zona de influencia del dispositivo receptor para que la identificación quede registrada.

Tarjetas de proximidad

De las distintas tecnologías de identificación por tarjetas, las de proximidad se han tornado en la opción cuya relación costo-beneficio es, para el común de los casos, la más adecuada. Esto se debe principalmente a su costo medio (tanto del lector como de las tarjetas), su alta robustez y duración, y la multiplicidad de aplicaciones que posee.

Existen dos tipos de tecnología asociada a las tarjetas sin contacto o de proximidad, la tecnología RFID de 125KHz y la tecnología Mifare. Ambas se basan en el mismo principio de comunicación por radiofrecuencia siendo la principal diferencia que las tarjetas Mifare pueden ser leídas y escritas mientras que las RFID de 125KHz, por regla general, sólo pueden ser leídas.

La tecnología RFID, por su diseño tecnológico, no puede ser duplicada. Permite utilizar tarjetas o llaveros de proximidad pasivos. La tarjeta no tiene rozamiento (se comunica con el equipo por radio frecuencia), por lo cual no se desgasta.

Hoy en día es una de las tecnologías más modernas y efectiva, por su practicidad y bajo coste de mantenimiento.

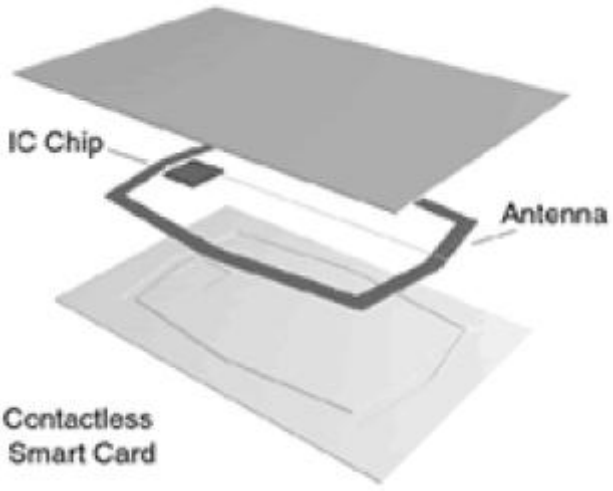


Ilustración 51.-Tarjeta con dispositivo RFID

Ilustración 52.-Tarjeta ciudadana de Gijón

Por otro lado, si además se desea almacenar información personal de un empleado en su tarjeta identificadora, la opción Mifare sería la elección ideal.

Los elementos identificadores sin contacto no se distribuyen exclusivamente en forma de tarjetas plásticas, sino que existen también como “tokens” de identificación que pueden ser utilizados en vehículos, de manera que un empleado realice el fichaje al entrar al garaje con su vehículo, sin necesidad de presentarse ante un dispositivo identificador.

Un sistema de tarjeta inteligente, Smart Card, sin contacto (ISO 14443A), se comunica con otros dispositivos sin la necesidad de contacto físico alguno, y lo hace a través de la tecnología RFID, la tarjeta pasiva es activada por el lector para realizar la transferencia de datos. Las implementaciones de estos sistemas en e-pasaportes, medios de pago electrónico y tarjetas de acceso físico, está incrementándose día a día. Es por ello que la seguridad de estas aplicaciones es claramente crítica. Sin embargo, existen puntos a favor como son su corto rango de operación, entre los 5 y 10 centímetros, según la ISO 14443A, ya que al tratarse de una etiqueta pasiva el rango es muy corto, y la comunicación entre un extremo y otro va cifrada.

Tarjeta RFID largo alcance

Las tarjetas RFID de largo alcance permiten ser leídas a cierta distancia sin necesidad de tener que acercar la tarjeta a un lector. De esta forma la manera de auto-identificarse resulta más cómoda para el usuario.

Además el sistema es capaz de leer múltiples tags de manera simultánea de tal forma que ante gran afluencia de personas, éstas pueden quedar registradas de manera simultánea.

Por otra parte el coste del sistema aumenta respecto a las tarjetas de proximidad.

2.4.2.4 Botones de memoria de contacto

Son encapsulados metálicos sumamente robustos, que cuentan en su interior con un chip de identificación único e irrepetible, característica asegurada por su único fabricante. Esta tecnología es comúnmente utilizada para los Sistemas de Control de Rondas y Recorridos, ya que toleran fácilmente la intemperie. En referencia al Control de Acceso y Asistencia, era usualmente elegido como medio de identificación cuando la cantidad de personal a controlar era baja (aproximadamente hasta 100 personas), ya que si bien su costo por unidad es elevado, el costo del lector para estos dispositivos es sumamente accesible.

En la actualidad, la mayoría de las empresas optan por la proximidad, ya que puede ofrecer un nivel alto de seguridad a precios similares por unidad, con la posibilidad también de agregar identificación a las tarjetas.

2.4.3 Comparativa general de las tecnologías de auto-identificación personal

A continuación se muestra una comparativa de todas las tecnologías de auto-identificación descritas anteriormente. Se ha de tener en cuenta que la comparación se realizará a nivel general:

	Código barras	Banda Magnética	Tarjeta de Chip	Proximidad	Largo alcance	Botones de memoria	Biometría
Seguridad inviolabili-dad	Baja	Media-baja	Media	Alta	Alta	Alta	Muy Alta
Alcance	Visión directa: <1.5 metros	Contacto	Contacto	Pocos cm	Metros	Contacto	Depende del método (cm)
Lecturas simultáneas	1	1	1	1	Múltiples	1	1
Desgaste tarjeta	Medio	Alto	Medio	No posee	No posee	No posee	No posee
Desgaste lector	Bajo	Muy alto	Medio	No posee	No posee	No posee	No posee
Vida útil	Corto	Depende del uso (9 meses-3años)	Depende del uso	Indefinido	Depende de la batería (3-5 años)	Largo	Depende del tipo de sistema. Largo
Precio mantenimien-to	Alto	Alto	Medio	No posee	En ocasiones la batería puede dar problemas	No posee	Bajo
Precio tarjeta	Bajo	Muy bajo	Medio	Medio	Alto	Alto	-
Precio lector	Alto	Bajo	Medio	Medio-bajo	Alto	Muy bajo	Medio-alto
Posibilidad de olvido	Sí	Sí	Sí	Sí	Sí	Sí	No
Posibilidad de intercambio	Sí	Sí	Sí	Sí	Sí	Sí	No

Tabla 10.-Tabla comparativa entre las diferentes tecnologías de auto-identificación personal

2.5 Experiencias en aplicación de las tecnologías de auto-identificación al control de personas

En este apartado se muestran las diversas aplicaciones estudiadas de auto-identificación de personas. Se describen los diferentes casos así como aplicaciones prácticas ya implantadas en la sociedad de las que se ha podido recabar información.

2.5.1 Implantes de RFID en humanos

2.5.1.1 Introducción

Las etiquetas RFID implantables, originalmente diseñadas para su uso en identificación de mascotas y animales están siendo utilizadas de manera progresiva en implantes en seres humanos.

Su perspectiva de futuro es inagotable, una etiqueta RFID implantable bajo la piel podría permitir la exclusión del robo de identidad, acceso a áreas restringidas sin uso de ningún dispositivo identificativo, acceso seguro a un ordenador, identificación segura ante un cajero automático, localización de pacientes con enfermedades mentales y un largo listado de ejemplos relacionado con la auto-identificación segura del individuo sin necesidad de portar nada que pudiera dar lugar a una falsificación o usurpación de identidad. Además, estos dispositivos podrían incorporar sensores y así controlar diversas funciones del cuerpo, como la tensión, la temperatura corporal o los niveles de glucosa provocando un gran avance en el sector de la sanidad.

En 2004, cuando la Administración Federal de Fármacos y Alimentos (FDA) de EE.UU aprobó la implantación de chips RFID en seres humanos, la empresa VeriChip empezó a desarrollar etiquetas RFID implantables. Todos los productos de la marca VeriChip marcados por el logotipo de la figura, en el cual se puede leer 'implantable', representan a las etiquetas RFID que VeriChip fabrica para implantes humanos con el propósito de la identificación automática mediante radio frecuencia.

Ilustración 53.-Logotipo de etiquetas RFID implantables en humanos

2.5.1.2 Empresas comercializadores

La empresa VeriChip es en la actualidad parte de PositiveID Corporation, que es una unidad de Digital Angel que se formó el 10 de noviembre de 2009 a través de la fusión de VeriChip Corporation y del Acero Vault Corporation ().

Ilustración 54.- Logotipo de emrpesa Positive ID

PositiveID representa la convergencia de un pionero en los registros de salud personal y la primera y única empresa habilitada por la FDA para la utilización del microchip implantable en la identificación del paciente.

PositiveID opera en dos divisiones principales: HealthID y la identificación de Seguridad HealthID. Una parte integral de la fundación de PositiveID es la identificación por radiofrecuencia (RFID) de microchips implantables para la identificación del paciente, el VeriChip. El Chip RFID de la compañía se remonta a los acontecimientos del 11 de

septiembre de 2001, cuando los bomberos de Nueva York escribieron su número de tarjeta de identificación en el pecho en caso de que se encontraran heridos o inconscientes. Era evidente que había una gran necesidad de información personal en situaciones de emergencia y el producto, el modelo de un microchip similar utilizado en animales domésticos, evolucionó a partir de allí. La compañía recibió la aprobación de la FDA para el microchip en octubre de 2004.

2.5.1.3 Funcionamiento e implantación en el cuerpo

El dispositivo que se introduce bajo la piel es un dispositivo de radiofrecuencia implantable de unos 12 milímetros por 2,1 milímetros. El Chip contiene un código identificador único de 16 dígitos, es más, el chip en sí no contiene ningún otro dato ni ningún tipo de GPS incorporado (Sistema de Posicionamiento Global) que permita la localización de una persona.

Ilustración 55.- Chip implantable

Este dispositivo permanece en estado de letargo hasta que la energía de radiofrecuencia del escáner llega hasta él y lo activa. Esta energía pasa a través de la piel. Al ser activado, el chip emite una señal de radiofrecuencia que contiene el número de verificación. Este número aparece en el display del escáner, que lo

transmite a una institución autorizada, que tiene una base de datos segura. La transmisión es realizada por personal autorizado vía teléfono o Internet (arjun).

Ilustración 56.-Esquema de funcionamiento de un RFID implantable

La intervención quirúrgica para el implante requiere anestesia local y se puede realizar mediante una jeringuilla. El proceso puede tardar unos 20 minutos y puede ser realizada en forma ambulatoria. Deja una muy pequeña cicatriz y es posible que se requiera de una banda adhesiva.

Ilustración 57.-Oran Barber/Beth Israel Deaconess Medical Center

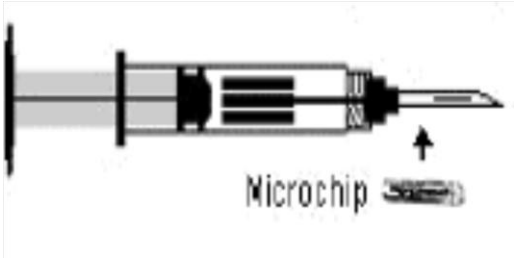


Ilustración 58.-La inserción se realiza mediante jeringuilla

2.5.1.4 Seguridad en implantes de chips RFID

Cualquier persona que posea un lector de VeriChip puede leer los 16 números que contiene el microchip RFID implantado en una persona. Los datos no están cifrados lo cual parece normal, pues para usos en urgencias médicas lo correcto es que no lleve codificación de protección alguna, para permitir su uso inmediato en una emergencia, si el portador se encuentra desmayado o mal herido. Un microchip RFID pasivo, que sólo contenga un único identificador de 16 dígitos, debe poder ser leído por un lector de VeriChip (actual PositiveID) que se acerque al lugar donde este insertado el chip. Los defensores de la privacidad argumentan que en lugar de usarse el sistema de implante inamovible, podría usarse por ejemplo, la inserción en la pulsera de un reloj, que en cualquier caso puede ser quitado, a voluntad del usuario.

Verichip (actual PositiveID) asegura que la base de datos asociada con el dispositivo que actualmente se emplea sólo contiene información relacionada con la salud, sin información financiera o número de seguridad social almacenado en él. Y que la información es conocida y aprobada por la persona que se implanta el microchip.

Precisamente porque es técnicamente posible extraer la información de tal implante, el chip contiene sólo un número de 16 dígitos anodino y aleatorio. Para acceder al registro personal de la salud asociado a su portador, se debe poseer una clave o contraseña de seguridad para el inicio de sesión, que se proporciona únicamente a las instalaciones médicas, y además hay un registro que señala cada vez que se accede al chip y a los registros del implantado.

2.5.1.5 Inconvenientes

A partir del momento en el que los primeros chips se empezaron a implantar en humanos empezó una gran polémica ya que existían estudios científicos de los años 90 que demostraban que estos dispositivos provocaban la aparición de tumores malignos en entre 1 y un 10% de animales de laboratorio en los que se inyectaban. Estos tumores aparecían en el lugar donde se implanta la cápsula que contiene el chip.

Estudios científicos realizados desde el año 1996, han demostrado que la tecnología RFID inyectada en el cuerpo humano en un 1% ha generado sarcomas, o neoplasias malignas que se originan en un tejido conjuntivo como puede ser un hueso, cartílago, grasa, músculo…, y tumores cancerosos en el lugar donde está implantada la cápsula que contiene el chip (Carrasco, 2009).

En el año 2007 la implantación de RFID en humanos se calculaba alrededor de 2000 personas en el mundo, hecho que ha crecido en los últimos años gracias a la publicidad de la empresa VeriChip (actualmente PositiveID Corporation) y a que existe más conocimiento de la existencia de esta tecnología.

Ilustración 59.-Implante RFID en humano

En estas implantaciones no sólo es importante la posibilidad de la aparición de tumores malignos sino también el innegable dilema moral que trae consigo. La vulnerabilidad de la privacidad juega un papel importante sin obviar que en

determinadas ocasiones el paciente puede verse obligado a tener un implante como medio por ejemplo de poder trabajar en un determinado puesto.

2.5.1.6 Aplicaciones prácticas

2.5.1.6.1 Discotecas

Una discoteca de Barcelona llamada Baja Beach Club, ha sido la primera en el mundo en 2004 en implantar este sistema de identificación a las personas VIP de la discoteca, lo que permite entrar en el local y pagar las consumiciones a través de un chip implantado en el brazo del cliente. Esto permite a la persona no mostrar ninguna identificación al entrar ni llevar dinero ni otra forma de pago con ella.

La respuesta a su implantación en 2004 fue todo un éxito según el propietario de la discoteca Conrad Chase que afirmó que eran más de un centenar las personas que lo llevaban implantado ().

Ponerse el chip costaba 125 euros y permitía al usuario ahorrar los 15 euros que costaba la entrada al local. En 2008, los nuevos propietarios decidieron suspender la oferta de implantación de chips. La colocación la realizaba personal médico de la propia discoteca y duraba unos cinco minutos. Era necesario concertar una cita previa y se colocaba siempre que el cliente no hubiera bebido alcohol.

Ilustración 60.-Entrada de la discoteca Baja Beach Club

El chip tiene 16 dígitos que un lector conectado con la base de datos de la discoteca lee. El sistema está cerrado y no está conectado a ninguna red, para evitar el acceso de personas indeseadas. El cliente solo tiene que aportar su nombre, una fotografía y la cantidad de dinero que quiere depositar en su cuenta.

El caso de implantes en discotecas también se ha dado en 2004 en una conocida discoteca holandesa que dispone de este sistema para sus clientes VIP: no sólo se les facilita el acceso a zonas restringidas sino que además no necesitan tarjeta de crédito ni metálico para pagar sus consumiciones.

2.5.1.6.2 Empresas

La empresa CityWatcher de vigilancia por video, inyecta a sus trabajadores un chip implantable de la empresa Verichip en el área del tríceps. La etiqueta puede ser leída a través de la ropa a unos pocos centímetros.

Este dispositivo está siendo utilizado para acceder a áreas restringidas y enlace a los registros médicos ().

Según informes publicados, sólo dos empleados se implantaron el chip y la empresa abandonó el programa (Palao).

2.5.1.6.3 Cárceles

Varias prisiones federales en EEUU están analizando el sistema con proyectos piloto. No se han encontrado noticias sobre el éxito o fracaso de estos proyectos.

2.5.1.6.4 Policía

El departamento de policía de México ha implantado en 2004 un chip RFID a unos 160 de sus oficiales de policía, para permitir el acceso a las bases de datos de la policía y para poder seguirlos en caso de ser secuestrados (Gardner). En la actualidad no se encuentra ninguna información que corrobore el éxito o fracaso de esta implantación

2.5.1.6.5 Ejército

La Verichip está promoviendo un chip para los soldados que permita sustituir la placa de identificación tradicional de los soldados.

El chip RFID permite poder identificar a los soldados en caso de que no se pudiera realizar por reconocimiento visual, donde las técnicas biométricas no tendrían paso en algunos casos. Esto hace que el chip RFID imponga una clara ventaja sobre la biométrica en estos casos.

2.5.1.6.6 Inmigración

En 2006 Verichip propuso la implantación de chips en inmigrantes para ayudar al gobierno de los EE.UU. a su identificación posterior.

Esta propuesta dio pie a múltiples debates sobre la obligación de los inmigrantes a implantar el chip para poder trabajar debido a su precaria situación económica y al costo de realizar estas intervenciones y quién debería pagarla. Se creó un arduo debate sobre una posible política de discriminación y la propuesta fue rechazada.

2.5.1.6.7 Detección virus

En la actualidad PositiveID en colaboración con su socio de desarrollo RECEPTORS LLC está desarrollando un sistema rápido de detección de virus para el virus H1N1 y otras enfermedades pandémicas mediante un chip implantado en humanos.

Es importante destacar que PositiveID cree que la clasificación del sistema de diagnóstico de la gripe será escalable y será capaz de adaptarse rápidamente para identificar nuevas cepas de la influenza y otros virus a medida que evolucionan ().

2.5.1.6.8 Biosensores

La empresa PositiveID también poseen las patentes relacionadas con un biosistema de sensores integrados. Una aplicación potencial de este sistema es un biosensor chip RFID implantable para medir los niveles de glucosa en el cuerpo.

El objetivo del proyecto es crear una forma alternativa para que los pacientes de diabetes controlen sus niveles de azúcar en la sangre, sin la necesidad de la extracción de sangre ().

2.5.1.6.9 Hospitales

El RFID implantado en pacientes podría ser un medio de identificación de pacientes que sean incapaces de comunicarse con el servicio del hospital, así como un medio de acceso rápido a los registros médicos del paciente pudiendo salvar vidas en esta situación donde se precisa velocidad y la comunicación paciente-médico resulta inviable.

Mientras el usuario hubiera dado su consentimiento informado y la privacidad del historial médico del paciente este cuidadosamente protegida, son pocos los problemas éticos en este caso.

También se podría promocionar el chip entre pacientes con enfermedades como la diabetes, los cuales deben acudir con frecuencia al médico, y aquellos que padecen trastornos como el Alzheimer.

La compañía Positive-Id ofrece un sistema de identificación del paciente. Su sistema ™ VeriMed para la identificación del paciente se compone de un microchip RFID implantable en humanos aprobado por la FDA que se vincula a un registro personal de salud y puede ayudar al personal de los hospitales a tratan a los pacientes que no puedan tener una comunicación rápida y eficaz en caso de una emergencia. El microchip contiene sólo un número de 16 dígitos que cuando se escanea con un lector de mano, se conecta a nuestra base de datos en línea segura. La base de datos almacena información de identificación del paciente y los datos de registro personal de salud.

2.5.2 Chips RFID no implantables

En la actualidad ya existen casos de control de personas mediante la tecnología RFID a través de tarjetas de identificación. Gracias a ellas y con una inversión no muy costosa es posible obtener en tiempo real informaciones tales como el número de personas presente en una instalación o dónde se encuentran ubicadas posibilitando de esta manera que las evacuaciones del edificio sean más fáciles o evitando el acceso de personal no autorizado.

Las aplicaciones en este campo son uno de los puntos fuertes de los sistemas RFID. La tecnología RFID puede, si no remplazar los sistemas actuales, si complementarlos.

Estas tarjetas son cada vez más funcionales, y normalmente obligan a introducir además un código secreto para evitar que la tarjeta sea usada por una persona incorrecta, pudiendo permitir no sólo el acceso a distintas zonas, sino también a máquinas expendedoras o por ejemplo para pagos pequeños en una cafetería de la empresa.

Ilustración 61.-Uso de una tarjeta identificadora con RFID

Los beneficios son, aparte de una reducción de costes en algunos casos, la versatilidad de las tarjetas para añadir o disminuir permisos de acceso o para adaptarse a situaciones poco habituales, como visitas o accesos puntuales.

Akrocard, empresa española fabricante de todo tipo de tarjetas plásticas, lanzó al mercado tarjetas híbridas que combinan dos tecnologías en un único soporte, es decir, en una misma tarjeta plástica. Esta combinación integra la tecnología sin contacto (RFID) de proximidad y un chip de contacto, obteniendo así tarjetas híbridas que funcionan con ambas tecnologías ().

Las aplicaciones más habituales de este tipo de tarjetas son el transporte público, la tarjeta ciudadana o de servicios municipales, el control de acceso, control de presencia, entradas y salidas de personal, tarjeta monedero, fidelización de clientes, identificación, etc.

2.5.2.1 Cárceles

El seguimiento de los presos es una de las principales preocupaciones en los sistemas carcelarios en EEUU. Especialmente cuando los reclusos son heridos o se enferman, y desde la prisión deben demostrar que proporcionaron todos los servicios que podían ofrecer antes del incidente.

Ilustración 62.-El sistema RFID puede ser muy útil para el sistema penitenciario.

En agosto de 2004, el Departamento de Rehabilitación y Corrección de Ohio (ODRH) aprobó un contrato de 415.000 dólares para ensayar la tecnología de seguimiento con Alanco Technologies. Los internos tienen unos transmisores del tamaño de un reloj de muñeca que podían detectar si los presos habían estado intentando quitárselas y enviar una alarma a los ordenadores de la prisión. Este proyecto no es el primero que trabaja en el desarrollo de chips de seguimiento en prisiones estadounidenses. Instalaciones en Michigan, California e Illinois emplean esta tecnología.

En una nueva iniciativa para realizar un seguimiento automático de documentos y de las interacciones críticas entre los detenidos y los guardias de la cárcel, Hardin County Jail en Eldora, Iowa ha implementado Clincher RFID pulseras.

Hardin County Jail instaló el sistema RFID en 2005 como un sistema de cumplimiento Penitenciario de sus 107 instalaciones de reclusos. De aplicación en diciembre de 2009, la adopción de Clincher pulseras RFID mejora la seguridad de la cárcel y la seguridad al proporcionar la identificación no transferible de los detenidos. Anteriormente, la cárcel del condado de Hardin utiliza credenciales de identificación para la identificación de los reclusos. Las tarjetas de identidad a veces se pierden por los detenidos o por otro recluso. Las pulseras RFID, de identificación del detenido permanecen intactas en todo momento. El cumplimiento de normativas dentro de la cárcel es un factor clave para las aplicaciones de RFID actualmente utilizados en la cárcel del condado de Hardin. Ser capaz de administrar y documentar las interacciones individuales entre guardias y

presos es fundamental para varios de los programas de seguridad, incluida la prevención del suicidio.

Hay varias aplicaciones destinadas a mejorar la seguridad de la cárcel y la seguridad de los detenidos, al tiempo que la automatización de procesos manuales para ahorrar tiempo y mano de obra. Seguimiento de la expedición y devolución de suministros especialmente peligrosos, como navajas de afeitar. Otra aplicación es el seguimiento de la transferencia de detenidos de la cárcel al juzgado y su vuelta para garantizar que todos los detenidos se tienen en cuenta (Editors).

Empresas como GEMALO+Security están trabajando en una solución basada en tecnología RFID que hace posible la localización y monitorización en tiempo real de internos y personal, el recuento de internos automatizado "online" y posee botón de pánico y detección de hombre a tierra.

2.5.2.2 Control en hospitales

Las predicciones de mercado sugieren que el despliegue de RFID en el sector sanitario crecerá de manera exponencial en los próximos años.

Las aplicaciones dentro del ámbito sanitario que pueden contribuir a la proliferación de RFID en este sector son:

- ✓ Control de activos
- ✓ Control de personas

Dentro del control de activos se entiende el seguimiento de medicamentos para evitar su falsificación, seguimiento de bolsas de sangre, control de maquinaria especializada, control de material sanitario, control del sistema de información sanitaria, de los contenedores de quirófano, de las camas de pacientes y ropa del personal y control de acceso y farmacia del hospital.

Ilustración 63.-Gestión de activos de alto valo

En cuanto a la gestión de las personas, se refiere a que se debe controlar al personal sanitario y a los pacientes del centro permitiendo realizar funciones tales como seguimiento e identificación de pacientes, control del cumplimiento por parte de los pacientes de las prescripciones facultativas en lo referente a medicación y mejora de los flujos de trabajo en los hospitales y centros de salud.

2.5.2.2.1 Personal sanitario

En los quehaceres diarios de un centro sanitario en ocasiones es fundamental tener localizado al personal. Lo ideal sería saber dónde están en cada momento. Con la tecnología RFID esto es posible. El personal de un hospital lleva puesto su uniforme mientras está trabajando. Este uniforme suele consistir en una bata, en la que llevan colgando una tarjeta identificativa, con sus datos (nombre, cargo…). En esta tarjeta es posible insertar un tag activo RFID. El tag funciona como transmisor, ya que, como su propio nombre indica, transmiten un identificador único cada cierto tiempo, lo que permite poder monitorizar en tiempo real la ubicación del personal.

Las antenas del sistema tienen zonas especificas de cobertura que se asocian a espacios físicos, sala de curas, quirófanos…

La precisión no es cuestión de las antenas, que tienen rango de sobra, sino que la define la gerencia del hospital. Dependiendo de las necesidades de cada hospital o de cada aplicación, en ocasiones será suficiente tener localización en una planta en general, o en una sala en concreto.

Otra cualidad es que el sistema también se puede configurar para que cuando sea necesario y de forma voluntaria o precisada, salten alarmas. Estas alarmas pueden provocarse pulsando un botón, por ejemplo en caso de que el personal sanitario precise ayuda, con la sencilla acción de presionar el botón, saltará una alarma, y de forma instantánea se sabrá la necesidad de ayuda y la localización exacta de la persona que lo solicita.

2.5.2.2.2 Pacientes

Para pacientes dentro de un hospital, se puede utilizar tanto RFID activa como RFID pasiva, dependiendo de las aplicaciones que se deseen realizar.

Con la RFID activa, funcionará de igual forma que con el personal sanitario. Se insertará una etiqueta RFID en una pulsera identificativa de paciente, y éste estará localizado en todo momento. El uso de la tecnología RFID activa tendrá muchas aplicaciones útiles, como puede ser por ejemplo para pacientes de una zona psiquiátrica, de este modo podría saltar una alarma si el paciente intenta salir de una zona determinada. Si un paciente fuese a salir de una zona determinada saltaría una alarma, y se podría evitar. Estas alarmas incluso pueden ser configuradas para que, de forma automatizada, se cierren puerta.

Las etiquetas RFID activas se utilizan con un sensor para monitorizar la temperatura corporal del paciente. Además, éstos constan de un botón de pánico para que los enfermos puedan presionarlo para solicitar ayuda cuando la precisen. Los brazaletes son resistentes al agua y a impactos fuertes. Si los pacientes intentan quitárselos salta una alarma, que avisa del peligro.

Con la RFID pasiva mediante una etiqueta insertada en una pulsera identificativa del paciente se obtendrá un control de los datos que se decidan incluir. De esta forma se podrá obtener los datos de la medicación que precisa el paciente en concreto y la cantidad de ésta. Para ello, el personal sanitario dispondrá de dispositivos inalámbricos, como pueden ser PDA, Pockets PC… los cuales dispondrán además de

Wifi, un lector RFID de manera que se puedan obtener los datos de manera sencilla con el simple gesto de acercar el dispositivo al paciente (RFId Activa+ RFID pasiva=Hospital del futuro).

Ilustración 64.-Monitoreo de pacientes usando tecnología RFID

De este modo se evitará que el personal sanitario tenga que transportar numerosas carpetas con el historial del paciente, reduciendo los errores de medicación o historial, en definitiva evitando los errores humanos.

2.5.2.2.3 Recién nacidos

Uno de los casos que más atención despierta ante las posibilidades que ofrece la RFID, es el de los recién nacidos. La empresa GEMA ABS posee una solución específica para estos casos: Gema LOC+ Baby Match. Mediante esta solución se realiza un test, por el cual se unen las informaciones del tag del bebé, con el tag de la madre (colocado en las muñequeras o tobilleras identificativas) ().

Al pulsar el botón se puede apreciar una señal luminosa que indica que todo es correcto, si la luz es verde, o que hay un error, si es roja. Además también permite proporcionar una localización e identificación en tiempo real de todos los neonatos en el recinto de la unidad, recibir dicha información “online” y visualizarla en la pantalla del ordenador.

2.5.2.2.4 Ejemplos prácticos

Hospital de Yu Li

En el hospital Yu Li de Taiwán, se han colocado 2.500 brazaletes RFID a pacientes mentales, de este modo controlan sus movimientos y evitan que salgan de zonas delimitadas.

Hospital Costa del Sol Marbella

El hospital Costa del Sol de Marbella, Málaga, ha sido uno de los centros que ha iniciado un proyecto RFID para mejorar la seguridad de los pacientes, en las áreas de Oncología y en pacientes quirúrgicos en el hospital Costa del Sol y en el Centro Hospitalario de Alta Resolución de Especialidades (CHARE) de Benalmádena. Por medio de chips RFID implantados en la pulsera del paciente, pueden saber qué medicación, dosis, etc. precisa de cada paciente, tras leer su etiqueta mediante una PDA ().

Tras un periodo de prueba entre febrero y julio de 2006, la experiencia con el sistema RFID ha sido positiva, ya que según el responsable de la unidad de calidad del centro, mejoró la identificación y la localización de los pacientes y los fármacos.

Este sistema consiste en unos códigos de identificación que se insertan en unas pulseras llevadas por los enfermos y en los envases de los fármacos. Estos códigos son leídos a través de dispositivos PDA, que vinculan los datos del paciente con los del fármaco para evitar errores de los enfermeros al abordar al paciente.

Ilustración 65.-Lectura del chip RFID en una pulsera que posee el paciente

Esta tecnología también se puso en fase de pruebas en otros centros como Son Llàtzer, en Mallorca, y en el Gregorio Marañón en Madrid.

El sistema fue diseñado por profesionales del Hospital Costa del Sol y de la empresa malagueña Cetecom y la participación del personal de enfermería en la creación del sistema ha sido una de las claves del éxito del sistema RFID.

Además, las pulseras tienen como ventaja que es posible escribir información adicional en la pulsera, ésta no se estropea con la humedad o el calor y además se puede leer por encima de una sábana gracias a que la tecnología RFID no necesita visión directa, así no hay que molestar al paciente si éste está durmiendo.

Hospital Jena University

En 2006 SAP, Intel y el Hospital Jena University, situado en Jena, Alemania, anunciaron la implementación de un sistema basado en RFID con el objetivo de reducir los errores médicos y mejorar el cuidado a sus pacientes. Mediante la utilización de tags RFID, la medicación puede ser seguida en tiempo real desde la farmacia del hospital hasta la ubicación del paciente. La medicación podrá ser comprobada y contrastada de manera automática y digital antes de administrarla al paciente, chequeando el identificador del brazalete RFID del paciente. Utilizando terminales móviles RFID, las enfermeras o enfermeros pueden leer los códigos y visualizar la información del paciente en la pantalla.

Además, el sistema se ha diseñado para registrar toda la medicación del paciente, incluyendo detalles sobre el tipo, la cantidad, hora de administración, etc. Para asegurar el proceso de transporte desde la farmacia hacia el paciente, todas las unidades de dosificación de medicamentos, cajas de transporte o contenedores del sistema interno de transporte han sido etiquetadas con tags RFID.

“Estudio internos revelaron que aproximadamente cada 20 pacientes uno sufría un error, y sobre el 55% de los casos eran evitables”, afirmaba Dr. Michael Hartmann, director de farmacia del hospital. La solución mejora la calidad del tratamiento, además la infraestructura RFID ayudará a optimizar los procesos logísticos y la gestión de la demanda en la cadena de suministro, reduciendo el capital situado en la farmacia del hospital. La infraestructura permitirá a los empleados realizar identificaciones digitales para verificar los tratamientos correctos para el paciente en concreto, además de advertirles de información como podría ser la expiración de una fecha de caducidad.

Virtua Health, compañía de Nueva Jersey que gestiona hospitales, está instalando en la actualidad un sistema RFID para realizar el seguimiento de miles de pacientes y personal de sus 4 hospitales, así como de más de 10000 activos.

El sistema utilizado es provisto por GE Healthcare. El mismo permite que Virtua tenga una mejor gestión de las admisiones de los pacientes ya que conoce en tiempo real qué camas están libres. Además, el sistema permite mejorar la eficiencia a través del conocimiento de la localización de los diferentes activos y equipos médicos.

Hospital de Cabueñes

En 2007 se implantó en el Hospital de Cabueñes en Gijón un sistema pionero de identificación por radiofrecuencia.

Este sistema de monitorización, denominado también 'chip del paciente', permite saber en todo momento dónde se encuentra el enfermo (si en boxes, radiología u observación), a qué pruebas fue sometido y cuánto tiempo de espera acumula desde el ingreso ().

La pulsera lleva los datos principales del enfermo -nombre y apellido, edad y motivo del ingreso-, junto a una pegatina donde se encuentra adosado el chip. Este dispositivo

dispone de un sistema de radiofrecuencia, a través del cual y gracias a la instalación de una serie de lectores en puertas y pasillos de Urgencias, se puede hacer un seguimiento minucioso del itinerario seguido por el paciente.

Ilustración 66.-Entrada del Hospital de Cabueñes (Gijón)

Los resultados de las pruebas clínicas ya no sólo se procesan en papel, sino que llega en cuestión de segundos hasta unas PDAs) que tienen los médicos.

El proyecto, pionero en Europa, permitirá agilizar trámites y pruebas diagnósticas, algo de vital importancia en un servicio como el de Urgencias, por el que pasaron en 2006 más de 110.000 personas (entre 280 y 290 al día).

La empresa Treelogic, fue la encargada de poner en marcha esta etiqueta de identificación.

Las pulseras cuentan con un dispositivo que utiliza la más innovadora tecnología por radiofrecuencia. Se trata de una etiqueta inteligente que suele ser utilizada por grandes distribuidoras y superficies comerciales y que por vez primera se aplicará en el ámbito sanitario. El de Cabueñes será el primero hospital europeo que estrenará este tipo de dispositivo.

La tecnología de identificación por radiofrecuencia (RFID), no sólo permitirá agilizar la atención a los enfermos sino también mejorar la información a los familiares, uno de los motivos que más quejas generan en Urgencias. A través de una pantalla de televisión instalada en la sala de espera, los familiares recibirán información detallada de lo que ocurre con el enfermo puertas adentro.

Para no atentar contra la intimidad del paciente, el nombre y el apellido del afectado serán sustituidos por un número codificado que se corresponderá con el historial clínico del enfermo. En la pantalla de televisión aparecerá, por ejemplo, si el enfermo se encuentra en boxes a la espera de ser examinado, si ha pasado a radiología o está a punto de ser subido a planta para su hospitalización.

Además, en la sala de espera se instalará un ordenador donde los familiares dispondrán de información mucho más detallada del proceso. Sólo se podrá acceder a él mediante una tarjeta con código de barra que se entrega al acompañante del paciente en el momento que el enfermo llega al hospital. Esa misma tarjeta será la que, en un futuro y tras la proyectada ampliación de Urgencias, sea empleada por el centro sanitario como método de acceso restringido al hospital.

Por otra parte, el gerente del Área RFID de Treelogic, precisó que a través de los localizadores instalados en las diferentes salas de urgencias, se podrá localizar de forma precisa a los pacientes. También se medirán los tiempos de espera.

Una vez que el enfermo abandona el hospital o pase a planta la pulsera queda inutilizada. El proyecto de Urgencias se ampliará en el futuro a la zona de quirófanos. Esta iniciativa estará orientada, fundamentalmente, a mejora la información que reciben los familiares mientras el enfermo permanece en el área quirúrgica.

El proyecto ha quedado en fase de suspensión y no se está utilizando a la fecha de redacción de este trabajo supuestamente por dificultades técnicas y económicas según personal consultado del Hospital.

2.5.2.3 Pasaportes

Muchos países tales como EE.UU, Canadá o Australia están incorporando ya la tecnología RFID a sus pasaportes. Con ello se dificulta su falsificación, se agilizan los trámites de lectura e incluso, en algún caso, ya se utilizan para ir registrando electrónicamente las entradas y salidas del país, etc.

En algunos casos, y con el fin de garantizar la privacidad del usuario, se apantallan los pasaportes con una fina hoja metálica de forma que sólo puedan leerse cuando están abiertos

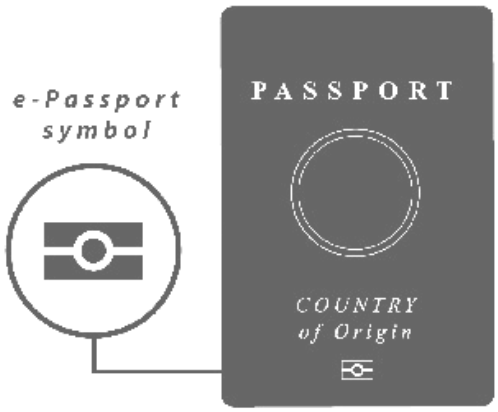


Ilustración 67.-Simbolo de un pasaporte que utiliza tecnología RFID

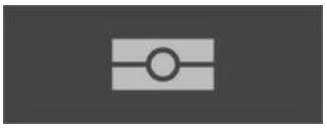


Ilustración 68.-Símbolo RFID en un pasaporte

El 19 de Octubre de 2005, el Gobierno sueco sacó a la luz el primer e−pasaporte cuya principal tecnología es el RFID. Cada tag tiene codificada la información personal habitual en los pasaportes convencionales (datos legales, altura, color de ojos y pelo, etc.) y una fotografía digital de su propietario.

Swenska Pass, una división de la empresa tecnológica Setec, ha sido la encargada de crear el e−pasaporte.

Además de la aplicación software en si, la solución permite la impresión del pasaporte que comporta un tag de 64KBytes de memoria donde se almacena la información del propietario una vez encriptada. Antes de la entrega, la división de policía encargada verificará la correcta encriptación de los datos, con el fin de asegurar la privacidad de estos.

Las tarjetas de identificación no son obligatorias, pero pueden utilizarse en lugar de pasaportes para la identificación cuando se viaje dentro del país.

Los lectores se pueden conectar a los ordenadores existentes en cada comisaría de policía a través de un puerto USB y controladores de software cargado en la máquina. La policía sueca supervisó la instalación de software para vincular los datos recogidos con la base de datos del gobierno sueco, así como la instalación de los interrogadores. En 2006, el gobierno sueco espera emitir unos 500.000 pasaportes electrónicos. Las etiquetas utilizadas en los nuevos pasaportes electrónicos y las tarjetas de identificación operar a 13,56 MHz y deben cumplir con las normas ISO 7816 e ISO 1443A . Para evitar que una etiqueta sea leída a distancia o por personal no autorizado, cada pasaporte electrónico se imprime con un código de acceso básico (BAC). Este primer código debe ser leído a través de un reconocimiento óptico de caracteres (OCR) del escáner o escribir manualmente en el interrogador RFID, que compara los datos . Si coinciden, el interrogador RFID tendrá acceso a toda la información almacenada en la etiqueta (Collins).

Ilustración 69.- Pasaporte de Suecia

2.5.2.4 Localización niños parque temático

El parque temático de Staffordshire, cerca de Manchester en Gran Bretaña, ofrece a cada persona que acceda a su recinto una pulsera que contiene un pequeño chip RFID. De este modo, los responsables de Alton Towers observan a los visitantes y los filman con cámaras mientras éstos se mueven por el parque. Al final del día, se da la opción a los visitantes de comprar sus imágenes en un DVD personalizado. Expertos de Venue Solutions, la compañía que trabaja en el proyecto, comentan que las etiquetas también se pueden utilizar para seguir a niños perdidos y para acabar con crímenes tales como robos y vandalismo. El sistema llamado *Your Day* también podría introducirse en el Bush Gardens en Florida y en Disneyland París.

Por otro lado, Liz Greenwood, de Alton Towers, comenta que el aspecto de la seguridad queda como un aspecto secundario ya que los brazaletes no son obligatorios. "Si la gente no desea participar, es su decisión". Greenwood también afirma que "solamente se filmará a las personas que decidan participar en el proyecto. Por lo tanto, si por ejemplo, se pierde un niño, el sistema tan sólo seguirá al niño si sus padres han decidido previamente que lo podían seguir".

Ilustración 70.-Sistema YourDay permite grabar tus movimientos en el parque temático

2.5.2.5 Eventos deportivos

Las etiquetas RFID proporcionan una muy conveniente y precisa manera de tomar los tiempos de los participantes en los diferentes eventos deportivos. Si los costos de los componentes RFID disminuyen, seguramente está práctica se popularice.

En larga escala de los eventos deportivos, como los maratones por ejemplo, los participantes quienes inician en la parte de atrás la carrera son siempre los perjudicados porque sus tiempos son calculados desde el inicio de la carrera, lo que implica perder varios minutos antes de empezar realmente el trayecto que deben seguir.

Para corregir estos desajustes de tiempo los competidores pueden llevar tags RFID en sus zapatillas de deporte de modo que el sistema monitoriza en todo momento los tiempos de los participantes. Estos tags son abrochados en los cordones de las zapatillas de los competidores y operan en la frecuencia de 135Khz

Ilustración 71.-Los transponder ChampionChips

2.5.2.6 Agilización de procesos administrativos y posibilidad de automatización mediante identificación rápida y fiable

El sistema de auto-identificación a través del sistema RFID permite agilizar procesos administrativos dado que la gestión de los datos de cada persona se puede realizar de manera informatizada a través de bases de datos permitiendo eliminar todo el "papeleo" existente en este tipo de procesos realizando una gestión eficaz de los datos personales y eliminando posibles errores humanos.

Como ya se ha visto en apartados anteriores automatizar actividades tales con el acceso de los trabajadores permite aumentar la seguridad de la instalación y ofrece a los trabajadores la comodidad de una identificación rápida y a la empresa la seguridad de una identificación fiable. También en el control de asistencia, automatizar todos los datos de las personas permite llevar un control eficiente y rápido de las personas que se encuentran en un lugar determinado y permite realizar todas las gestiones administrativas de manera cómoda y segura.

Un ejemplo de que la implantación del sistema RFID ha mejorado notablemente el nivel de productividad de los empleados, reduciendo la pérdida de documentos y mejorando las condiciones de trabajo ha sido la universidad de Florida (13) donde este sistema lleva funcionando desde 2006. El sistema se adoptó con la idea de implantar un sistema de gestión documental que fuera capaz de gestionar de manera eficiente y eficaz el gran volumen de documentos que se ponen en circulación diariamente en la universidad (proyectos de investigación, becas…) con el objetivo de automatizar el máximo posible las operaciones, reducir o eliminar por completo la pérdida de documentos y controlar las entradas y salidas de los mismos.

Si bien, antes de la implantación de este sistema, el trabajador que quería buscar un documento debía poner en una tarjeta el número de documento y ponerla en el espacio donde estaba situado. Una vez fuera de las instalaciones podía pasar meses, incluso pasar por diferentes personas, así cuando el documento se devolvía al centro, se volvía a poner el documento donde estaba la tarjeta con su número de identificación y se eliminaba.

Con este sistema lo más normal era perder documentos o ubicarlos mal. Por este motivo, en el 2005, la universidad inició la búsqueda de un nuevo sistema de gestión

documental. Este sistema no es otro que un sistema de identificación por radiofrecuencia (RFID) 3M Tracking System, una de las más implantadas en Bufetes de abogados en los Estados Unidos. El sistema esta compuesto de etiquetas RFID en HF (13,56 MHz), lectores fijos y móviles. El sistema basado en ISO 15693 utiliza tags de Texas Instruments con una capacidad de 2K (2048 bits) de memoria.

El lector, llamado Tracking Pad Monitor, es fijo y esta conectado a una antena de tamaño medio, que puede ser instalada en la pared o en cualquier mesa o escritorio. Este lector se conecta al software de gestión (System Manager Software). La antena tiene un rango de lectura alrededor del medio metro.

Los lectores fijos tienen dos funcionalidades: codificar todos los documentos con una numeración única de 6 dígitos y leer los movimientos que se producen en la oficina a nivel de entrada y salida. El lector móvil con una antena que sobresale para mejorar el comportamiento tiene un rango de lectura de unos 10-15 centímetros.

El System Manager recolecta los datos de los tags y los envía al File Locutor, que genera un informe de inventario de cada una de las estanterías escaneadas. Al mismo tiempo también genera un informe de las estanterías que no han sido leídas o de los documentos que no se han leído y no están marcados como check out de las oficinas, así como los que no se encuentran en el lugar correcto.

Cuando el documento es devuelto, el trabajador simplemente acerca el documento al lector RFID que recibe la información y la envía al software de gestión que muestra al trabajador el área al que pertenece el documento, con este dato el empleado sitúa el documento en la caja correspondiente a el área para que los estudiantes que trabajan en la institución los vuelvan a situar el sitio correcto.

El personal administrativo cuando recibe un nuevo documento, entra en la base de datos donde se encuentra la ficha del proyecto aprobado, aquí se añade un código de 6 dígitos se imprime y se codifica el tag. Una vez asociada la información en el tag y la base de datos, se adhiere la etiqueta electrónica al documento mediante el lector y antena de sobremesa.

Ilustración 72.-Empleado insertando tag en la carpeta del documento.

2.5.3 Caso particular de los centros docentes

2.5.3.1 Introducción

Este apartado se centrará en estudiar los diferentes casos donde se implantó tecnología RFID en centros docentes con el fin de identificar a los alumnos para mejorar el servicio del centro.

Se realizará un estudio cronológico de los casos más significativos que ocurrieron a escala mundial describiendo sus características, empresa que implanto el sistema así como la respuesta social, del colegio y de los alumnos ante la implantación del sistema.

Ilustración 73.-Insignia de un colegio con chip RFID en su interior

En la siguiente tabla, se puede observar cronológicamente los diferentes centros que implementaron esta tecnología y su lugar de procedencia.

AÑO	ESCUELA	SITUACIÓN
2003	Enterprise Charter School	**Buffalo, Nueva York**
2004	Escuela Primaria de Osaka	**Osaka, Japón**
2005	Brittan School	**California**
2006	Rikkyo Elementary	**Tokio, Japón**
2007	Hungerhill School	**Doncaster, Reino Unido**
2007	Na Hu Elementary	**Taipei, Taiwán**
2008	Escuela primaria de Aquineck	**Rhode Island, EE.UU.**
2010	Taipei American School	**Taipei, Taiwán.**
2010	**Love Dale Central School**	**Belgaum. La India.**

Tabla 11.-Resumen de los centros docentes analizados.

2.5.3.2 Escuelas analizadas

2.5.3.2.1 Enterprise Charter School

En el año 2003, el director de la escuela Enterprise Charter School de Buffalo, Nueva York, Gary Stillman decide implantar el sistema RFID en la escuela para organizar de manera más eficaz el recuento de los alumnos. De esta forma el director de la escuela argumentaba que el colegio sería más eficaz y seguro (Scheeres).

Antes, el recuento de los alumnos se hacia de forma manual, de manera que cada profesor debía llevar la cuenta de la asistencia de sus alumnos y enviar los informes a la oficina correspondiente. Con el nuevo sistema, ya no se perderá más tiempo en esto, y el recuento se realizará de manera más rápida y eficaz.

Ilustración 74.-Estudiante acerca la tarjeta RFID identificativa al lector

Los estudiantes usan pequeñas tarjetas de plástico alrededor del cuello que tienen su foto, nombre y grado impreso en ellos, e incluyen un chip RFID incrustado. Cuando los niños entran a la escuela, se acercan a un "kiosk" (ver figura 6.27) donde se activa la señal del chip y se muestra su fotografía. Los estudiantes tocan la fotografía, y el momento de su entrada en el edificio se registra en una base de datos. Un miembro del personal de la escuela supervisa el proceso de check-in.

El director de la escuela, Stillman originalmente quería que las etiquetas RFID estuvieran directamente cosidas en los uniformes de los estudiantes, pero los profesores temían que los niños podían cambiar los uniformes para engañar al sistema, por lo que se decidió que los estudiantes llevaran las etiquetas alrededor del cuello con su fotografía.

Ilustración 75.- "Kiosk" de la empresa IntuiteK

La escuela también tiene previsto utilizar la tecnología RFID para controlar los préstamos de biblioteca, compras de cafetería y la salud de los estudiantes y los registros disciplinarios.

El presidente de la empresa que implanta el sistema, IntuiteK David M. Straitiff dice que su empresa realizó un sistema de protección de la privacidad en el sistema de RFID de la escuela, incluyendo la limitación del rango de lectura de los "Kiosk" a menos de 20 pulgadas y hacer que los estudiantes deban tocar la pantalla del "Kiosk" en lugar de esperar pasivamente siendo escaneados por él. El sistema RFID utilizado es Tecnología RFID de 13,56 MHz de TI-RFID.

La escuela ha gastado 25.000 dólares en el sistema de identificación.

2.5.3.2.2 Escuelas primarias de Osaka

Las autoridades escolares en la ciudad japonesa de Osaka decidieron en el año 2004 que los beneficios del sistema RFID en centros docentes superaba los inconvenientes y en la actualidad los niños poseen chips RFID identificativos en la escuela primaria.

Las etiquetas son leídas por los lectores instalados en las puertas de la escuela y otros lugares clave para rastrear los movimientos de los niños.

Los chips RFID se pondrán en mochilas escolares para niños (Best).

2.5.3.2.3 Brittan School

Una pequeña empresa de California denominada Incom desarrolló una identificación de radio frecuencia (RFID), denominado sistema InClass para automatizar la toma de asistencia en las escuelas primarias y secundarias. El sistema utiliza frecuencia ultra alta (UHF). Los lectores instalados en las puertas de clase y las etiquetas RFID pasivas adjuntas a la tarjeta de identificación que debe llevar cada estudiante permiten su funcionamiento. InClass estaba siendo probado en la escuela primaria Brittan en

Sutter, la pequeña ciudad al noreste de Sacramento, donde se fundó InCom. Después de que un número de padres de alumnos protestaran a la escuela por el uso de la RFID, InCom anunció el 15 de febrero en una reunión de la junta escolar que daba por concluida la prueba piloto (RFID Takes Attendance—and Heat, 2005).

El piloto se inició 18 de enero de 2005. La escuela quiso probar el producto InClass para ver si se podría disminuir la cantidad de tiempo perdida por los docentes cuando pasan asistencia manualmente al principio de cada clase. También estaba estudiando el uso el producto InClass para ayudar a localizar a los estudiantes en el campus, aunque el piloto fue probar el uso de InClass sólo para tomar asistencia. Coincidiendo con el despliegue InClass, los administradores de la escuela Brittan habían emitido una identificación con foto tarjetas a todos sus estudiantes como un medio para aumentar la seguridad de la escuela, asegurando que todos los estudiantes pueden ser fácilmente identificación visual.

El piloto InClass en Brittan Elementary fue probado únicamente en las aulas de séptimo y octavo grado, con los lectores de instalados en las puertas de las clases. La única información de la prueba piloto InClass podría haber proporcionado a la administradores de la escuela era la de si el estudiante de séptimo u octavo grado había entrado o salido de uno de esos aulas.

Ilustración 76.-Alumna de Brittan School con su tarjeta identificativa RFID

El colegio Brittan, recibió una avalancha de atención de los medios, ya que un número no especificado de los padres de los estudiantes de Brittan, se preocuparon por el uso de la tecnología RFID en la escuela y la emisión de tarjetas de identificación con foto a todos los estudiantes Brittan. Las tarjetas de identificación muestran la imagen del estudiante y el nombre completo pero que no contienen un visualizador del chip RFID. Cada estudiante usa su tarjeta dentro de un plástico transparente que contiene una etiqueta RFID y se une a un cordón para ponerla alrededor del cuello. Aunque sólo el séptimo y octavo grado participaron en el InCom piloto, todos los estudiantes Brittan debían usar sus tarjetas de identificación con foto en todo momento, mientras estuvieran en la escuela.

Los padres señalan una serie de preocupaciones sobre la emisión de etiquetas RFID para los estudiantes. Algunos dicen que la asignación de números de identificación a los estudiantes y el uso de ese número para identificarlos tienen efectos fisiológicos negativos sobre los estudiantes. Los padres también temen que los estudiantes podrían ser seguidos fuera de de la escuela o fuera de la gama de los lectores de RFID, a pesar de que funcionarios de la escuela han explicado que esta cosa que no es posible.

El producto InClass permite que los docentes de Brittan tengan datos generados por la asistencia a clase, período, día o semana. Y los administradores de la escuela podrían utilizar el sistema de InClass para enviar mensajes o los anuncios a los maestros a través de la PDA.

2.5.3.2.4 Rikkyo Elementary

En la escuela Rikkyo Elementary de Japón en 2006 se puso en marcha una prueba piloto de seguimiento mediante chips de RFID que detectan el paradero de los jóvenes. El gigante de la electrónica Fujitsu ha colaborado con una escuela privada de Tokio, Rikkyo Elementary, para poner en marcha un ensayo en el cual se han colocado chips de RFID en las mochilas de los estudiantes. A medida que el estudiante entra y sale de las instalaciones de la escuela, cada detalle es registrado a través de las señales que envía el chip a los receptores colocados en las puertas del centro escolar. Las etiquetas

de RFID se pueden unir a los libros, a los bolsos o a otros artículos personales. Los escáneres pueden leer los tags desde una distancia de hasta 10 metros, de este modo no se requieren ningún tipo de entradas especiales, y los estudiantes pueden ir y venir libremente sin tener que detenerse en un punto de comprobación de seguridad. Sus entradas y salidas se registran de manera sencilla cada vez que los estudiantes pasan por los escáneres.

Ilustración 77.- Estudiantes de la escuela Rikkyo Elementary a la entrada del centro.

Por otra parte, los padres obtienen toda la información directamente en su teléfono móvil y pueden recibir notificación, por ejemplo, de que sus niños llegaron seguros a la escuela. Los profesores y el personal de los centros comentan que la preocupación por la seguridad de los estudiantes impulsó esta idea y el proyecto. "Más del 70% de los padres apoyaron los ensayos, datos que indican la amplia conformidad con este tipo de proyectos," afirma Ichiro Ishihara, profesor en una escuela primaria pública en la ciudad de Iwamura, de la prefactura de Gifu. De los 334 estudiantes de la escuela, 72 han estado llevando las etiquetas desde que se iniciaron las pruebas a principios de septiembre. En un futuro, el sistema también podría utilizarse para restringir la entrada a gente no autorizada. "Nos tomamos la seguridad de la escuela muy seriamente, ya disponíamos de cámaras de seguridad y tenemos también vigilantes en los alrededores de la escuela las 24 horas al día", comenta Tsukasa Tanaka, uno de los responsables de la escuela primaria Rikkyo. Durante el desarrollo del sistema, Fujitsu y

la escuela primaria de Rikkyo dieron mucha importancia a los temas de privacidad y de seguridad. A medida que los estudiantes van pasando por la puerta de entrada del centro, unos lectores colocados allí mismo registran la señal emitida por los chips de RFID y trasladan la información a un ordenador central donde se va guardando. El sistema no sólo registra a cada alumno como va y viene, sino que también detecta a los visitantes que son identificados a través de un sensor infrarrojo que hace sonar una alarma tan pronto como las personas sin los chips de RFID traspasan la entrada. La tecnología de supervisión es una respuesta de las escuelas al aumento del miedo de los padres. En Japón, los crímenes forzados siguen siendo relativamente raros, tales como el asesinato, las lesiones corporales y los robos. Sin embargo, según un estudio hecho público recientemente, más de la mitad de los japoneses cree que su país se está convirtiendo en cada vez más inseguro.

2.5.3.2.5 Hungerhill School

En 2007 la escuela inglesa Hungerhill School (Walker) inició un programa piloto donde 10 alumnos del colegio de secundaria llevaban cosido al uniforme un chip RFID. De esta forma se pretendía que los alumnos fueran detectados a la entrada del centro mediante un lector y que el profesor no tuviera que pasar lista de forma manual sino que ésta quedará registrada de manera automática. Se pretendía de esta forma mejorar agilizar este proceso y evitar la pérdida de tiempo que conllevaba el proceso tradicional.

Ante esta prueba, la organización “Dejad a los niños en paz” protestó enérgicamente por lo que suponía era una mediada que atentaba a la intimidad de los niños.

2.5.3.2.6 Nan Hu Elementary

Desde su creación en 1995, la escuela municipal de Taipei Nan Hu ***Elementary School*** ha adoptado activamente la implementación de nuevas tecnologías para proporcionar garantías para sus estudiantes en ***la escuela.***

En 2007, la escuela pública de Taipei, Taiwán, implementa un sistema RFID para controlar la entra y salida de los niños ().

2.5.3.2.7 Escuela Primaria Aquidneck

El Distrito Escolar de Middletown, en colaboración con MAP Information Technology Corp, lanzó en 2008 un programa piloto para la implantación de chips RFID en las mochilas escolares de 80 niños en la Escuela de Aquidneck. Cada chip puede ser programado con un número de identificación del estudiante, y ser leído por un dispositivo externo instalado en uno de los dos autobuses escolares. Los autobuses también están equipados con sistema de posicionamiento global (GPS) (Gutierrez).

Los padres o los funcionarios escolares pueden iniciar sesión en un sitio web de la escuela para ver si los niños se encuentran en el autobús escolar y para buscar la ubicación actual del autobús en las condiciones previstas por el dispositivo GPS.

La American Civil Liberties Union (ACLU) ha criticado el plan como una invasión de la privacidad de los niños y un riesgo potencial para su seguridad.

El distrito escolar por su parte mantiene que su plan actual no es diferente de otros programas ya en vigor para los padres de supervisar la experiencia escolar de sus hijos.

Debido a que el programa piloto se está prestando para el distrito escolar sin costo, no requieren la aprobación de la Comisión de Ética de Rhode Island.

Se quiso prohibir su uso (noviembre 2009) pero el gobernador veto el proyecto de ley (Rhode Island Governor Vetoes Restrictions on RFID, 2009).

2.5.3.2.8 Taipei American School

En la escuela Pública de Taipei, Taiwán se ha instalado el sistema Campus**.** Cada tarjeta contendrá una fotografía del titular de la tarjeta de identificación y un código de barras y / o un chip RFID. Para los estudiantes más pequeños de la escuela, sólo tendrán un código de barras, mientras que la escuela media y estudiantes de escuela superior, así como del personal tendrán las tarjetas RFID.

Su implantación se producirá en breve.

2.5.3.2.9 Love Dale Central School

Los administradores de Love Dale Central School de Belgaum, La India, se encuentran en la actualidad en medio de las pruebas de un nuevo método de seguimiento de estudiantes, con la ayuda de la tecnología RFID.

La escuela, recientemente, ha lanzado un nuevo programa que requiere a todos los estudiantes el uso de una tarjeta RFID y que los padres y docentes puedan realizar el seguimiento de los estudiantes durante todo el día.

El nuevo sistema, denominado Keeptrack, no solo sirve para la identificación, también ayuda a mantener en los registros la asistencia del alumno, su rendimiento académico y su ubicación actual.

Los lectores instalados en todo el campus permiten dar la información de entrada y salida de estudiantes. Los padres se pueden inscribir a un servicio de mensajes sms en sus teléfonos móviles con el paradero de su hijo en un momento dado (www.cr80news.com, 2010).

2.5.4 Biométrica combinada con tecnología RFID en auto-identificación

2.5.4.1 Introducción

En los últimos años se ha producido un gran desarrollo en el campo de la auto-identificación. Se han investigado nuevos sistemas biométricos que permiten dotar al sistema de mayores tasas de fiabilidad y seguridad y en el campo de la auto-identificación mediante radio frecuencia se han estudiado nuevos sistemas que permiten al usuario utilizarlos de una manera cómoda y ágil. Estos estudios, han sido enfocados de manera independiente y si bien es cierto que los sistemas biométricos siempre serán más seguros que cualquier otra técnica de auto-identificación dado el carácter irremplazable e insustituible de los elementos de reconocimiento no dejan de presentar ciertos problemas a la hora de su utilización en cuanto a la comodidad de su uso y su aceptación por parte de la sociedad.

En este apartado se detallan algunos de los sistemas que ponen en práctica la combinación de estas dos tecnologías (biometría y RFID) en el campo de la auto-

identificación. Se describen a continuación algunos casos prácticos que están empezando a surgir.

2.5.4.2 Ejemplos prácticos

2.5.4.2.1 Broadcom y Privaris

En 2006 el fabricante de semiconductores Broadcom lanzó un chip procesador que requería la autorización mediante huella digital para que la etiqueta RFID diera los datos integrados en ella ().

El chip del procesador de Broadcom fue un decidido paso adelante en la seguridad de las aplicaciones RFID usando la tecnología RFID y biométrica en tándem. Si una huella digital no coincide con aquella que esta almacenada, la información integrada en la etiqueta RFID no será accesible.

El chip está diseñado para ser utilizado para aplicaciones de acceso seguro a las áreas físicas y dispositivos tales como ordenadores portátiles.

Privaris es una empresa que ha desarrollado el sistema “fob” que utiliza el procesador Broadcom. Su “fob” trabaja en diferentes canales de comunicación () :

• 125 kHz RFID (tarjetas de proximidad)

• 13,56 MHz RF (tarjetas inteligentes sin contacto - el apoyo a ISO 14443 A y B, ISO 15693, y NFC)

• ISO 7816 y cumple CCID – compatible con el estándar de Microsoft Windows ® inteligente tarjeta de infraestructura para el inicio de sesión de equipo

• ™ Bluetooth

• IEEE 802.15.4 (para aplicaciones de largo alcance tales como el acceso de la puerta)

Como características principales destacan que:

Soporta múltiples instalaciones y múltiples formatos de tarjetas para los actuales sistemas de lector de la puerta.

Proporciona acceso a los recursos de TI tales como aplicaciones de PC's, sitios web, correo electrónico VPN, y los archivos cifrados

Ofrece el acceso de vehículos a distancias de hasta 100 metros

Almacena de forma segura y transmite hasta 2 MB de credenciales de usuario (tales como contraseñas, códigos de construcción de acceso, los documentos de identidad, fotos etc.)

Todo el procesamiento de datos biométricos se realiza en el dispositivo personal de usuario por lo que no se exponen a los datos biométricos a servidores externos, lectores o bases de datos.

Trabaja en el mismo lector como los sistemas de proximidad y tarjetas inteligentes sin contacto.

Elimina la necesidad de lectores biométricos en todas las puertas.

Elimina la necesidad de una base de datos biométricos.

Tasas de falsos aceptación de 1 de cada 100.000

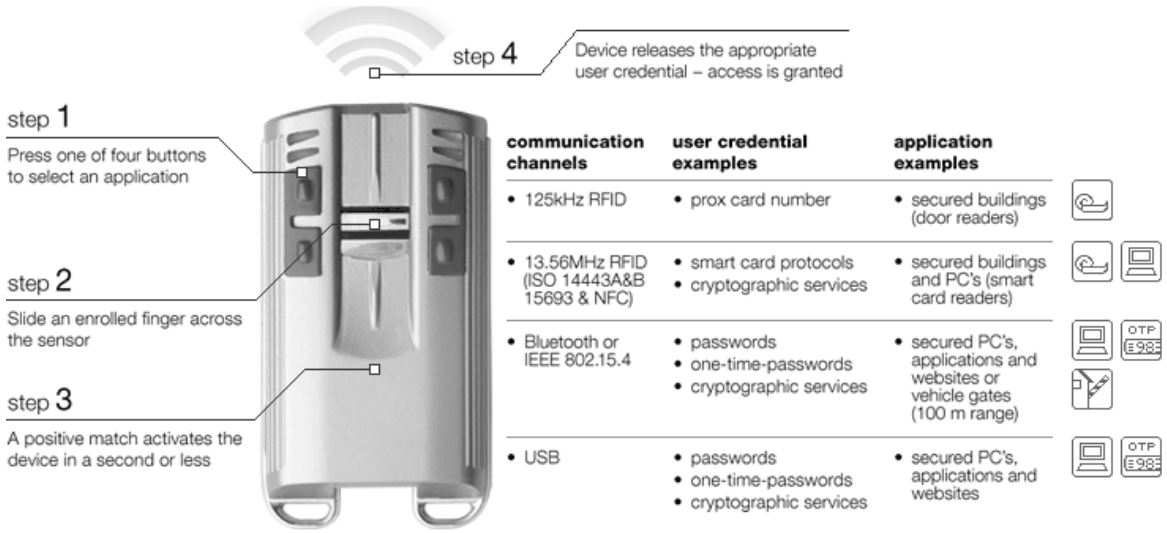


Ilustración 78.-Funcionamiento del sistema "fob"

Para los empleados que deben cumplir con las mayores necesidades de seguridad de la empresa, el sistema proporciona un dispositivo identificador no invasivo y sencillo de tal forma que la seguridad de los datos biométricos se ve mejorada sin comprometer la privacidad personal.

Las plantillas de huellas digitales se almacenan con seguridad y emparejado en el propio dispositivo, el usuario no expone los datos biométricos a servidores externos, lectores o bases de datos. Esto protege a los usuarios de la grave amenaza del robo de identidad. Si una base de datos biométricos fuera atacada y robados los datos biométricos, a diferencia de una contraseña o número de tarjeta de crédito, la huella digital no puede ser reeditada.

Ilustración 79.-Sistema "fob"

2.5.4.2.2 Empresa de transporte TransCore y Privaris

En 2005 la compañía de transporte TransCore puso en marcha un sistema seguro de control de acceso que combinaba RFID y biometría para identificar positivamente a los vehículos y los conductores en su intento por entrar en una instalación ().

El sistema funciona de forma inalámbrica, e incluye en un llavero un dispositivo biométrico de huellas dactilares que opera desde dentro del vehículo (Privaris). De esta forma se elimina la necesidad de detener el vehículo en la puerta de acceso y verificar su identidad con una fotografía.

La etiqueta RFID localizada en el parabrisas del vehículo es una etiqueta pasiva que opera a 928MHz de frecuencia, siendo un dispositivo programable que no requiere una batería o conexión con algún sistema eléctrico del vehículo. Esta pegatina esta diseñada para soportar temperaturas extremas, luz solar, humedad y vibraciones.

El sistema Privaris BPID autoidentifica al usuario a través de su huella dactilar. Antes de que el dispositivo biométrico libere la información que contiene debe verificar que el usuario es el correcto. La transmisión inalámbrica usa el protocolo IEEE 802.15.4 en la banda de radiofrecuencia de 2,4 GHz.

El sistema fue diseñado para su uso en bases militares, plantas nucleares y químicas, y otras instalaciones que requieren de múltiples capas de seguridad y control al mismo tiempo además de un acceso rápido y cómodo para los conductores autorizados.

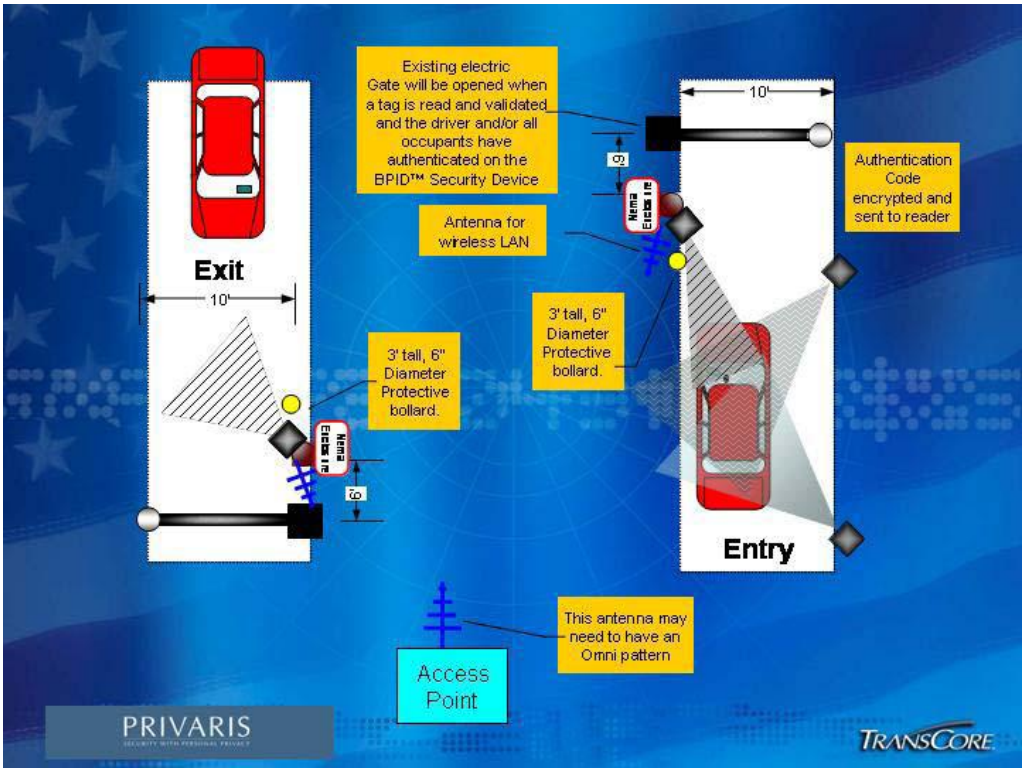


Ilustración 80.-Esquema de funcionamiento del sistema

Para la prueba inicial del sistema con los militares de EE.UU., TransCore combinó su propia tecnología RFID con el *Dispositivo de Seguridad BPID* Privaris (un dispositivo inalámbrico de mano que utiliza la autenticación biométrica de huellas digitales de su usuario antes de liberar la información sensible o confidencial.).El dispositivo no necesita una base de datos biométrica centralizada. Los datos almacenados en el

dispositivo sólo se liberan en una autenticación biométrica con éxito del usuario registrado.

Un beneficio clave en este caso es que los vehículos que no estén registrados y no se verifique la identidad del usuario, son automáticamente aislados. Dependiendo de la situación, el sistema también puede personalizarse con una serie de alarmas y acciones de contingencia para manejar las etiquetas RFID no válidas, la no autenticación biométrica, las entradas ilegales, los posibles accidentes en la entrada, y otros escenarios de riesgo para la seguridad.

2.5.4.2.3 Universidad de Deusto, Gaia y Bizgorre

La Universidad de Deusto**,** GAIA y Bizgorre han desarrollado un sistema de control de acceso basado en la identificación de personas mediante las venas de las manos. El proyecto, denominado BioGiltz (CSO) , está orientado a discapacitados con dificultades para abrir puertas con llaves tradicionales y podrá comercializarse en 2010. BioGiltz (Llave Biométrica) es el proyecto impulsado por el Cluster de Telecomunicaciones, Electrónica e Informática de Euskadi GAIA junto con la Universidad de Deusto y su centro tecnológico (grupo de investigación eVIDA-PAS) y la empresa Bizgorre. Se trata del prototipo de un sistema integral de control de acceso basado en el uso de la identificación por radiofrecuencia y el patrón biométrico de las venas de la palma de la mano, junto con técnicas de sintetización y reconocimiento de voz para la adaptación del sistema a personas con discapacidad visual, así como un mecanismo de gestión remota de la plataforma. Además, posee una serie de indicadores luminosos para facilitar su uso al colectivo de personas con discapacidad auditiva. En la actualidad está siendo testado por el grupo de investigación eVIDA-PAS de la Universidad de Deusto en Bilbao y se realizan los últimos desarrollos para la finalización del proyecto.

El sistema se utilizará como control de acceso a áreas de gran seguridad así como para facilitar el acceso a colectivos que puedan padecer dificultades para abrir puertas con llaves tradicionales. Uno de los objetivos de BioGiltz es, de hecho, mejorar la calidad de vida de personas discapacitadas y la de las personas que les asisten, eliminando las llaves de las vidas de personas invidentes o con pérdida de memoria, ya que éstas suponen una importante barrera arquitectónica. Este nuevo sistema contribuye a mantener su autonomía, facilitando el desarrollo de su vida diaria.

Ilustración 81.-Sistema BioGlitz

Por un lado, cuenta con un emisor de radiofrecuencia que lleva todo usuario que tiene permitida la entrada y un receptor de radiofrecuencia que informa al sistema de la identidad del usuario que intenta acceder a la zona. Por el otro, el sistema consta de un sensor biométrico, comercializado por Fujitsu, que una vez detectado un usuario en el entorno de la puerta espera a que éste sitúe la palma de la mano sobre el sensor. En caso de que el patrón biométrico obtenido coincida con el patrón almacenado para el usuario, el sistema comenzará el proceso de apertura de la puerta e indicará, mediante el sintetizador de voz y los indicadores luminosos, que la puerta está abierta.

El prototipo, diseñado e implementado por el Grupo Pas de la Universidad de Deusto, se ha realizado utilizando una arquitectura modular y abierta. De esta forma, la plataforma BioGiltz puede entenderse como la unión de una serie de componentes estancos, que funcionan de manera coordinada. Cada uno de estos módulos realiza una función determinada y previamente definida.

El primer bloque es el encargado de verificar la identidad de un supuesto usuario que quiere acceder a la plataforma. Para ello, se han utilizado dos de las tecnologías más novedosas: RFID y biometría. La primera de ellas se utiliza para identificar al usuario mediante la lectura de su tag RFID personal. Sin embargo, éste puede haber sufrido una pérdida del mismo, con lo que el sistema no tiene la capacidad de saber si el usuario es realmente quien dice ser. El mecanismo por el cual se verifica esta identidad es a través del uso de la biometría. Mediante la lectura del patrón biométrico del

usuario se puede verificar la identidad del mismo. Gracias a la unión de ambas tecnologías se consigue autenticar la identidad del usuario de una forma rápida y segura.

Para poder añadir y borrar usuarios en el sistema, es decir, realizar las tareas de gestión, es necesario disponer de una interfaz gráfica de usuario (GUI) y una base de datos dónde queden recogidos.

Por último, se ha desarrollado un bloque de accesibilidad que permite que la plataforma pueda ser utilizada por personas con cualquier tipo de discapacidad visual o auditiva. Mediante la unión de un sintetizador y un reconocedor de voz, el sistema es capaz de guiar a la persona por la interfaz gráfica. Solamente con el uso de la voz, el usuario podrá tener el control del programa que controla, a su vez, el sistema. Además, se han instalado unos indicadores luminosos a partir de los cuales las personas con discapacidad auditiva pueden conocer si tienen o no acceso al inmueble. (Gracias a la colaboración con la Asociación de Personas Sordas de Bilbao y Bizkaia, se han elaborado unos videos para explicar el funcionamiento de la herramienta de gestión, con textos adaptados y en lenguaje de signos. El software implementado se ha desarrollado en tres idiomas: inglés, castellano y euskera)

Cada uno de los módulos antes mencionados se compone a su vez de sub-apartados. Disponer de una arquitectura modular permite intercambiar estos componentes por otras implementaciones similares que cumplan las especificaciones; por ejemplo, aunque el prototipo construido lleva incorporado el sensor biométrico basado en el patrón de las venas de la palma de la mano realizado por Fujitsu, se puede utilizar cualquier otro sensor biométrico.

El módulo de autenticación de usuarios consta de un sensor biométrico para el que no se requirió ninguna implementación hardware, puesto que se emplea un sensor biométrico comercial, concretamente Palm Vein Secure de Fujitsu. Sí se realizó un controlador de dicho hardware, para que pueda hacerse uso del sensor desde la plataforma BioGiltz. Por otro lado, en la parte de identificación RFID se desarrolló un lector RFID integrado en una placa electrónica y el correspondiente software para dotar de lógica al mismo. Además, fue necesario implementar un mecanismo para poder comunicar este módulo con el sistema embebido, a través del puerto serie de comunicaciones (RS-232).

3 Análisis del interés de las posibles aplicaciones al campo docente.

Con el fin de entender las posibilidades reales de evolución de las tecnologías y su aplicación real es fundamental entender el apetito de la sociedad por la resolución de un problema siendo el desarrollo tecnológico el que permitirá conseguirlo con los niveles de fiabilidad y coste suficientes para conseguir su adopción como "nueva forma de hacer las cosas". De acuerdo a esta reflexión se estudió el grado de interés actual real del sector educativo en la aplicación de las tecnologías de autoidentificación. Para ello se hizo un estudio en Asturias en diferentes tipos de centros de la región buscando entender los perfiles de centro docente donde las aplicaciones de los sistemas de auto-identificación pueden resultar interesantes y dónde no.

Para la realización de este estudio, se utilizó como herramienta de recolección de información la encuesta.

3.1 Realización de la encuesta

3.1.1 Determinación de los objetivos

Los objetivos que se pretenden cubrir mediante la recolección de esta encuesta entre un público objeto que se describe en apartados posteriores son los siguientes:

- ✓ Conocer la situación tecnológica y el nivel de satisfacción de los centros docentes en Asturias.
- ✓ Conocer el nivel de conocimiento existente en referencia a la tecnología RFID y el conocimiento que poseen sobre sus aplicaciones en la vida real.
- ✓ Conocer cuáles son las características del sistema de auto-identificación aplicado a centros docentes que más importancia tienen entre el público y que son más necesarias para ellos.
- ✓ Nivel de interés general por la automatización de la identificación de los alumnos
- ✓ Conocer el soporte y localización del método de auto-identificación por parte de los alumnos

3.1.2 Determinación de la información requerida

Se debe determinar cuál será la información que se va a recabar para alcanzar los objetivos anteriormente expuestos. Se definieron una serie de preguntas intentando llegar a un compromiso razonable entre la duración de la entrevista y el grado de detalle de las preguntas con el fin de obtener un resultado óptimo.

Información sobre la titularidad, tipo de enseñanza, tecnologías implantadas y nivel de satisfacción con las mismas.

- ✓ Tipo de colegio: Público/Concertado/Privado
- ✓ Tipo de enseñanza impartida: Primaria/ Secundaria/ Bachiller/ FP
- ✓ ¿Posee biblioteca?
- ✓ ¿Utiliza algún sistema informatizado para la gestión de documentación, libros, etc.? Grado de satisfacción con el sistema utilizado
- ✓ ¿Utiliza algún sistema informatizado para gestión de listas de alumnos? Grado de satisfacción con el sistema utilizado

Grado de conocimiento sobre las tecnologías RFID y biométrica

- ✓ ¿Conoce los sistemas de auto-identificación?Ejemplos
- ✓ ¿Conoce qué es el sistema RFID (sistema de auto-identificación por radiofrecuencia)?
- ✓ ¿Conoce alguna de sus aplicaciones en la vida real?

Aplicaciones del sistema en los centros docentes

- ✓ Qué grado de interés ve a las distintas aplicaciones del sistema RFID en el ámbito docente? *Muy interesante/ Interesante/ Poco interés/ Innecesario.*

  Aplicaciones:

  - Control de asistencia automatizado de los alumnos
  - Localización de los alumnos en las diferentes áreas del local
  - Envió de sms a los padres cuando el alumno entra o sale del centro.
  - Control de accesos a diferentes áreas
  - Gestión de bibliotecas.

Nivel de interés general por la aplicación

A nivel global el sistema: No interesa/ Interesa sólo de manera gratuita/ Interesa posible estudio económico/ Ns/Nc

Localización de los elementos del sistema.

¿Dónde le parecería mejor llevar los elementos del sistema? *Tarjeta/ Pulsera/ Uniforme/ Otros.*

3.1.3 Ámbito de la encuesta

3.1.3.1 Ámbito poblacional

El universo está compuesto por los centros de docencia. A continuación se describe con más detalle este grupo.

Centros de docencia: Dentro de este grupo están incluidos el director de cada centro o en su caso el jefe de estudios o administrador.

Los centros de docencia que se estudiarán serán según el tipo los siguientes:

COL: Colegio privado o concertado
C.P.: Colegio público
I.E.S.: Instituto de Enseñanza Secundaria

Atendiendo al nivel de enseñanza los centros encuestados serán:

- ✓ Infantil
- ✓ Primaria
- ✓ Enseñanza Secundaria
- ✓ Bachiller
- ✓ Formación Profesional

3.1.3.2 Ámbito geográfico

El estudio se realizará a centros docentes dentro del ámbito regional de Asturias concretamente en los 3 municipios con mayor población:

Municipio	Población (ambos sexos)
Gijón	277.554
Oviedo	224.005
Avilés	84.242
Otros	499.488
Total	1.085.289

Tabla 3.1.-Población por municipios. Fuente: Instituto Nacional de Estadística (2009)

En la figura 7.1 se puede observar gráficamente la proporción de población en estos municipios:

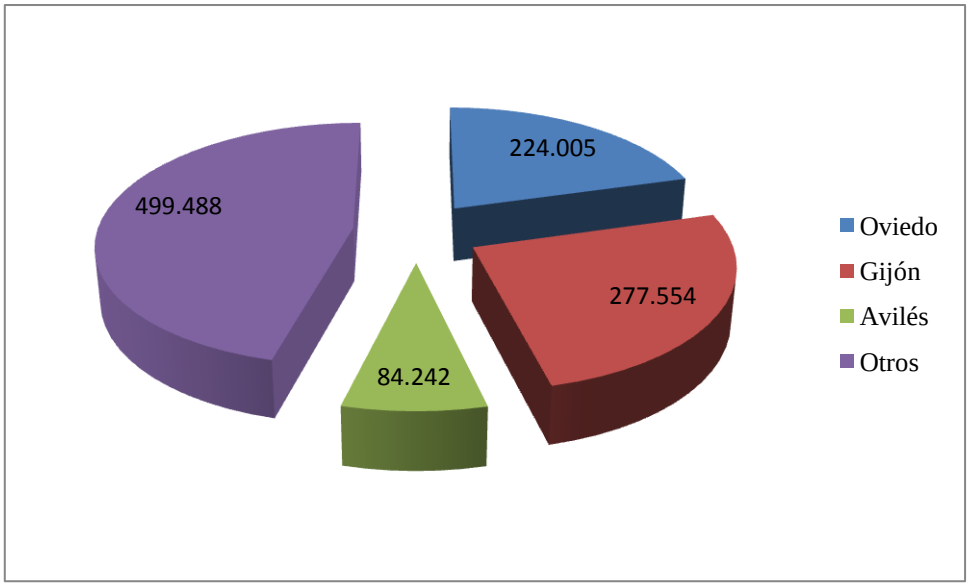


Figura 3.1.- Población de los principales municipios en Asturias.

3.1.3.3 Marco temporal

Las encuestas se realizaron en mayo de 2010.

3.1.4 Diseño del cuestionario

A continuación se describe la definición adoptada para el cuestionario y la ejecución de la encuesta.

3.1.4.1 Presentación

En la presentación se deben indicar los datos sobre el organismo responsable de la encuesta y el proyecto en el que se encuadra.

El estudio se enmarca en el proyecto “Análisis de posibilidades de tecnologías de auto-identificación para la ubicación de personas y su aplicación a centros docentes” de la Universidad de Oviedo en colaboración con la empresa Oxígeno Empresarial de Gijón para determinar las posibles mejoras en seguridad y gestión de los centros docentes gracias a la implantación de sistemas de auto-identificación.

3.1.4.2 Tiempo requerido

La encuesta tendrá una duración estimada de 10 minutos.

3.1.4.3 Breve descripción de los objetivos y explicación del sistema

A través de esta encuesta se pretende dar luz a las posibles mejoras dentro del ámbito docente en cuanto a seguridad y gestión que permitan realizar estas tareas de manera más sencilla y eficaz proporcionando tanto al alumno como al centro las herramientas adecuadas para mejorar así la calidad docente mediante el uso de sistemas de auto-identificación por radiofrecuencia.

Se pretende asimismo determinar el perfil de centro que muestra mayor interés hacia las aplicaciones de técnicas de auto-identificación

El sistema de auto-identificación conocido por sus siglas RFID (identificación por radiofrecuencia) consiste en aplicar la radio frecuencia para la identificación, por lo que nos permite identificar objetos o personas mediante ondas radio, es decir a distancia. Es un paso hacia delante para las tecnologías de identificación automática.

Se puede encontrar el uso de esta tecnología en aplicaciones de la vida cotidiana como puede ser en las bibliotecas, la tarjeta ciudadana de Gijón, el pasaporte emitido actualmente o en el uso de esta tecnología en hospitales para control de pacientes o recién nacidos.

Gracias a las enormes ventajas que nos ofrece esta tecnologías (mayor velocidad de información, eliminación del error humano, mejora de la eficiencia y flexibilidad, mejora de la seguridad y mayor comodidad de uso) los centros docentes pueden ver

incrementado su eficiencia y seguridad a través de las distintas aplicaciones del sistema.

3.1.4.4 Preguntas

Centros de docencia

Datos generales

1.-Tipo de centro
2.-Tipo de estudios impartidos
3.- ¿El centro posee biblioteca?
4.1.-¿Se encuentra gestionada mediante algún tipo de programa informático?
4.2-En caso afirmativo responda ¿cuál?
5.-Las tareas administrativas se encuentran gestionadas mediante algún programa informático?
5.1- En caso afirmativo, ¿cuál?

Conocimientos de la tecnología

1.-¿Sabe que son los sistemas de auto-identificación?
2.-¿Conoce algún ejemplo de sistema de auto-identificación?
2.1.- En caso afirmativo, ¿cuál?
3.-¿Conoce el sistema RFID?
3.1. En caso afirmativo, ¿Conoce alguna de sus aplicaciones?

Implantación del sistema

1.- Califique como muy interesante/interesante/práctico/no necesario las siguientes ventajas que puede ofrecer la implantación del sistema de auto-identificación en el centro docente:

Localización en tiempo real del alumno dentro del centro.

Mediante esta característica el alumno poseedor de un sistema identificativo (tarjeta, pulsera…) puede estar localizado en tiempo real sabiendo en qué aula se encuentra. Los lectores colocados detectan al alumno y se puede llegar a visualizar su ubicación a través de un sinóptico colocado donde el centro considere necesario. Esta medida se puede enfocar desde el modo preventivo, puesto que en caso de algún tipo de incidente se podría tener localizado a todos los alumnos en tiempo real.

Posibilidad de enviar mensajes al teléfono móvil de los padres para indicar si su hijo se encuentra en el centro o ya ha salido.

El alumno poseedor del sistema identificativo queda registrado en su entrada o salida del centro a través de lectores colocados en las salidas del mismo. De manera automática se puede enviar un mensaje al teléfono móvil de los padres que así lo deseen alertándoles de la salida o entrada del alumno.

Control de accesos a diferentes áreas del centro

Los alumnos pueden tener acceso a diferentes áreas del centro dependiendo del curso que estén realizando o de su edad. El acceso puede ser a laboratorios, gimnasio, biblioteca etc.

Identificar al alumno automáticamente sin necesidad de pasar lista

A través de este sistema el alumno quedaría registrado automáticamente y no es necesario pasar lista e introducir manualmente los datos en el sistema informático.

Gestión de las bibliotecas mediante sistema RFID

Mediante este sistema y en sustitución del sistema de código de barras implantado en la totalidad de bibliotecas escolares que se encuentran informatizadas se pueden realizan inventarios de manera más cómoda y eficiente, dado que el lector es capaz de leer simultáneamente diversos

libros. Además se puede realizar el auto-préstamo y auto-devolución por parte de los alumnos

2.- ¿Le interesaría implantar estas características a nivel general en el centro?

3.- ¿Dónde le parece más eficaz que el alumno lleve la etiqueta identificadora?

3.1.4.5 Sugerencias

Se introduce en la encuesta un párrafo donde se invita al encuestado a realizar cualquier otro tipo de comentario o duda que pudiera surgir en la resolución del mismo. De esta forma, el encuestado puede mostrar su interés por ampliar sus conocimientos sobre el sistema o sugerir alguna posible mejora dentro del ámbito docente.

3.1.4.6 Agradecimientos

Se agradece a todos los encuestados su interés y su disponibilidad en la realización de la encuesta.

3.1.5 Determinación de la muestra

Se calcula a continuación el número de muestras para el grupo.

Número de centros encuestados

La realización del estudio será a nivel regional de Asturias realizándose el estudio entre los centros de los 3 núcleos más poblados en la región (Gijón, Oviedo y Avilés) sondeando a los distintos tipos de centros de docencia existentes en Asturias.

Los centros de docencia entre los 3 núcleos poblacionales descritos anteriormente según el tipo son los siguientes:

Tipo	Número de centros
Colegio (privado o concertado)	41
Colegio público	71
Instituto de Enseñanza Secundaria	29
Total	141

Tabla 3.2. Número de centros según el tipo.

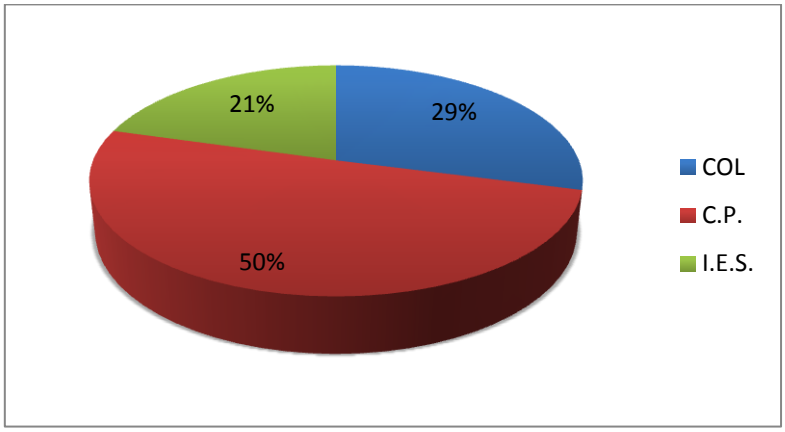


Figura 3.2.- Proporción de centros según el tipo.

Municipio	Número de centros
Gijón	65
Oviedo	54
Avilés	22
Total	141

Tabla 3.3.- Número de centros distribuidos entre los 3 municipios

En este caso como la población es finita, conocemos el número exacto de centros existentes entre estas 3 poblaciones, se calculará la muestra mediante la siguiente fórmula:

$$n = \frac{N * Z_{\alpha}^{2} p * q}{d^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

Donde:

N: Es el tamaño de la población o universo (número total de posibles encuestados).

Z: Es una constante que depende del nivel de confianza que asignemos. El nivel de confianza indica la probabilidad de que los resultados de la investigación sean ciertos: un 95,5 % de confianza es lo mismo que decir la probabilidad de equivocarse es del 4,5%.

Los valores de Z más utilizados y sus niveles de confianza son los siguientes:

Z	1.15	1.28	1.44	1.65	1.96	2	2.58
Nivel de confianza (%)	75	80	85	90	95	95.5	99

Tabla 3.4. Nivel de confianza

d: Es el error muestral deseado. El error muestral es la diferencia que puede haber entre el resultado que se obtiene preguntando a una muestra de la población y el que se obtendría si se pregunta al total de ella.

p: Es la proporción de individuos que poseen en la población la característica de estudio. Este dato es generalmente desconocido y se suele suponer que p=q=0.5 que es la opción más segura.

q: Es la proporción de individuos que no poseen esa característica, es decir, es 1-p.

n: Es el tamaño de la muestra (número de encuestas que se van a realizar).

Se toma para el cálculo de la muestra los siguientes datos:

N	**141**
Z	1.65
d (%)	10
p	0.5
q	0.5

Tabla 3.5. Datos de la muestra

Resultando un tamaño de la muestra de:

n	**46 centros**

Para realizar las encuestas se desarrolla un muestreo aleatorio estratificado, considerando que los 3 núcleos poblacionales estudiados no poseen la misma proporción de centro cada uno. Por ello se realizará una afijación proporcional de acuerdo al tamaño (número de centros) que hay en cada municipio.

Por ello con los datos de la tabla 7.3 se elabora una muestra proporcional de centros encuestados

Municipio	Número de centros
Gijón	65
Oviedo	54
Avilés	22
Total	141

Tabla 3.6.- Número de centros en cada municipio

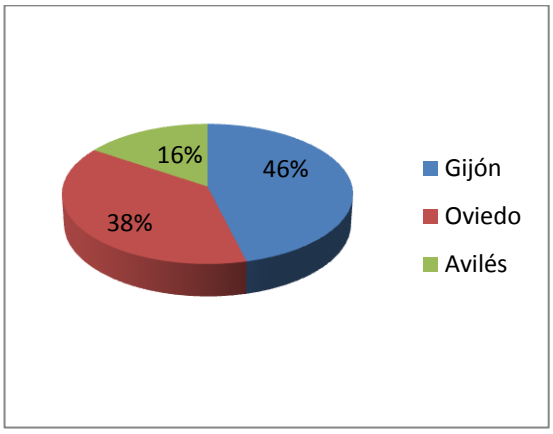


Figura 3.3.-Proporción número de centros en cada municipio

Municipio	Número de centros
Gijón	21
Oviedo	18
Avilés	7
Total	46

Tabla 3.7.- Número de centros encuestados en cada municipio

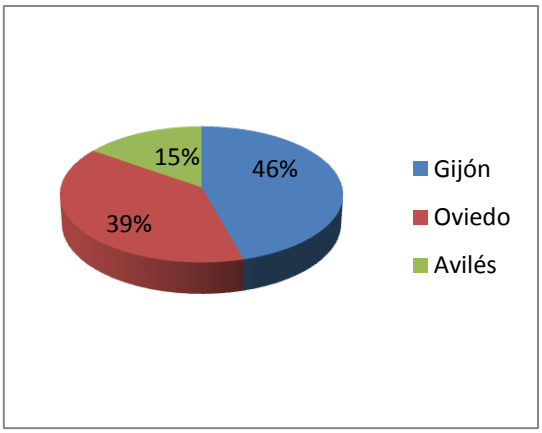


Figura 3.4.- Proporción del número de centros encuestados en cada municipio.

En resumen, la muestra tendrá las siguientes características:

Universo	**Centros docentes (colegios públicos, privados o concertados) e institutos de enseñanza secundaria en los municipios de Gijón, Oviedo y Avilés en Asturias N=141**
Tamaño de la muestra	n=46 encuestas
Unidad de muestreo	Directores, jefes de estudio, secretarios o administradores de los centros docentes
Selección de la muestra	Muestreo aleatorio estratificado, afijación proporcional respecto al tamaño poblacional de cada municipio
Error muestral	±10%
Nivel de confianza	90%

Tabla 3.8.- Resumen de características de la muestra

3.1.6 Trabajo de campo

Para cumplir el objetivo de muestreo con los recursos disponibles se decide realizar las encuestas mediante el método de encuesta telefónica.

3.1.7 Conteo y codificación de resultados

La muestra a estudiar como se ha descrito en apartados anteriores está compuesta por 46 centros docentes localizados en los 3 municipios de mayor población en Asturias.

A continuación se muestra el listado de centros encuestados. El 100% de los centros denominados c.p. (colegio público) imparten enseñanza infantil y primaria, mientras que en los col (colegio privado o concertado) se imparte tanto enseñanza infantil, primaria como secundaria y en el 27% de los casos imparten también módulos de formación profesional. Por su parte los I.E.S. (institutos de enseñanza secundaria) imparten en su totalidad enseñanza secundaria obligatoria y bachiller y el 25% de ellos también imparten ciclos formativos de grado medio o superior.

	Tipo centro	Localidad
Alfonso Camín	c.p.	Gijón
Alfonso II	i.e.s.	Oviedo
Áramo	i.e.s.	Oviedo
Asturias	c.p.	Gijón
Baudillo Arce	c.p.	Oviedo
Begoña	c.p.	Gijón
Carreño Miranda	i.e.s.	Avilés
Clarín	c.p.	Gijón
Corredoira	i.e.s.	Oviedo
Doctor Fleming	i.e.s.	Oviedo
Eduardo Martínez Torner	c.p.	Gijón
El llano	c.p.	Gijón
El Piles	i.e.s.	Gijón
Evaristo Valle	c.p.	Gijón
Fernández Vallín	i.e.s.	Gijón
Fundación Masaveu	COL	Oviedo
Germán Fernández Ramos	c.p.	Oviedo
Guillen LaFuerza	c.p.	Oviedo
Honesto Batalón	c.p.	Gijón
Jovellanos	i.e.s.	Gijón
Julián Gómez Elisburu	c.p.	Gijón
La Corolla	COL	Gijón
La Eria	c.p.	Oviedo
La Eria	i.e.s.	Oviedo
La Inmaculada	COL	Gijón

La Magdalena	i.e.s.	Avilés
La Milagrosa	COL	Gijón
Leopoldo Alas Clarín	i.e.s.	Oviedo
López y Vicuña	COL	Gijón
Loyola	COL	Oviedo
Manuel Martínez Blanco	c.p.	Gijón
Marcelo Gago	c.p.	Avilés
Mata Jove	i.e.s.	Gijón
Mauristas Auseva	COL	Oviedo
Menéndez Pelayo	c.p.	Oviedo
Monte Naranco	i.e.s.	Oviedo
Pando	i.e.s.	Oviedo
Ramón Menéndez Pidal	i.e.s.	Avilés
Rosario Acuña	i.e.s.	Gijón
San Fernando	COL	Avilés
San Ignacio	COL	Oviedo
San Miguel	COL	Gijón
Santo Tomas	COL	Avilés
Severo Ochoa	c.p.	Gijón
Veneranza Manzano	c.p.	Oviedo
Versalles	c.p.	Avilés

Tabla 3.9. Listado de centros encuestados

De los 46 centros el 46% pertenecen al municipio de Gijón, el 38% a Oviedo mientras que el 16% imparten docencia en Avilés. Dentro de los tres tipos posibles de centros el 41% de los centros son colegios públicos, el 35% institutos de enseñanza secundaria y el 24% restante pertenecen a colegios privados o concertados.

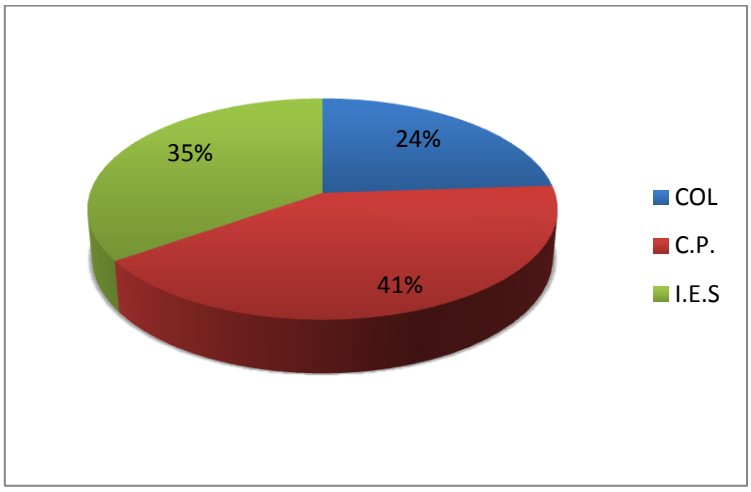


Figura 3.5. Distribución de centros encuestados según tipo.

3.1.7.1 Conocimiento de la situación tecnológica de los centros docentes y su nivel de satisfacción

Para conocer la denominada situación tecnológica de los centros docentes, se busca conocer si se realizan las gestiones de manera informatizada o en cambio se realizan manualmente y por otra parte, se busca conocer si poseen biblioteca y si ésta se encuentra gestionada también de manera informatizada. Además se desea averiguar el grado de satisfacción que poseen con los programas informáticos.

En los colegios públicos y en los institutos de enseñanza secundaria éstos deben utilizar unos programas determinados para la gestión de bibliotecas y gestión administrativas:

Abies: El programa de gestión de las bibliotecas escolares Abies es una herramienta que facilita la organización de la biblioteca: catalogación, tejuelado, préstamo...

Se presenta en un CD-ROM que contiene el programa y un depósito de 400.000 referencias bibliográficas de literatura infantil y juvenil, extraídos de los fondos de la Biblioteca del MEC, de la Nacional, de las Bibliotecas Públicas y de la Fundación Germán Sánchez Ruipérez. Este depósito facilita las labores bibliotecarias.

Sauce: El Sistema para la Administración Unificada de Centros Educativos es la aplicación de gestión académica y administrativa de los centros educativos asturianos.

Se encuentra en el área de aplicaciones del portal de la Intranet Educativa.

Los colegios concertados o privados, deben utilizar algunas partes del programa Sauce pero otras gestiones pueden ser realizadas mediante otros programas informáticos y las bibliotecas no tienen por qué ser gestionadas mediante Abies.

Es por ello, que en el caso de los colegios públicos y en el de los institutos se preguntó sobre el grado de satisfacción en el uso de los programas anteriormente descritos dado que son obligatorios en estos centros. El 100% de los centros

encuestados poseen biblioteca por lo que también se les preguntó sobre el grado de satisfacción con el programa Abies.

La puntuación de los programas va desde 1 a 4 siendo la escala de puntuación la siguiente:

Calificación	Puntuación
Muy bueno	4
Bueno	3
Aprobado	2
Necesita mejorar	1
Ns/Nc	-

Tabla 3.10.- Escala de puntuación

Como se pueden ver en los gráficos siguientes, el programa Abies goza de una buena puntuación entre los centros teniendo una nota media de 3,18 sobre 4 en los colegios públicos y una nota de 2,85 sobre 4 en los institutos. Las desviaciones típicas son respectivamente 0,38 y 0,53.

El programa Sauce por su parte obtiene una media de 2,26 en los colegios públicos con una desviación de 0,96. En los institutos la media se sitúa en 2,13 y su desviación es 0,88.

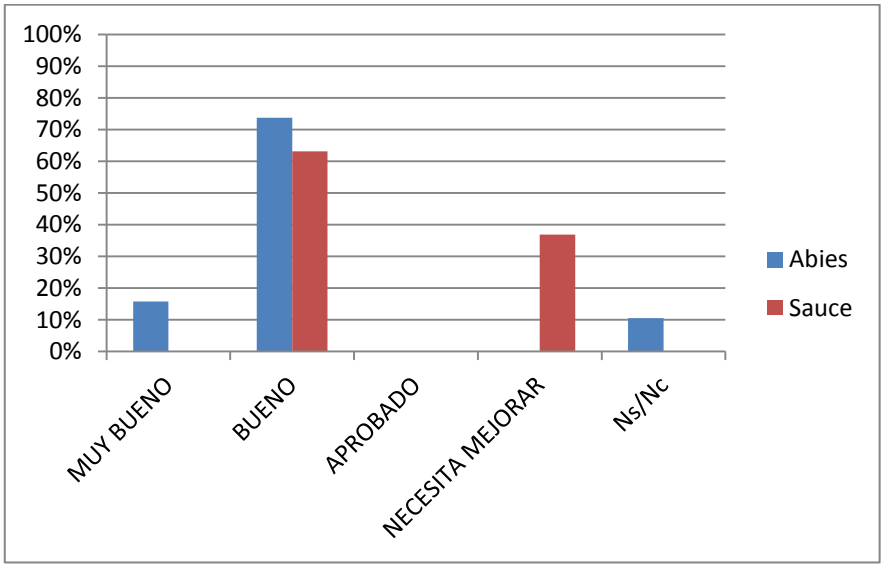


Figura 3.6.- Grado de satisfacción del programa Abies y Sauce en los centros públicos de enseñanza primaria.

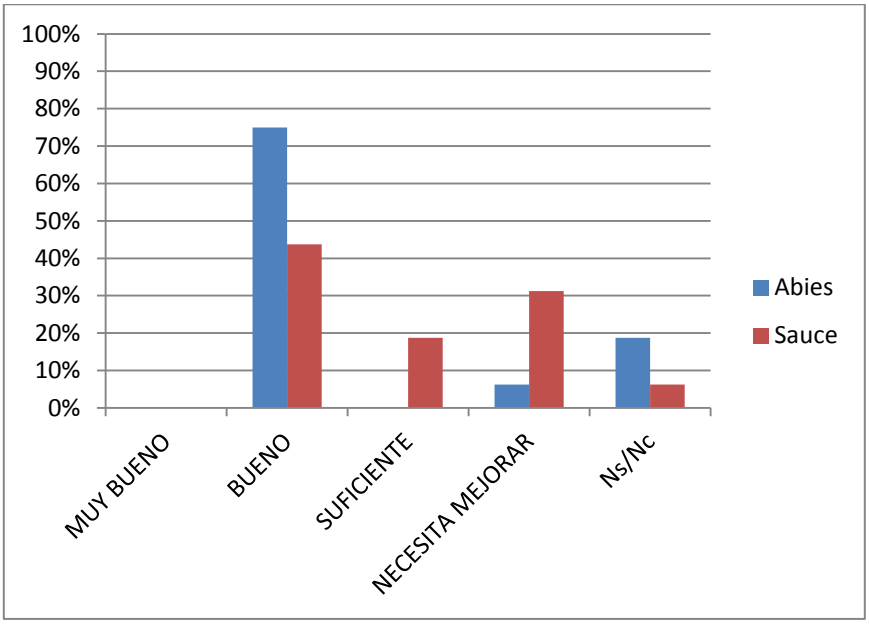


Figura 3.7.- Grado de satisfacción del programa Abies y Sauce en los institutos de enseñanza secundaria.

Por su parte, un 54% de los colegios privados o concertados poseen bibliotecas gestionadas informáticamente mientras que el 27% afirma utilizarla con métodos manuales y el 18% restante se encuentra en estos momentos informatizándola.

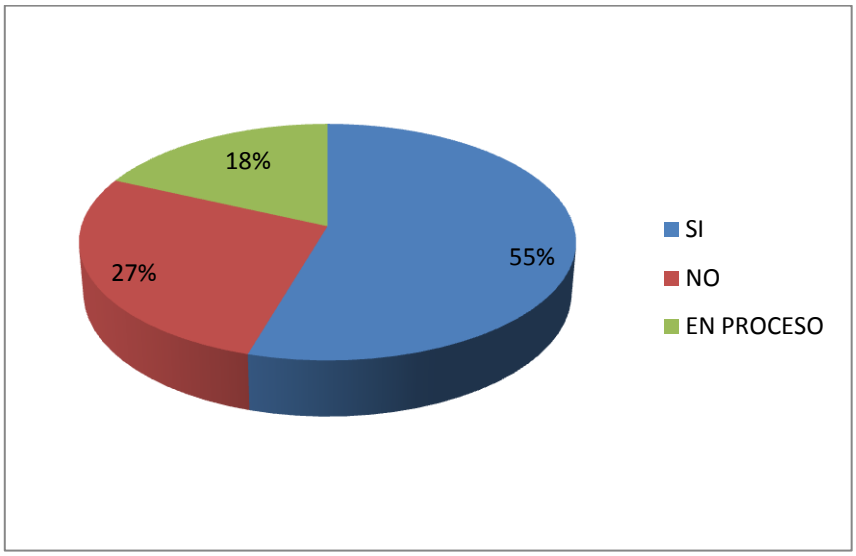


Figura 3.8.- Informatización de la biblioteca

En aquellos centros donde la biblioteca no se encuentra informatizada no ven la necesidad de realizarlo dado que su uso es muy minoritario puesto que los alumnos pueden buscar información a través de salas de internet existentes en los centros. Aquellos que están informatizándolas lo hacen en su totalidad mediante código de barras.

En cuanto a la gestión administrativa, este tipo de centros debe usar para determinadas acciones el programa Sauce y para el resto se utilizan programas propios de cada centro. En referencia al grado de satisfacción con el programa Sauce en particular la media se encuentra en 3 siendo la desviación típica de 0,47. Los porcentajes se muestran en la figura que sigue a continuación.

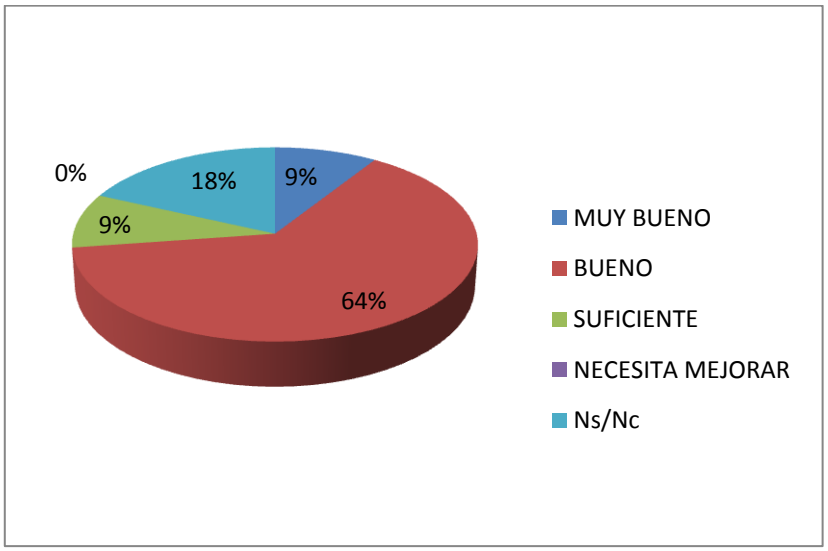


Figura 3.9.- Grado de satisfacción con el programa Sauce de los colegios privados o concertados.

Las principales desventajas en general para todo tipo de centros que presenta Sauce entre los colegios que calificaron al programa como "Necesita mejorar" según el grado de frecuencia son:

- Sobrecarga de red en determinadas fechas. Lentitud del programa
- Maniobrabilidad deficiente: Es necesario volver al mismo menú para ir a determinados sitios lo que hace el programa poco ágil.
- Dificultad de generar documentos propios
- Dificultad para realizar convocatorias de inventarios.

3.1.7.2 Nivel de conocimiento existente en referencia a la tecnología RFID y el conocimiento que poseen sobre sus aplicaciones en la vida real.

En general, al preguntar sobre el grado de conocimiento de los sistemas RFID (identificación por radiofrecuencia) un 89% afirma no conocer qué son este tipo de sistemas ni para qué se utilizan frente a un 11% que afirma conocerlos.

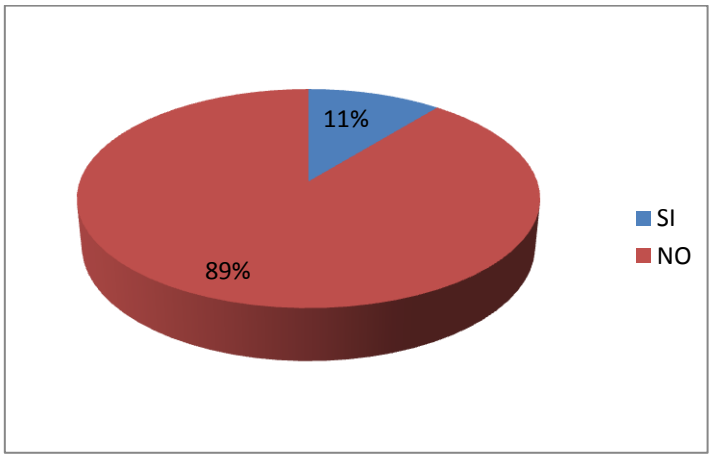


Figura 3.10.- Porcentaje de centros que conocen o no qué es la tecnología RFID

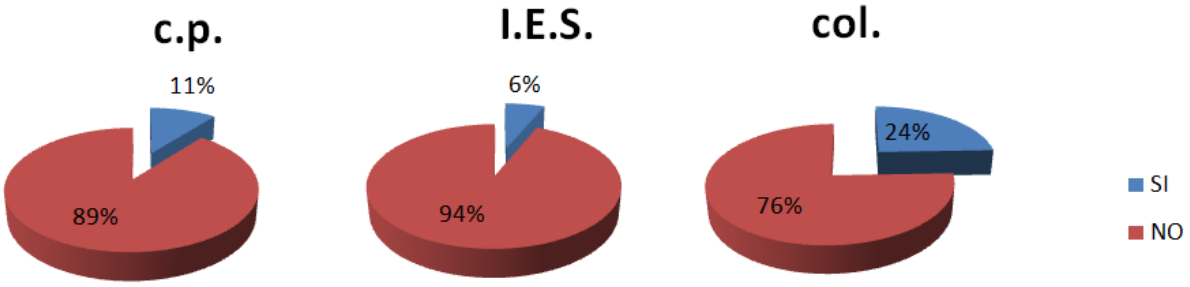


Figura 3.11. Porcentaje según tipo de centro

En general las personas encuestadas de los centros muestran su desconocimiento sobre este tipo de tecnologías pero sí reconocen utilizarlas en el caso por ejemplo de la tarjeta ciudadana de Gijón aunque desconociendo el tipo de tecnología que utilizaban.

3.1.7.3 Conocer cuáles son las características del sistema que más importancia tienen entre el público objeto y que son más necesarias para ellos.

Se busca encontrar que características del sistema causan mayor interés entre los diferentes tipos de centros y cuáles resultan innecesarias. Las características que se comentan son las siguientes:

- ✓ Localización en tiempo real del alumno dentro del centro.
- ✓ Posibilidad de enviar mensajes al teléfono móvil de los padres para indicar si su hijo se encuentra en el centro o ya ha salido.
- ✓ Control de accesos a diferentes áreas del centro
- ✓ Identificar al alumno automáticamente sin necesidad de pasar lista
- ✓ Gestión de las bibliotecas mediante sistema RFID.

La puntuación según el grado de interés que muestren los centros hacia las distintas características en particular son las siguientes:

Calificación	Puntuación
Muy interesante	4
Interesante	3
Poco interesante	2
No necesario	1
Ns/Nc	-

Tabla 3.11.- Puntuación dependiendo de la calificación otorgada por los centros

Para tener una visión global de todas las características, se muestra a continuación unos gráficos donde se observa el porcentaje de las distintas puntuaciones otorgadas a todas las características según el tipo de centro encuestado. A continuación se irán desglosando las características una a una para un análisis más profundo.

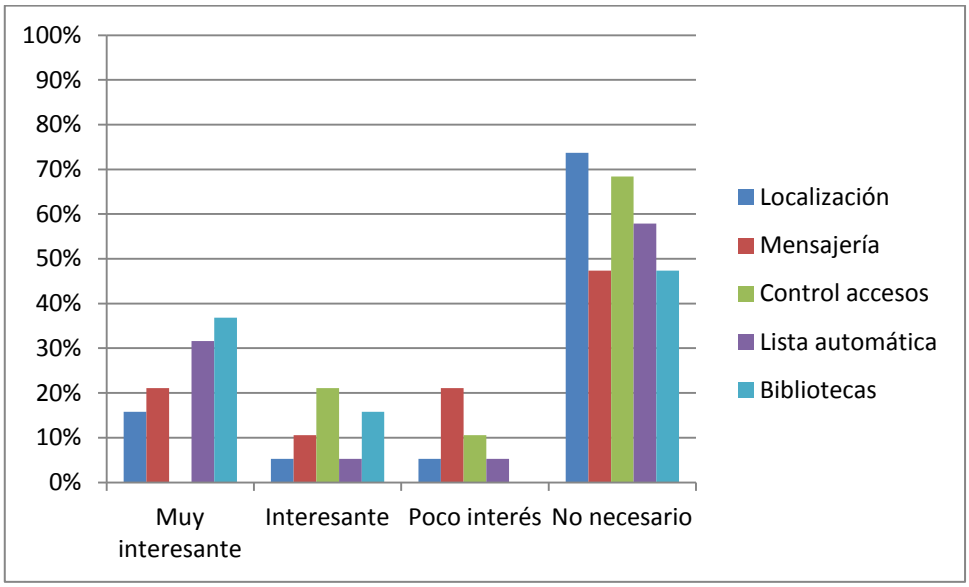


Figura 3.12.- Porcentajes de centros públicos atendiendo a su nivel de interés por las diferentes características

Atendiendo a la figura anterior, se observa que los mayores porcentajes se sitúan en la calificación "No necesario" obteniéndose un 73% para la localización, un 47% para la mensajería móvil, un 58% para el control de accesos, un 47% para la lista automática y un 47% para la automatización de bibliotecas a través de RFID. No obstante cabe destacar que un 37% de los encuestados muestran como muy interesante el sistema RFID para bibliotecas y un 32% muestra también su interés por la lista automática.

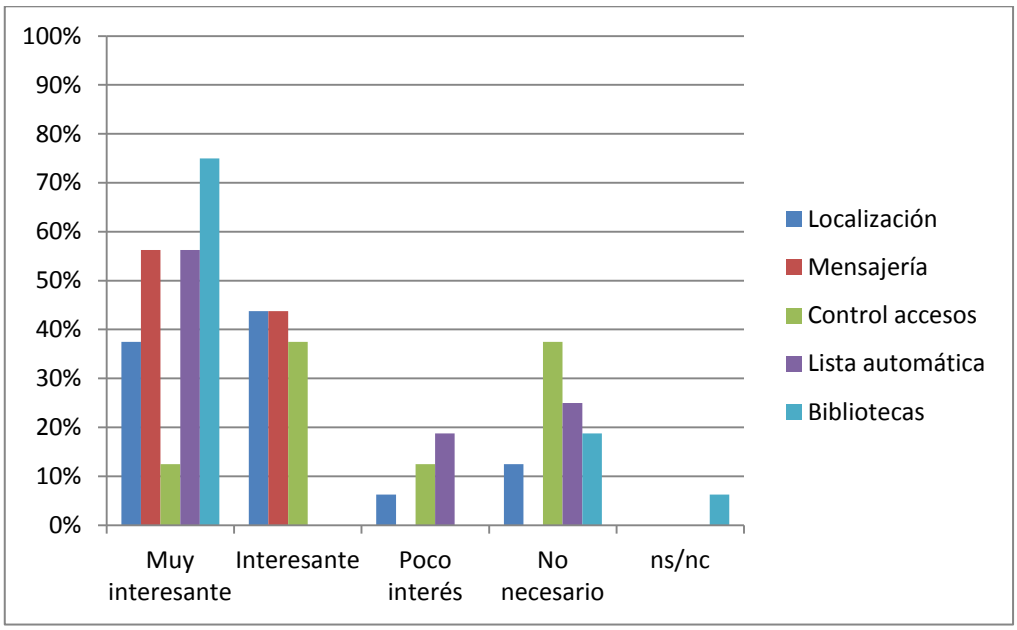


Figura 3.13.- Porcentajes de I.E.S atendiendo a su nivel de interés por las diferentes características

En el caso de los institutos de enseñanza secundaria sin embargo, se observa una tendencia de las diferentes características como muy interesante a excepción del control de accesos al que sólo consideran como muy interesante el 12% de los centros encuestados frente al 37% que lo considera innecesario.

Cabe destacar los buenos porcentajes que obtiene la alerta de entrada y salidas del alumno mediante el móvil con un 56% como muy interesante y un 43% como interesante. La lista automática también obtiene buenos resultados con un 56% que considera la característica como muy interesante. Por último la localización del alumno ofrece también resultados positivos al situarse con un 38% en muy interesante y un 44% en interesante.

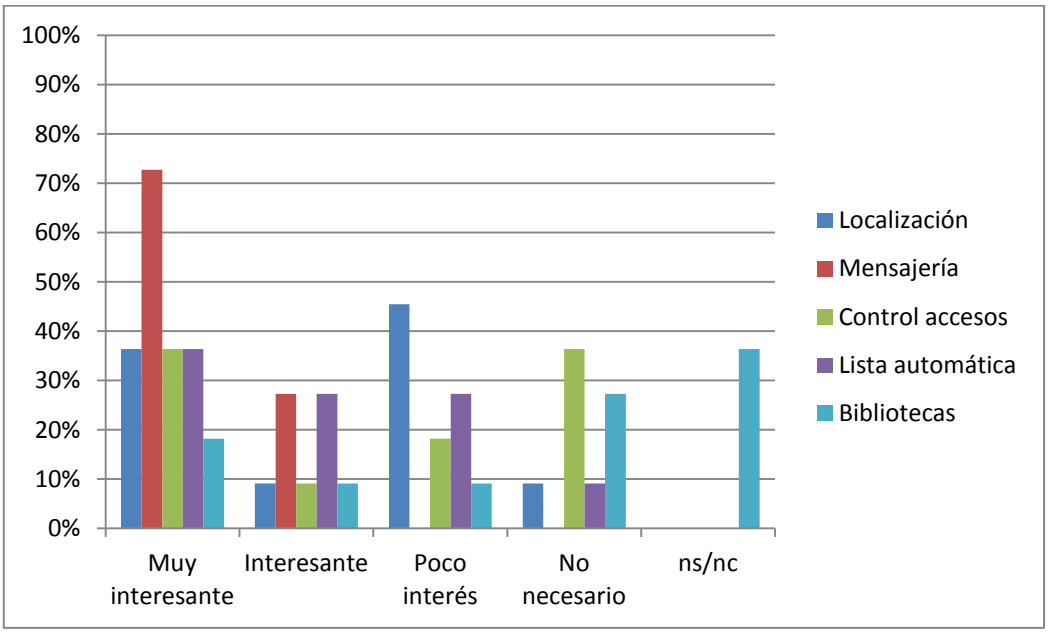


Figura 3.14.- Porcentajes de colegios privados o concertados atendiendo a su nivel de interés por las diferentes características

En el caso de los colegios privados o concertados destaca por encima de todas las características el aviso de la salida o entrada del alumno a través de sms a los padres con un 73% de los centros que lo consideran como muy interesante y el 27% restante lo considera interesante. Como en el caso de los colegios privados o

concertados el 45% de ellos no se encuentran informatizados o los que están en proceso lo están haciendo mediante código de barras esta característica no poseen mucha puntuación obteniéndose que un 27% no lo consideran necesario y un 36% no sabe o no contesta.

A continuación se desglosa cada característica particularmente:

Localización en tiempo real del alumno dentro del centro.

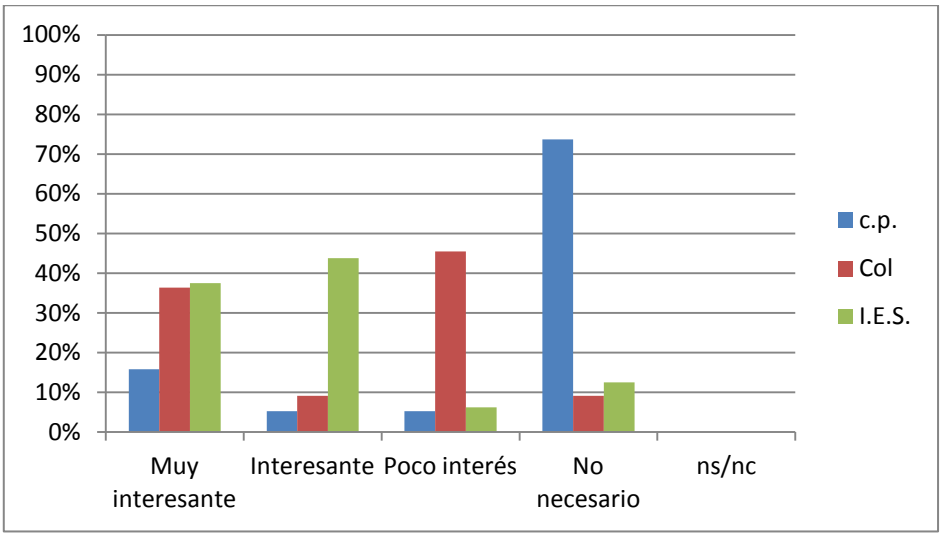


Figura 3.15.- Localización en tiempo real del alumno

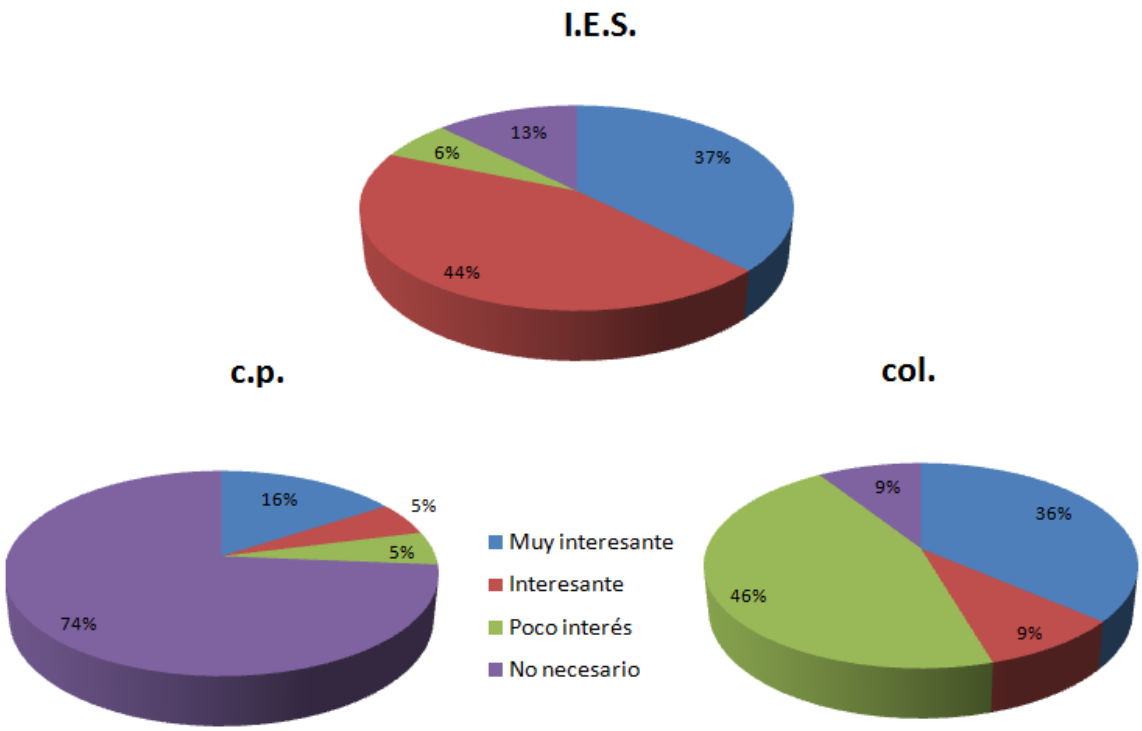


Figura 3.16.- Diagrama de sectores

Se observa que esta característica posee poco o ningún interés entre los centros públicos de enseñanza primaria -74% de los centros consideran no necesaria su

implantación- y los centros concertados o privados -46% de los centros consideran de poco interés esta característica. Sin embargo frente a este porcentaje un 36% lo considera muy interesante. Esta diferencia de criterio se debe en muchos casos a la diferencia de tamaño de los distintos centros entrevistados considerando esta opción interesante en aquellos centros cuyas dimensiones y número de alumnos es elevado. Lo mismo ocurre con los I:E:S, donde el tamaño y el número de alumnos es superior al de los colegios de primaria y donde el interés por está opción esta en el 37% como muy interesante y 44% como interesante.

Posibilidad de enviar mensajes al teléfono móvil de los padres para indicar si su hijo se encuentra en el centro o ya ha salido.

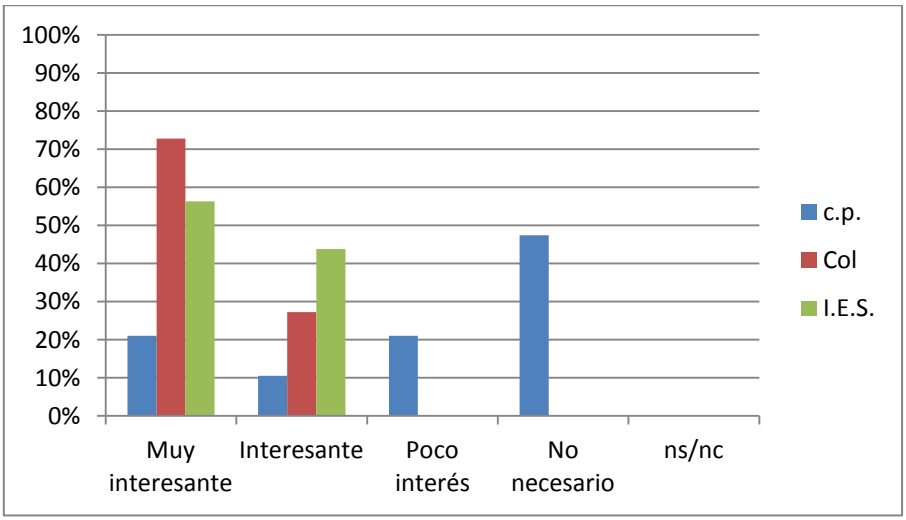


Figura 3.17.- Mensajes a los padres en caso de salida o entrada del alumno en el centro

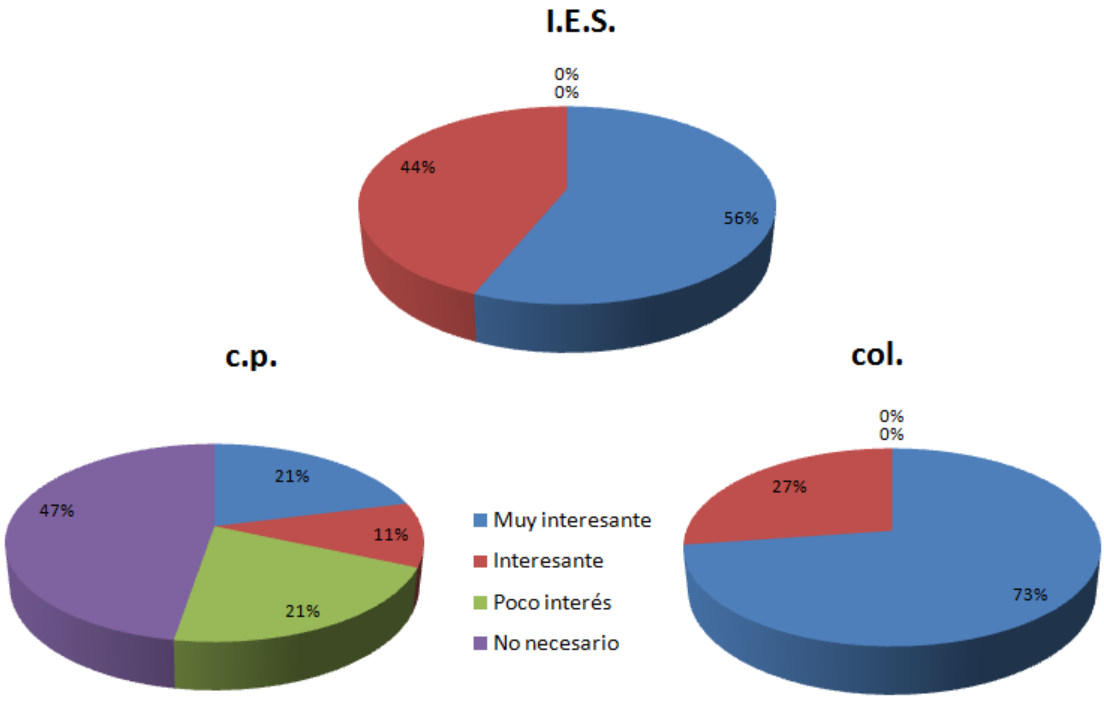


Figura 3.18.- Diagramas de sectores

En este caso, tanto los colegios privados o concertados como los institutos muestran su interés por esta característica. Un 73% de los colegios privados o concertados entrevistados considera esta función como muy interesante y el 27% restante como interesante. Los institutos de enseñanza secundaria también muestran su interés con un 56% de ellos que lo consideran muy interesante el restante 43% como interesante.

Por el contrario los centros de primaria públicos consideran esta función innecesaria -47%- debido a que los niños de infantil y primaria donde ellos imparten clase se encuentran permanentemente vigilados por los profesores a su cargo y son grupos pequeños.

Control de accesos a diferentes áreas del centro

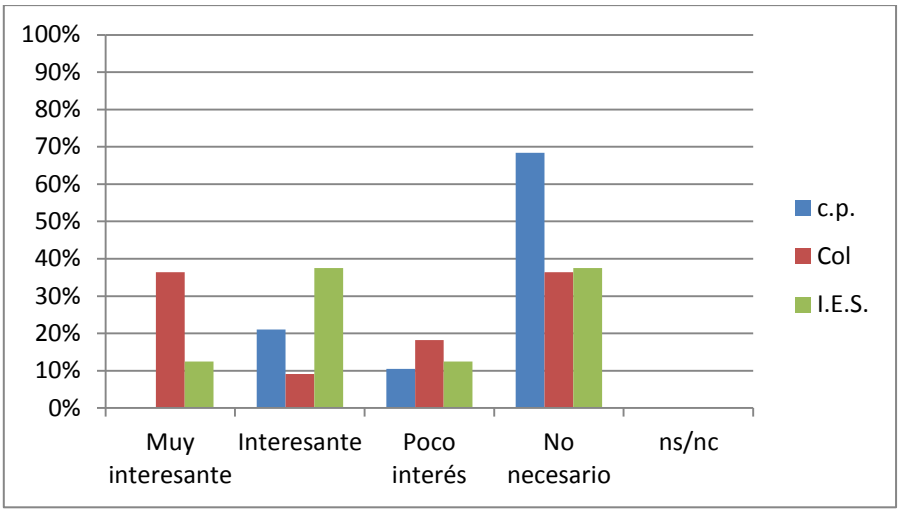


Figura 3.19.- Control de accesos a diferentes áreas del centro

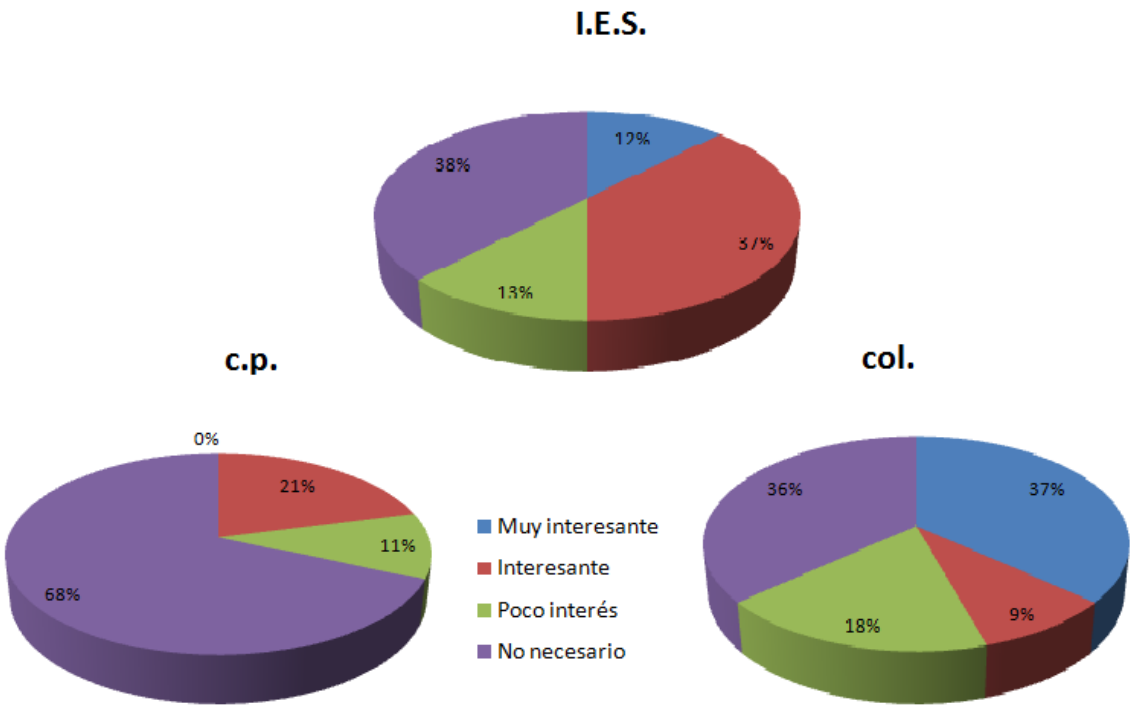


Figura 3.20.- Diagrama de sectores

En este caso tanto todos los tipos de centros muestran mayoritariamente su desinterés a través de un 68% de centros públicos de enseñanza primaria e infantil que consideran el sistema innecesario, un 36% y 18% de colegios privados o

concertados que muestran que es una medida no necesario o de poco interés respectivamente o los institutos donde el 37% lo considera innecesario y el 13% de poco interés. Cabe destacar que los centros de dimensiones mayores tanto de institutos como de colegios privados o concertado el interés aumente obteniéndose un 37% de los institutos que consideran interesante la medida y un 36% de los centros concertados o privados que califican la función como de muy interesante.

Identificar al alumno automáticamente sin necesidad de pasar lista

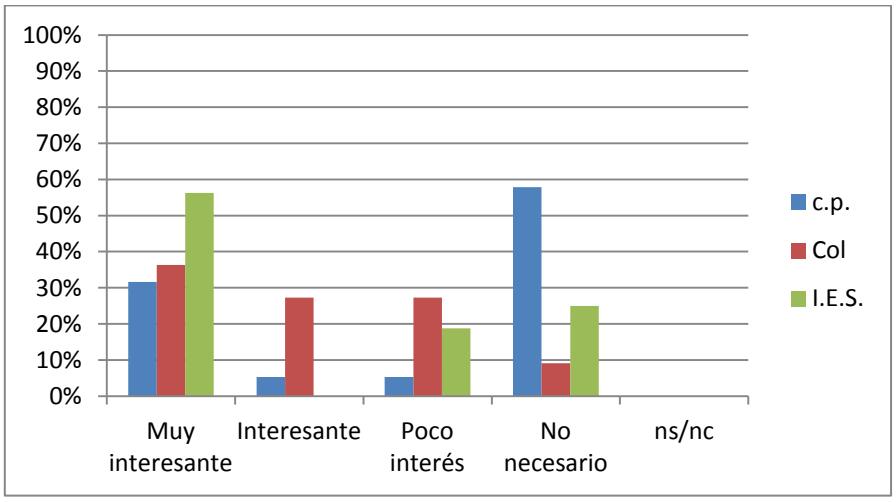


Figura 3.21.- Lista automática

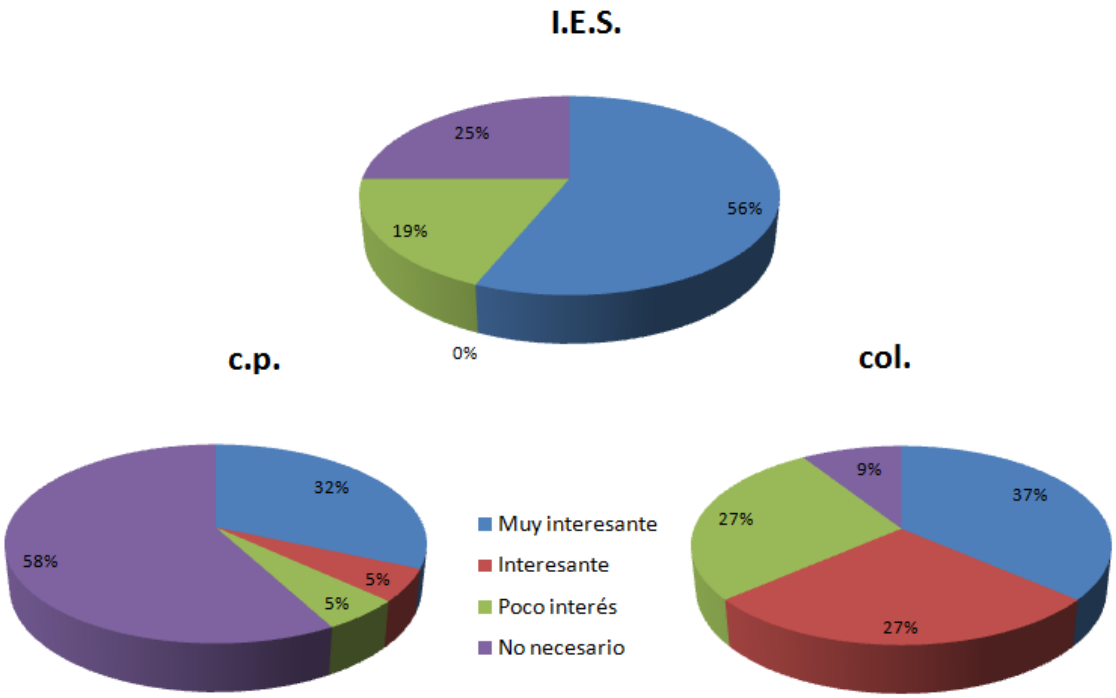


Figura 3.22.- Diagrama de sectores

En el caso de pasar lista de manera automática a través del sistema RFID los colegios públicos de primaria muestran su desinterés por el sistema a través del 58% de los encuestados dado que los grupos de alumnos son reducidos. Sin embargo el 32% de éste mismo tipo de centro muestra su máximo grado de interés por el sistema como método de realizar el control de forma más cómoda. El tipo de centro que muestra mayor interés por el sistema son los institutos con un 56% de ellos mostrando la característica como muy interesante. Los colegios privados o concertados muestran la función como muy interesante -36%- o interesante -27%-

Gestión de las bibliotecas mediante sistema RFID.

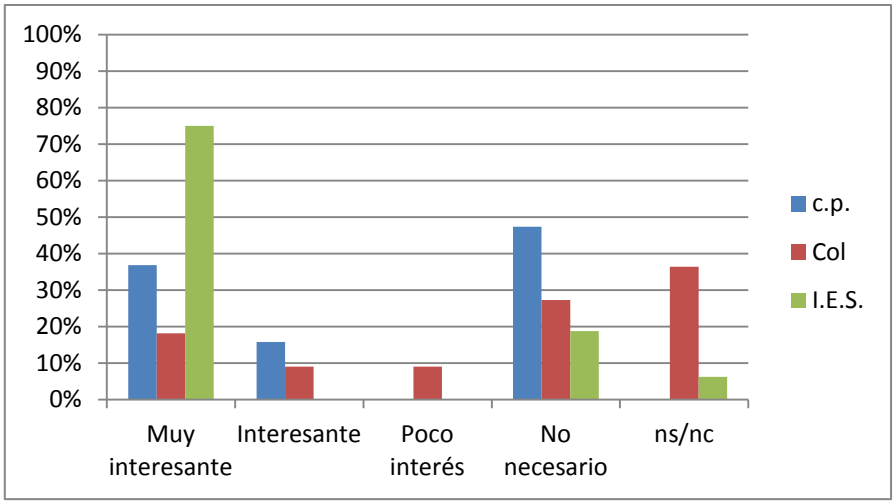


Figura 3.23. Gestión de bibliotecas mediante sistema RFID

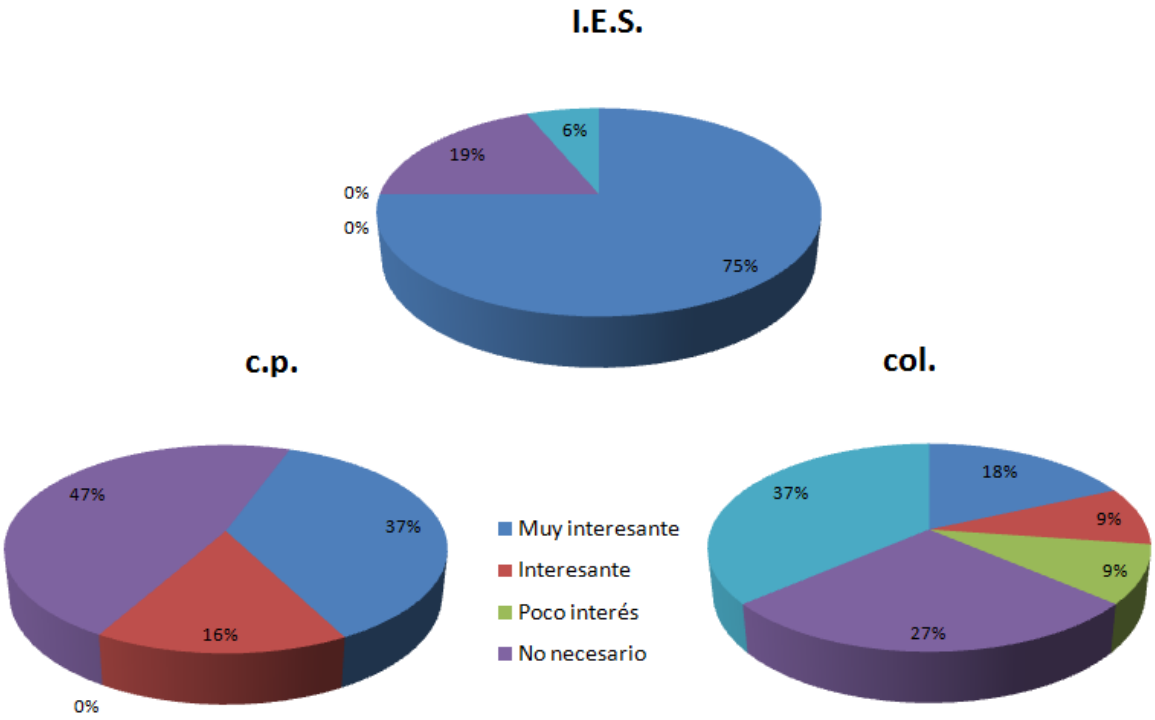


Figura 3.24.- Diagrama de sectores

En este tipo de característica los institutos de enseñanza secundaria mayoritariamente con un 75% muestran su máximo grado de interés por las características del sistema. Los colegios privados o concertados como un 45% de ellos todavía no poseen biblioteca informatizada o están en proceso mediante código de barras muestran su desinterés o desconocimiento sobre las ventajas que puede aportar dado que las bibliotecas no tienen mucho peso en estos casos.

En la tabla 7.12 se resumen las notas medias sobre 4 que alcanzan las distintas características del sistema en función del tipo de centro así como sus desviaciones típicas.

		Localización	Mensajería	Control accesos	Lista automática	Gestión biblioteca
c.p.	Media	1.63	2.05	1.53	2.11	2.42
	Desv.	1.13	1.19	0.82	1.37	1.39
II.E.S.	Media	3.06	3.56	2.25	2.88	3.4
	Desv.	0.97	0.50	1.09	1.32	1.20
CCol.	Media	2.72	3.72	2.45	2.91	2.29
	Desv.	1.05	0.45	1.30	1.00	1.28

Tabla 3.12.- Resumen de la nota media y desviación típica para las diferentes características del sistema en función del tipo de centro.

3.1.7.4 Conocer si a nivel general el sistema interesa y si se estaría dispuesto a asumir algún importe económico.

Una vez vistos los porcentajes en cuanto al grado de interés de las distintas aplicaciones que tendría el sistema RFID en los centros docentes se pregunta a nivel general si las características descritas por el sistema interesarían al centro y si se estaría dispuesto a estudiar el proyecto en caso de tener un coste. A nivel general los porcentajes son los siguientes:

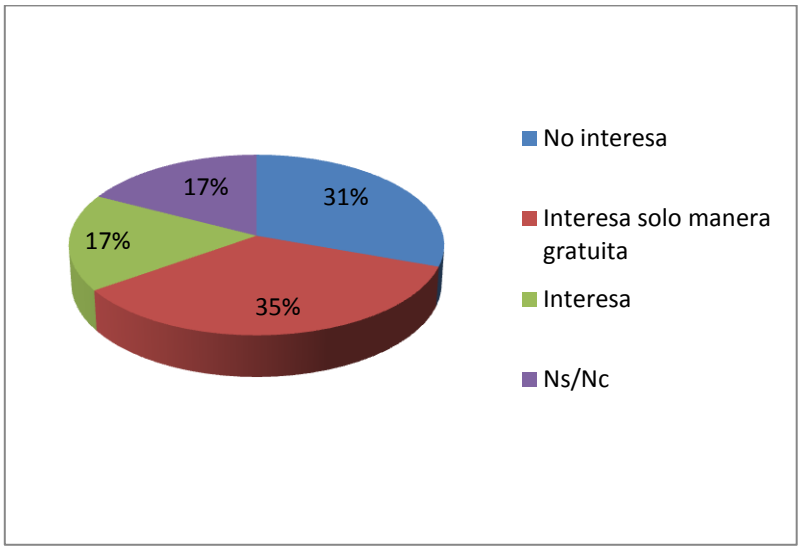


Figura 3.25.- Porcentaje de centros según el nivel de interés por los sistemas

Se observa que el 31% de los centros no muestran interés por las características del sistema mientras que el 35% de ellos las implantarían si fuesen de manera gratuita. El 17% de los centros estudiarían la propuesta en caso de que tuviera un coste económico.

Desglosando estos porcentajes según el tipo de centro encuestado se observan que los porcentajes varían sustancialmente dependiendo de que el centro imparta a infantil y primaria o a secundaria, bachiller y formación profesional. Los porcentajes dependiendo del tipo de centro son los siguientes:

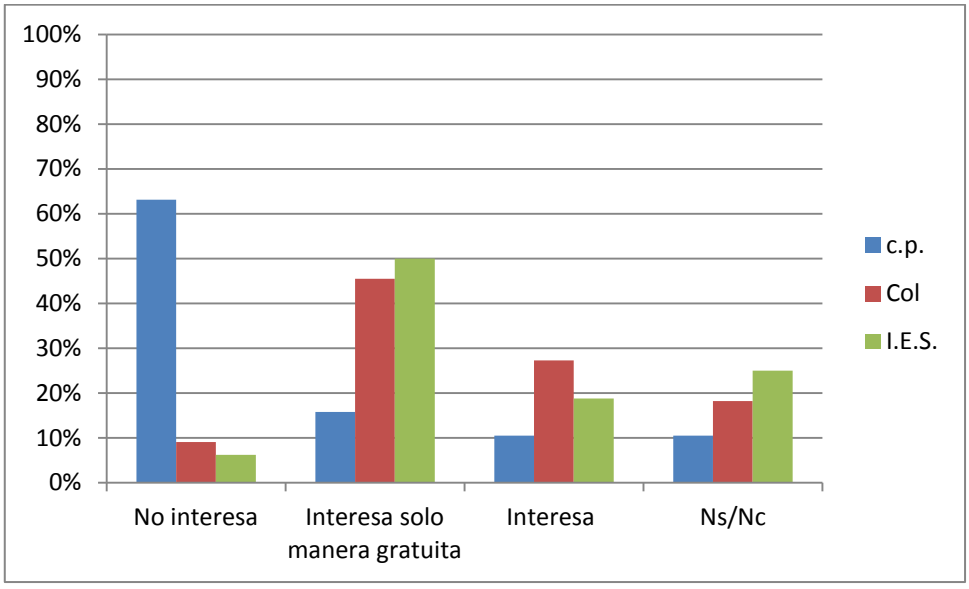


Figura 3.26.- Nivel de interés por las características globales del sistema según tipo de centro

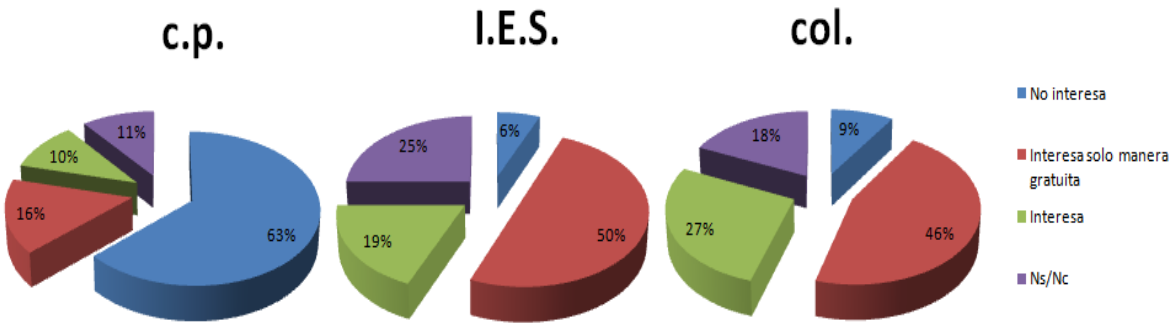


Figura 3.27.- Porcentajes en diagramas de sectores

Se aprecia que en los centros públicos de enseñanza infantil y primaria la mayoría -63%- no considera de interés las diferentes aplicaciones del sistema. Por su parte los institutos de enseñanza secundaria y los colegios privados o concertados donde se imparte además de enseñanza infantil y primaria, secundaria y en algunos casos formación profesional muestran un incremento en el porcentaje de interés

obteniéndose un 69% de los I.E.S que les interesaría el sistema bien fuera de manera gratuita o abonando una cantidad económica a estudiar. Por su parte los colegios privados o concertados el porcentaje aumenta hasta el 73%.

En gran parte de los centros de primaria donde se realizaban las encuestas les parecía interesante las diversas características del sistema pero no aplicado al centro encuestado en concreto dado que en su mayoría son centros de pequeño tamaño y con pocos alumnos sino aplicado a alumnos con mayor edad y centros con mayor capacidad de estudiantes.

3.1.7.5 Conocer la localización más adecuada del sistema en el alumno por parte del centro docente

Se desea conocer entre los centros que muestran interés por el sistema, que ubicación sería la más eficaz y correcta del sistema en caso de aplicar RFID por parte del alumno. A nivel global los resultados arrojan que el 38% muestra como método más eficaz el uso de una tarjeta identificadora seguido de un 24% que prefiere una pulsera como soporte. El 28% de los encuestados muestran su desconocimiento sobre que soporte sería más eficaz.

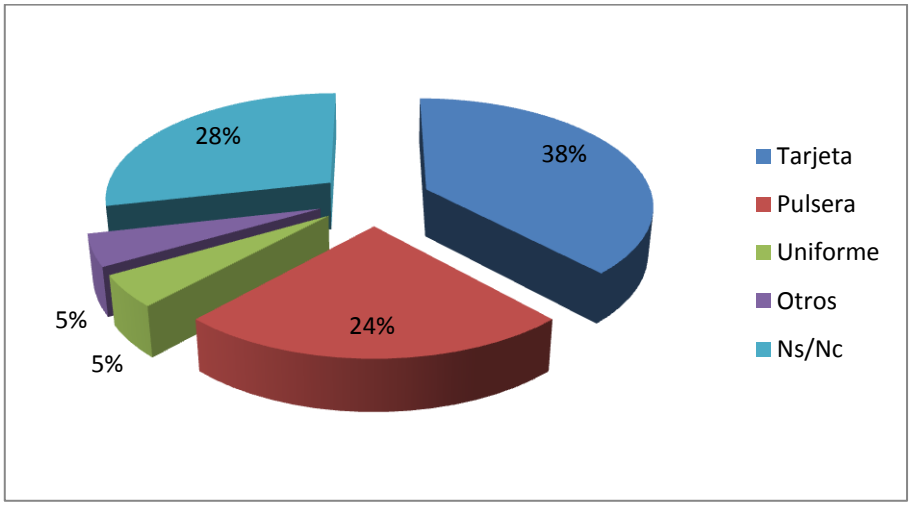


Figura 3.28.- Ubicación del sistema de auto-identificación por parte del alumno

Desglosando estos resultados según el tipo de centro se tiene que entre los colegios públicos de educación infantil y primaria el 60% opta por el uso de una pulsera dado que es más difícil de perder por parte del niño frente a un 40% que considera mejor una tarjeta dado que la pulsera ofrece connotaciones negativas. En los institutos el 73% se muestra a favor del uso de una tarjeta dado que los alumnos son más responsables. Por último un 46% de los colegios privados o concertados muestran mayor interés por el uso de una tarjeta mientras que el 15% apoya el uso de una pulsera como soporte.

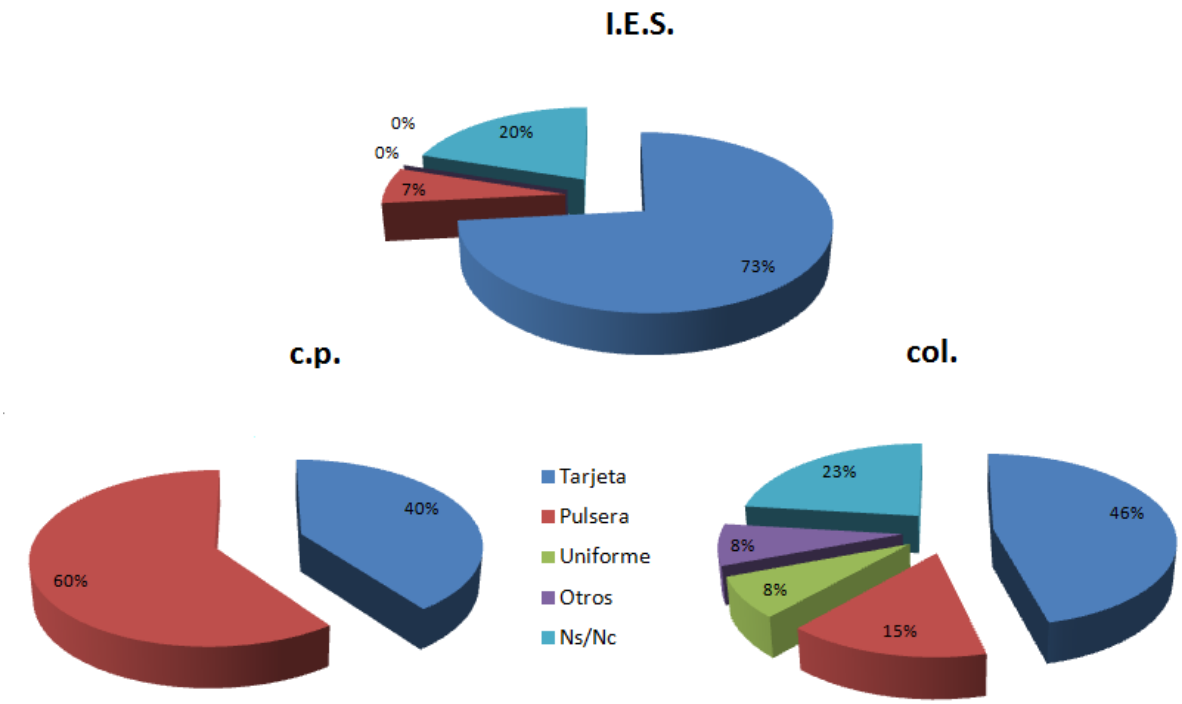


Figura 3.29.- Desglose según tipo de centro

3.1.8 Análisis de la encuesta

3.1.8.1 Conocimiento de la situación tecnológica de los centros docentes

Los centros docentes se encuentran informatizados de forma generalizada. Tanto las tareas administrativas como la gestión de activos en las bibliotecas se realizan de manera informatizada.

Los centros públicos tanto de primaria como de secundaria se encuentran gestionados globalmente mediante Abies (bibliotecas) y Sauce (gestiones administrativas) siendo su funcionamiento calificado como bueno y aprobado respectivamente.

En los centros concertados o privados no se encuentran obligados a utilizar estos programas si bien para algunas tareas administrativas deben utilizar algunas características de Sauce. Es en este tipo de colegios donde se encuentra que algunas bibliotecas no se encuentran gestionadas informáticamente y las que lo están realizando lo hacen mediante código de barras.

Se puede llegar a la conclusión que los centros docentes en Asturias poseen suficiente conocimiento y práctica en el uso de programas informáticos para la gestión tanto de bibliotecas como tareas administrativas y su grado de satisfacción con el mismo es en general bueno por lo que se encuentran adaptados a su uso. Es por ello que la implantación de un sistema RFID a través de un programa informático no supondría a priori inconveniente entre los docentes en su manejo y utilización.

3.1.8.2 Nivel de conocimiento existente en referencia a la tecnología RFID y el conocimiento que poseen sobre sus aplicaciones en la vida real.

La inmensa mayoría de los centros encuestados -89%- dicen no conocer qué son las tecnologías RFID (identificación por radiofrecuencia) ni conocer ningún caso de aplicación. Sin embargo, en la mayoría de los casos reconocen ser usuarios de algunos sistemas que utilizan este tipo de tecnología como puede ser el pasaporte o la tarjeta ciudadana de Gijón.

Esto pone de manifiesto el desconocimiento de la tecnología RFID a nivel de usuario (en este caso en los centros docentes) dado que a nivel empresarial su conocimiento y utilización se encuentra ampliamente implantado en el sector industrial.

3.1.8.3 Conocer cuáles son las características del sistema que más importancia tienen entre el público y que son más necesarias para ellos.

A través de los resultados ofrecidos en los apartados anteriores sobre los porcentajes de centros que mostraban su interés o desinterés sobre una funcionalidad en concreto que podría tener el sistema RFID implantado en el centro se pueden llegar a afirmar que:

En el caso de poder localizar al alumno dentro del centro con vista, por ejemplo, a medidas preventivas en caso de ocurrir algún incidente los colegios públicos que imparten enseñanza infantil y primaria muestran en general su desinterés mientras que los colegios privados o concertados y los institutos de enseñanza secundaria se encuentran muestran su mayor grados de interés sobre todo entre centros de mayor dimensiones.

Se puede concluir por tanto que en el caso de centros de infantil y primaria, al ser centros de dimensiones pequeñas, con un número reducido de alumnos en cada clase y que se encuentran permanentemente vigilados por un profesor este tipo de característica no supone ninguna ventaja dentro del centro. En el caso de los otros 2 tipos de colegios, el grado de interés depende en gran medida de las dimensiones del centro. Aquellos centros con grandes dimensiones y que dan acogida a gran número de alumnos muestran su interés por este tipo de característica.

Por tanto, este tipo de función tiene su campo de acción dentro de los centros que cumplan estas características:

- ✓ Centro de dimensiones elevadas
- ✓ Gran número de alumnos
- ✓ Preferentemente alumnos de secundaria o posteriores que no se encuentran permanentemente vigilados y poseen más radio de acción dentro del centro.

En cuanto al envío de mensajes a los padres de los alumnos a través del teléfono móvil informando de si su hijo ha salido o entrado en el centro, los institutos de enseñanza secundaria y los colegios privados o concertados muestran su máximo interés sobre el sistema mientras que los colegios públicos en su mayoría creen innecesario el sistema.

Se concluye por tanto que en los centros de primaria e infantil como ocurría en el caso anterior los niños se encuentran permanentemente vigilados en grupos reducidos, por lo que el profesor siempre sabe qué es lo que va a hacer el alumno. En aquellos centros que imparten a alumnos de mayor edad el problema es mayor dado que en estos casos los alumnos son más difíciles de controlar y se encuentran en edades conflictivas donde se pueden producir ausencias injustificadas.

Por tanto este tipo de característica obtendría su máximo reclamo entre centros:

- ✓ Que impartan clase a alumnos de secundaria.
- ✓ Que posean gran número de alumnos.

En el caso de control de accesos de forma automática los centros que muestran mayor interés son los privados o concertados seguidos de los institutos. Los centros públicos de enseñanza infantil y primaria ven innecesaria la mediada.

Se observa además que el grado de interés de la característica varía positivamente en función de que el tamaño de centro sea mayor y disponga de áreas que solamente puedan ser utilizadas por determinados alumnos en función de su grado de enseñanza. Es por ellos que los centros de infantil y primaria, no se ajustan a estas características por lo que muestran su desinterés por esta funcionalidad.

Se puede llegar a concluir, por consiguiente, que los centros que muestran mayor interés por esta característica son:

- ✓ Centros de dimensiones elevadas donde se tengan zonas destinadas para determinados alumnos en función del curso que se esté realizando
- ✓ Centros con alumnos de secundaria o posteriores que puedan acceder al área sin necesidad de que un profesor este a su cargo.

En cuanto a la funcionalidad de poder pasar lista de los alumnos de manera automática los institutos de enseñanza secundaria son los máximos interesados en el sistema, seguido de los colegios privados o concertados y ya mostrando en general desinterés los colegios públicos.

Este orden es debido a que en los institutos y colegios privados o concertados el número de alumnos es mayor y la lista debe ser pasada por todos los profesores que dan la clase a los alumnos, que normalmente suelen ser varios al día. Sin embargo en los colegios de infantil o primaria normalmente se encuentra un profesor con los alumnos durante todo el día por lo que solamente es necesario que pase lista una vez al día.

Por tanto, el perfil de centros que adoptarían esta medida como mejora en sus funcionalidades es el siguiente:

- o Centros que formen a alumnos de educación secundaria o posteriores
- o Centros que posean gran cantidad de alumnos
- o Centros donde cada clase disponga de varios profesores que tengan que pasar lista varias veces al día.

Por último, la gestión de bibliotecas a través de sistema de radiofrecuencia muestra gran interés por parte los institutos, los colegios privados o concertados donde no se le da tanta importancia a la biblioteca debido al uso de internet no poseen tanto grado de interés. En los colegios públicos se encuentran divididos entre los que muestra interés y los que lo ven innecesario. En muchas ocasiones esta decisión depende del tamaño de la biblioteca y del uso que el centro este haciendo de ella.

El perfil de centros que muestran interés por la implantación del sistema RFID en bibliotecas son:

- ✓ Centros que posean informatizada la biblioteca

- ✓ Centros en los que el uso de la biblioteca sea frecuente por parte del alumno
- ✓ Centros de educación secundaria preferiblemente

3.1.8.4 Conocer si a nivel general el sistema interesa y si se estaría dispuesto a asumir algún importe económico por la implantación del mismo

En términos generales se puede decir que las variables que hacen crecer proporcionalmente el nivel de interés por parte de los centros son:

- ✓ Las dimensiones del centro
- ✓ El número de cursos impartidos en el centro
- ✓ El número de alumnos del centro
- ✓ La edad de los alumnos

Por tanto los centros que poseen mayor interés en la implantación del sistema son los institutos de enseñanza secundaria y los colegios privados o concertados que ofertan gran cantidad de cursos y que poseen grandes instalaciones y gran número de alumnos.

En cuanto al importe económico a pagar, los institutos de enseñanza secundaria dependen en gran medida de los presupuestos de la consejería por lo que están supeditados a los mismos. Los colegios privados o concertados en su mayoría dependiendo de su presupuesto estarían dispuestos a estudiar la implantación del sistema.

3.1.8.5 Conocer la localización más adecuada del sistema en el alumno por parte del centro docente.

A medida que los centros imparten a niveles superiores de enseñanza y que los alumnos tienen mayor edad se decantan por el uso de una tarjeta como soporte para llevar el sistema de identificación por parte de los alumnos, un 73% y 43% de los institutos y colegios concertados o privados así lo hacen saber. Sin embargo el porcentaje en los colegios de primaria disminuye, un 40% a favor frente al 60% que prefiere el uso de una pulsera.

Algunos centros muestran su malestar hacia la identificación mediante una pulsera pues les ofrece connotaciones negativas ya que se compara a los alumnos como ganado o presos.

La tarjeta que goza de mayor porcentaje aunque ofrece cierta inquietud ante las consecuencias sobre el sistema de una posible pérdida u olvido que pudiera tener el alumno de la tarjeta.

Por tanto, a niveles de infantil o primaria el soporte ideal es la pulsera dado que evita pérdidas u olvidos por parte de los niños. En los alumnos de secundaria y posteriores cursos el soporte más adecuado es la tarjeta dado que el alumno es lo suficientemente responsable para no perderla u olvidarla.

3.1.8.6 Análisis de las sugerencias mostradas por los encuestados

Se describe a continuación algunas sugerencias mostradas desde los diferentes centros:

> Posible aplicación de la característica de localización de alumnos para el profesorado
> Aplicación del sistema de alerta por mensaje en el caso de que el alumno salga del centro aplicado a casos conflictivos como por ejemplo en divorcios complicados.

3.1.9 Conclusiones de la encuesta

Así pues, una vez analizados todos los datos, se decide realizar una descripción de diferentes tipos de sistemas que pueden aportar alguna o varias de las características anteriormente encuestadas procediendo a una descripción tecnológica de cada aplicación así como una estimación del coste de sus elementos.

El perfil de centro que muestra en general interés por el sistema son los institutos de enseñanza secundaria y colegios privados o concertados que impartan este tipo de enseñanza.

Tomando como base que en Asturias este perfil según RECDNU (Registro Estatal de Centros Docentes No Universitarios) lo ostentan 142 centros de los cuales 69 pertenecen a colegios privados o concertados que al menos imparten secundaria y 73 a institutos públicos de enseñanza secundaria obligatoria. Tomando como referencia un caso de éxito del 10% se tiene que los centros que implantarían el sistema sería de 15 centros.

Se debe tener en cuenta, que no se puede realizar un estudio económico en detalle hasta conocer las particularidades de cada centro. Es decir, en primer lugar las necesidades que posee y las características propias de cada centro (número de alumnos, número de aulas…) Por ello, en el capítulo siguiente, se realizará una descripción de forma general.

3.2 Descripción de las aplicaciones de sistemas de auto-identificación en centros docentes.

A continuación se describen las diferentes aplicaciones valoradas de los sistemas de auto-identificación dentro del ámbito docente. Como se ha descrito en capítulos anteriores los sistemas de auto-identificación presentan innumerables ventajas no sólo dentro de la auto-identificación de objetos sino también dentro de la auto-identificación personal.

Se describen las diferentes funciones de los sistemas de auto-identificación que aplicados a centros docentes pueden mejorar la eficiencia y seguridad de los mismos. Se comentará cada uno de ellos, describiendo sus aplicaciones, la tecnología que es necesaria para su implantación así como sus beneficios dentro del centro.

Las aplicaciones objeto de valoración son las siguientes:

- ✓ Localización en tiempo real del alumno dentro del centro.
- ✓ Posibilidad de enviar mensajes al teléfono móvil de los padres para indicar si su hijo se encuentra en el centro o ya ha salido.
- ✓ Control de accesos a diferentes áreas del centro.
- ✓ Identificar al alumno automáticamente sin necesidad de pasar lista de forma manual.
- ✓ Gestión de las bibliotecas mediante sistema RFID.

3.2.1 Descripción de las aplicaciones

A continuación se describen diferentes sistemas que pueden ser implantados en los centros docentes y que dependiendo de cuál se implante ofrecerá unas aplicaciones u otras. De esta forma, cada centro puede escoger las aplicaciones que considere más beneficiosas para su caso e implantar un sistema u otro.

En cada apartado se describirá cada sistema poniendo de manifiesto qué elementos son necesarios para su instalación y una descripción general de cómo funcionaría el sistema. Además se comentará qué aplicaciones tendría cada sistema.

3.2.1.1 Consideraciones generales

3.2.1.1.1 Método de auto-identificación personal

Se ha de tener en cuenta que el sistema de auto-identificación por parte del alumno puede ser de varios tipos, albergando cada uno sus ventajas y desventajas. Después de ver los diferentes tipos de sistemas de auto-identificación y tras analizar las encuestas realizadas a los centros docentes, se decide estudiar en más profundidad los siguientes sistemas de auto-identificación:

- ✓ Sistemas biométricos

En este caso, el alumno utilizará una parte de su cuerpo para proceder a la auto-identificación.

- ✓ Sistemas RFID de proximidad

En este caso, el alumno poseedor del tag RFID (utilizando como soporte una tarjeta) deberá acercar la etiqueta al lector para que éste pueda ser leído.

- ✓ Sistemas RFID largo alcance

A través de este sistema el alumno que porta la etiqueta RFID puede pasar a cierta distancia del lector (dependiendo del rango de alcance del mismo) y puede ser leído sin necesidad de acercar el tag al lector.

En las conclusiones de la encuesta realizada, se extrae que los centros que muestran mayor preferencia por la implantación de las diferentes características ven como mejor soporte de la tecnología a utilizar una tarjeta. Es por ello que en el análisis de la tecnología RFID se tomará como soporte una tarjeta. Se analizará sistemas RFID de proximidad y de largo alcance dado que ambos poseen gran seguridad y su mantenimiento no resulta costoso. Tanto el sistema de largo alcance como de proximidad aportan beneficios ante ciertas situaciones o desventajas dependiendo de la aplicación para la que se utilicen. En la tabla 8.1 se muestran sus ventajas y desventajas respecto a la identificación personal junto con los sistemas biométricos.

Se ha añadido este tipo de sistemas (biométricos) porque uno de los mayores problemas que se tiene al utilizar tarjetas por parte de los alumnos es la posibilidad de intercambio u olvido. Si bien estas posibilidades pueden evitarse mediante diferentes medidas, el uso de sistemas biométricos garantiza con la máxima seguridad la imposibilidad de olvido o intercambio. Es por ello que también se tomará en cuenta para la aplicación de algunos casos. En otros su uso al igual que las tarjetas RFID de proximidad no tendrán sentido.

Se ha desechado la opción de tarjeta de código de barras y banda magnética debido a la poca seguridad que ofrecen, su mantenimiento resulta costoso y su vida útil no es muy elevada.

Por otra parte los botones de memoría sólo resultarían viables para poca gente, no siendo este tipo de aplicación el caso.

A continuación se muestra una tabla con las ventajas y desventajas que posee cada uno de los sistemas en las aplicaciones que se comentarán a continuación:

	Ventajas	Desventajas
Sistemas biométricos	**Seguridad:** Dado el carácter irremplazable e insustituible de los elementos de reconocimiento, éstos no pueden ser falsificados. **Imposibilidad de olvido**. Debido a que mediante este sistema se lee una característica intrínseca del individuo la posibilidad de olvido o pérdida es nula.	**Comodidad:** En algunos sistemas biométricos puede resultar incómoda la identificación. **Pérdida de tiempo:** Se identifica cada persona de manera individual con la consiguiente pérdida de tiempo. Se podrían poner varios lectores pero se incrementaría el coste. **Aceptación:** Muchos sistemas biométricos se consideran invasivos para la persona. **Detección salida**: Si se quiere detectar también la salida del alumno, éste deberá pasar de nuevo por el lector para que quede registrado.

RFID proximidad (tarjeta)	**Seguridad:** Debido a su diseño interno, no puede duplicarse. Cada una posee un código distinto y no puede existir dentro del sistema una tarjeta con igual código. Distancias cortas de lectura. No hay lugar para lecturas externas **Comodidad:** Proporcionan acceso fiable y cómodo, puesto que solo se requiere acercar la tarjeta en el lector para que registre el acceso. **Lectores sin mantenimiento:** Los lectores son unidades totalmente selladas y sin partes móviles, lo que garantiza un funcionamiento correcto sin límite de uso y sin que haya que hacerles algún tipo de mantenimiento. **Tarjetas sin desgaste:** La tarjeta no tiene ningún tipo de contacto con el lector dado que la identificación se logra por radiofrecuencia, por lo cual no tiene desgaste de ningún tipo y permite incluso su reutilización. **Resistencia a condiciones ambientales**: No se inutilizan por exposición a campos magnéticos como teléfonos, MP3, monedas o imanes.	**Pérdida de tiempo:** Se debe aproximar la tarjeta al lector. Por tanto se pierde tiempo en ello. **Lectura más lenta:** Al no poder realizar la lectura simultáneamente el proceso se vuelve más lento. Como posible solución cabría la posibilidad de instalar múltiples lectores para agilizar el proceso con el consiguiente aumento del coste. **Posibilidad de olvido.** Al ser un elemento que el individuo no lleva siempre consigo se puede dar el caso de olvido o extravío de la tarjeta P**osibilidad de intercambio:** Debido a que no es un elemento propio del individuo, éste puede intercambiarse con otro compañero. **Detección salida**: Si se quiere detecar también la salida del alumno, éste deberá pasar de nuevo por el lector para que quede registrado.

RFID largo alcance (tarjeta)	Posee las mismas ventajas que el anterior con la diferencia de: **Rango de alcance:** No es necesario acercar la tarjeta al lector. El lector la puede leer a distancia por consiguiente el sistema resulta más cómodo y eficiente. **Simultaneidad de lectura.** Mediante este sistema se puede leer múltiples tags simultáneamente. Beneficioso cuando el volumen de niños entrando al mismo tiempo es elevado **Detección entrada/salida:** Se puede registrar tanto la entrada como la salida del alumno sin de forma cómoda y rápida	**Posibilidad de olvido.** Al ser un elemento que el individuo no lleva siempre consigo se puede dar el caso de olvido o extravío de la tarjeta P**osibilidad de intercambio:** Debido a que no es un elemento propio del individuo, éste puede intercambiarse con otro compañero. **Coste:** El coste es más elevado que el sistema de proximidad

Tabla 3.13.- Resumen de las ventajas y desventajas de utilizar distinta tecnología para realizar la auto-identificación personal.

Según el sistema elegido se utilizarían los siguientes tipos expuestos en la tabla 8.2 junto a su coste para su posible implantación en un centro escolar. En el caso de las técnicas biométricas se mostrarán las tecnologías de huella digital y cartografía vascular palmar por ser de coste más asequible son fáciles de usar y no resultan invasivas para la persona que los utiliza.

A continuación se realizará una comparativa del coste de manera general para las 3 tecnologías.

		Coste	
		Lector (€)	Tags (€)
Sistemas biométricos	Huella digital	300	-
	Cartografía vascular palmar	400	-
RFID de proximidad (hf)		200	1
RFID largo alcance (uhf)		2000	2

Tabla 3.14.- Comparativa de costes.

3.2.1.1.2 Software

Evidentemente, cada sistema poseerá un programa software que permita realizar todas las funciones para las que el sistema ha sido diseñado. No obstante se debe tener en cuenta que los colegios públicos utilizan para la gestión de la información el programa facilitado por la consejería de educación SAUCE (Sistema para la Administración Unificada de Centros Educativos) para realizar las tareas administrativas. El programa implementado debería ser compatible con este tipo de programa para poder realizar un funcionamiento correcto. En el caso de los colegios privados o concertados el programa SAUCE solamente se utiliza para determinadas labores usándose programas propios para las demás tareas por lo que en este caso se podría implementar un programa propio o implementarlo complementándose con otros.

En el caso de las bibliotecas, el programa utilizado por los centros públicos es el ABIES por lo que el programa software de la aplicación que se describirá para bibliotecas debería ser compatible con el mismo.

3.2.1.1.3 Privacidad

Un aspecto de gran relevancia en las aplicaciones que se van a describir a continuación es el tema relacionado con la privacidad del alumno. Según el estado del arte que se analizó en apartados anteriores sobre las aplicaciones de sistemas de auto-identificación en los centros docentes un aspecto que hizo que muchas de las pruebas piloto fuera anuladas o que el sistema no siguiera adelante fueron las protestas de los padres ante lo que creían una vulnerabilidad de la privacidad de sus hijos y ante el miedo de que sus hijos pudieran ser seguidos fuera de las aulas.

Si el sistema seleccionado para la autoidentificación del alumno es algún sistema biométrico o una tarjeta de proximidad la posibilidad de un posible rastreo es nula, dado que la distancia necesaria para realizar el ratreo o leer de manera fraudulenta los datos es nula en el caso de sistema biométrico y casi despreciable en el caso de tarjetas de proximidad. En el caso de que el sistema elegido fuera de RFID de largo alcance, se podría proteger fácilmente la lectura fraudulenta de la tarjeta utilizando una funda protectora que actuara como jaula de Faraday para impedir su lectura fuera del centro por otros lectores.

3.2.1.1.4 Combinación de funcionalidades

Los casos que se van a describir a continuación muestran diversas aplicaciones relacionadas con la auto-identificación en el ámbito docente. Se debe decir que cada caso, se podría implantar independientemente, aunque también cabe la posibilidad de combinar varios para obtener las máximas funcionalidades. Así pues se podría combinar el caso donde se describe el control de accesos de manera automática, con la localización en tiempo real del alumno por ejemplo.

En este caso se describen aplicaciones generales pero éstas se pueden adaptar a las necesidades de cada centro.

3.2.1.2 Clases de sistemas

3.2.1.2.1 Caso 1: Envió de sms o email a los padres en caso de retraso o ausencia del niño en el centro.

Descripción del sistema

El sistema funcionaría de la siguiente forma, el alumno se identificaría en la entrada del centro mediante alguno de los sistemas que se han visto en apartados anteriores. Una vez identificados, los datos pasarían del lector al software mediante red inalámbrica WIFI, GPRS o cableada en función de los condicionantes de cada centro y la instalación disponible donde se tendría de manera actualizada los datos de llegada o salida de los alumnos al centro. De esta forma se podría enviar mensajes o correos electrónicos a los padres de los alumnos que no llegasen al centro o llegasen tarde. Mediante este sistema también se podría llevar un control de los alumnos que se encuentran actualmente en el centro pudiendo imprimir informes en tiempo real del listado de niños que se encuentran en la escuela en ese momento.

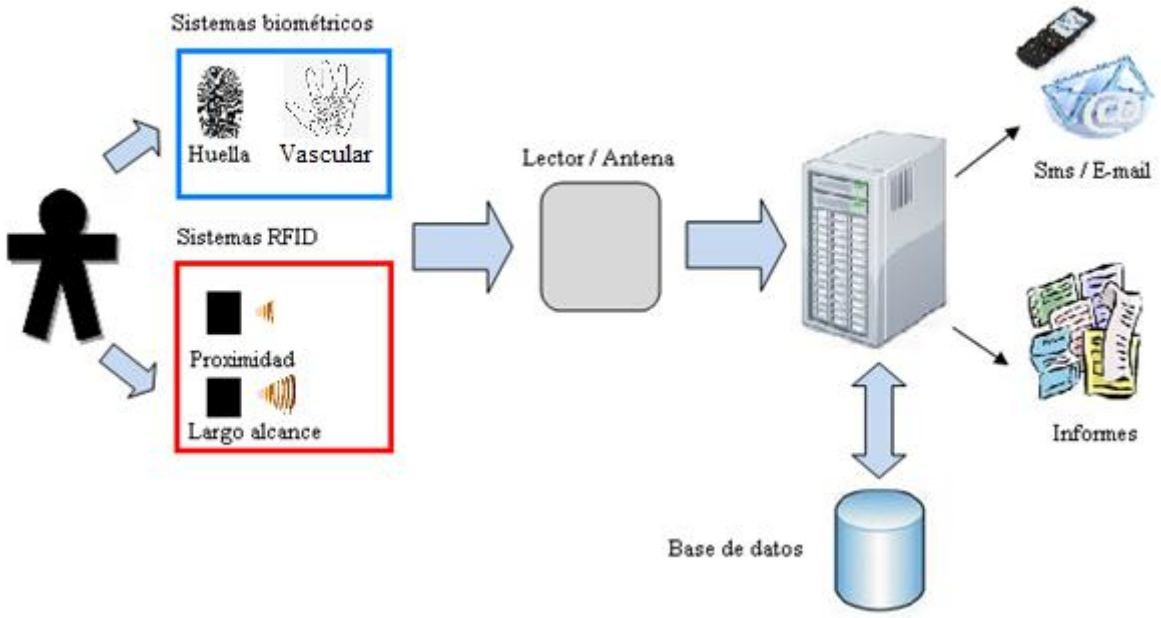


Figura 3.30.- Esquema de funcionamiento caso 1

Posibles aplicaciones

- ✓ Envío de sms o correo electrónico a los padres/tutores de los alumnos en caso de llegar tarde o no encontrarse en el centro.
- ✓ Posibilidad de tener a disposición en tiempo real del alumnado que se encuentra en el centro en ese momento.

3.2.1.2.2 Caso 2: Control de accesos

Descripción del sistema

A través de este sistemas, los centros que tengan áreas donde el acceso este limitado por unos determinados alumnos como puede ser laboratorios u otras salas, pueden restringir el acceso a los alumnos que no poseean la identificación adecuada. Así pues, por ejemplo los alumnos que deban hacer unas prácticas en un laboratorio podrán acceder a él gracias a su tarjeta identificativa o mediante su huella dactilar por ejemplo, que les permitirá el acceso además de quedar registrado el mismo. De esta forma el acceso se puede realizar de forma libre por el alumno responsable y con su propia tarjeta identificativa o método biométrico sin necesidad de usar llaves o de avisar a algún profesor.

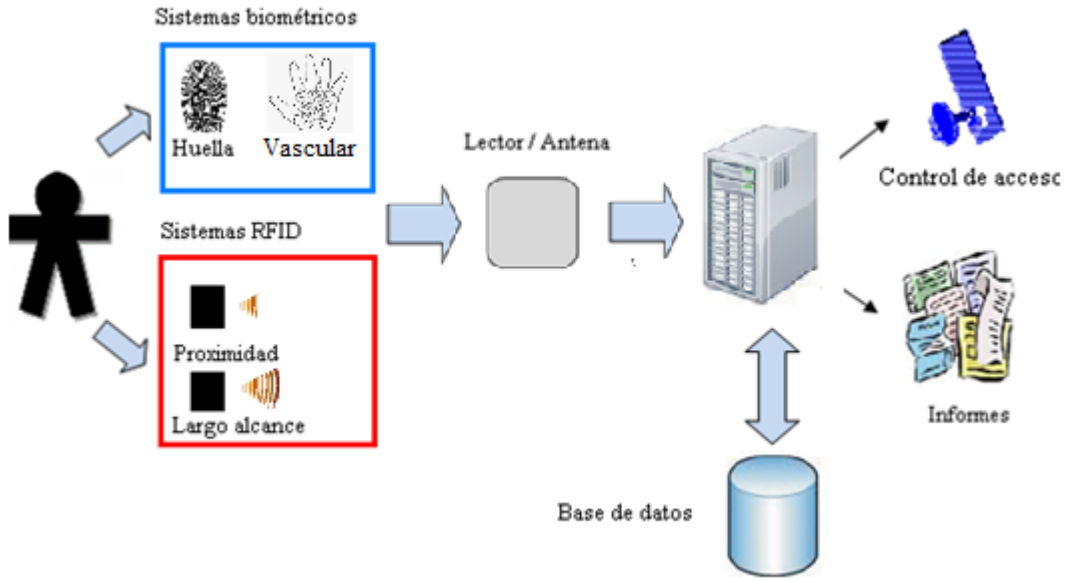


Figura 3.31.- Esquema caso 2.

Posibles aplicaciones

- ✓ Control de accesos a áreas restringidas
- ✓ Posibilidad de emitir informes sobre qué alumnos han estado en estas salas y a que hora entraron.

3.2.1.2.3 Caso 3: Localización de los alumnos por aulas

Descripción del sistema

Mediante este sistema, se puede tener localizado al alumnado (en qué aula está en ese momento) en tiempo real. El sistema funcionaría del siguiente modo. En cada aula donde se quisiese localizar el alumno habría un lector (biométrico, RFID proximidad o largo alcance) Cuando el alumno entrase o saliese quedaría captado que está o ha salido del aula en el caso del sistema de RFID largo alcance. En el caso de los otros 2 métodos el alumno tendría que volver a identificarse en la salida por lo que en este caso parece evidente que el sistema RFID de largo alcance es el más apropiado dado que los otros dos retrasarían en gran medida todo el sistema dado que el alumno debería identificarse en cada aula y en cada entrada y salida que hiciese. De esta forma y a través de por ejemplo un sinóptico se podría tener perfectamente controlado a todo el alumnado del centro. Se puede instalar un lector también a la entrada del centro de tal forma que también queden registrados las entradas y salidas del mismo.

Cabe la posibilidad, de que en caso de algún incidente, se puede imprimir donde se encuentran los alumnos en ese mismo instantes con vistas a realizar cualquier tipo de medida de evacuación de una manera más eficiente y segura sabiendo además cuantos alumnos se encuentran en el centro en ese preciso instante.

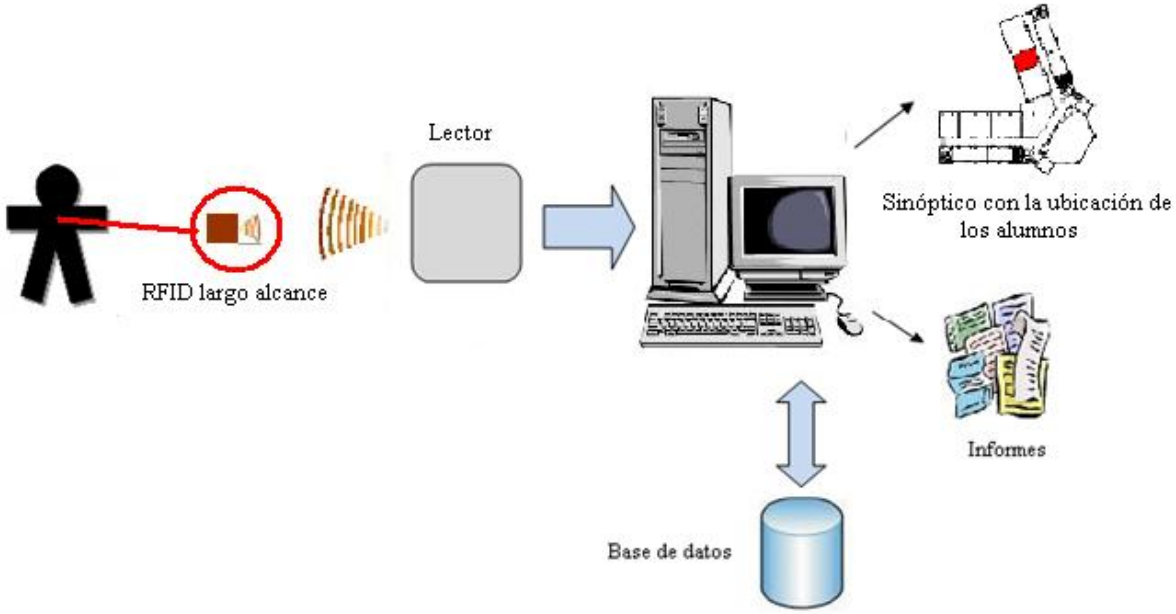


Figura 3.32.- Esquema caso 3. Utilización de RFID largo alcance.

Posibles aplicaciones

- ✓ Localización en tiempo real del alumnos dentro del centro (por aulas)
- ✓ Posibilidad de imprimir un listado con todos los alumnos que hay en el centro y dónde se encuentran
- ✓ Posibilidad de visualizar mediante un sinópico la situación de cada alumno en el centro.

3.2.1.2.4 Caso 4: Lista automática

Descripción del sistema

En este sistema se realizará la descripción para el caso de RFID de largo alcance dado que como pasaba en el caso anterior tanto para los sistemas biométricos como para las tarjetas de proximidad se tendría que realizar una identificación individual tanto en la entrada de las aulas como en la salida por lo que resulta más eficiente el sistema RFID de largo alcance.

En ese caso los alumnos pasan a través de los lectores que se han instalado en cada aula y los datos captados se cargarán en una PDA que posee el profesor con los datos de los presentes y ausentes. De esta forma, y con sólo un golpe de vista el profesor puede comprobar que la lista mostrada se ciñe a la realidad. Una vez realizada la comprobación valida los datos y envía éstos al sistema por lo que la lista de alumnos quedaría actualizada de forma automática.

El principal inconveniente de este sistema sería que el sistema no pudiera detectar a algún alumno. Este problema se subsanaría mediante la supervisión visual del profesor en clase.

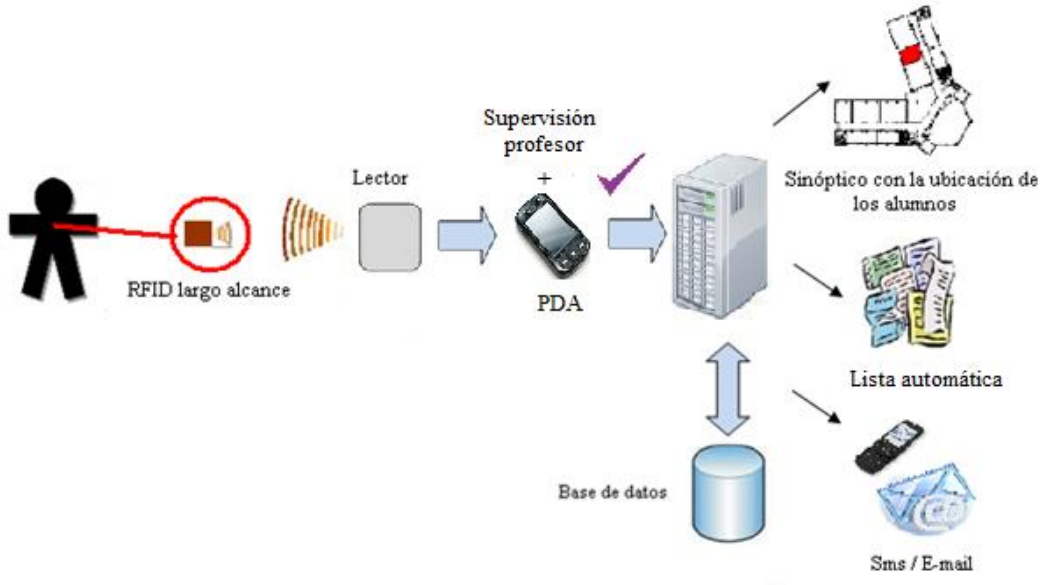


Figura 3.33.- Esquema de funcionamiento caso 4

Posibles aplicaciones

- ✓ Envío de sms o correo electrónico a los padres/tutores de los alumnos en caso de llegar tarde o no encontrarse en el centro.
- ✓ Posibilidad de tener a disposición en tiempo real del alumnado que se encuentra en el centro en ese momento.
- ✓ Pasar lista de manera automática a los alumnos.
- ✓ Posibilidad de tener un sinóptico con la ubicación del alumno en tiempo real (en qué aula se encuentra)

3.2.1.2.5 Caso 5: Aplicación en bibliotecas

Descripción del sistema

Una descripción general del funcionamiento de una biblioteca utilizando el sistema RFID sería la siguiente:

Todos los libros de la biblioteca deben poseer un tag RFID (normalmente se utiliza tags pasivos a 13,56 MHz aunque se podría utilizar tecnología uhf si para otros sistemas se utiliza). Gracias a la posesión de estos tags se puede realizar inventarios de manera más cómoda y sencilla. La forma sería la siguiente: El bibliotecario tendría un lector portátil RFID que le permitiría ir moviéndose por la biblioteca de estantería en estantería e iría leyendo múltiples tags simultáneamente de los libros colocados en las estanterías. (No haría falta ir de uno en uno ni moviéndolos de su sitio). En el caso de que por ejemplo se quisiese buscar un libro la forma sería igual, el personal de la biblioteca rastrearía el libro gracias al lector portátil RFID hasta encontrarlo. La tarea de búsqueda de libros o de realización de inventario se reduce por tanto notablemente gracias a este sistema.

Gracias a este sistema también se podrían instalar cabinas de auto-préstamo o auto-devolución donde sería el propio alumno el que sacaría o devolvería un libro. El sistema se describe a continuación. El alumno una vez que ha elegido el libro que quiere tomar prestado debe dirigirse a una estación de autopréstamo donde debe pasar tanto el libro que quiere llevarse como su tarjeta identificativa RFID (u otros, dependiendo del lector que poseea la máquina). El sistema le mostrará su estado actual de préstamos y devoluciones y si es apto para sacar el libro. Si todo es correcto el alumno pasa el libro por el lector designado para ello y de esta forma la información del libro pasa a la base de datos como prestado a ese alumno en concreto. Mediante esta acción también se puede desactivar un bit (el bit de alarma) para evitar que la alarma se active cuando el alumno pase por los lectores colocados a la salida de la biblioteca y que detectan si ese bit está activado o desactivado. En los sistemas habituales de codificación de libros las funciones de registro de los datos y la de seguridad se encuentran separadas por lo que cuando se realiza la devolución o préstamo es necesario realizar una operación adicional. En el caso de las etiquetas RFID, éstas ya contienen codificado el número de registro y el bit antirrobo por lo que estás dos operaciones se pueden realizar de manera conjunta.

En el caso de la auto-devolución el procedimiento sería el mismo pero a la inversa, al pasar el libro por el lector se activaría el bit de alarma y los datos del libro pasarían a constar como que ese alumno en concreto ha devuelto el libro.

Como principal desventaja esta el coste de la implantación y el desconocimiento inicial del personal hacia la tecnología RFID por lo que requerirá un adiestramiento en este ámbito.

Figura 3.34. Esquema de funcionamiento de una biblioteca con el sistema RFID

Posibles aplicaciones

- ✓ Inventarios más eficientes: El uso de lectores portátiles capaces de leer varias etiquetas de los libros simultáneamente y a distancia posibilita que las tareas de inventariado se realicen de una forma más cómoda y eficiente. Además mediante este sistema es posible también comprobar la ubicación de los libros y comprobar de esta forma si alguno se encuentra situado en una localización incorrecta.
- ✓ Auto-préstamos y auto-devolución: La tarea de auto-préstamo y auto-devolución permite automatizar este proceso de tal forma que el/la bibliotecario/a puede estar realizando otras tareas aumentando de esta manera su rendimiento.
- ✓ Realización de estadísticas: El sistema de gestión ofrece también la posibilidad de realizar estadísticas con los datos (libros más

demandados etc) siendo una herramienta muy útil para la mejora de los servicios de la biblioteca.

3.2.1.3 Estimación de costes

A continuación se realizará una estimación de los costes de los elementos necesarios para su implementación según la tecnología utilizada.

La estimación del coste se realiza en base al desarrollo entre 15 centros. Se toma para los cálculos una demanda de 2000 etiquetas en el caso RFID.

Caso 1

En este caso se debe tener en cuenta el número de lectores instalados en el centro. Éste número dependerá del número de entradas que posea el centro y del número de alumnos. La instalación constaría de los siguientes elementos y su coste dependiendo qué tipo de tecnología se utilice. El precio del lector es unitario.

Caso 1				
	Biometría		Rfid hf (€)	Rfid uhf (€)
	Huella digital (€)	Cartografía vascular (€)		
Lector	300	400	200	2000
Tag	-	-	2000	4000
Sofware	700	700	700	700
Servidor	3000	3000	3000	3000
Otro cableado	500	500	500	500
Router wifi	100	100	100	100

Tabla 3.15. Coste de los elementos caso 1. Fuente: Oxígeno Empresarial

Caso 2. Control de accesos

En este caso los lectores deben ser instalados en los lugares donde se requiera el control. En la tabla aparece el precio unitario del lector.

	Caso 2			
	Biometría		Rfid hf (€)	Rfid uhf (€)
	Huella digital (€)	Cartografía vascular (€)		
Lector	300	400	200	2000
Tag	-	-	2000	4000
Sofware	1000	1000	1000	1000
Servidor	3000	3000	3000	3000
Otros: cableado	2000	2000	2000	2000
Router wifi	100	100	100	100

Tabla 3.16.- Costes de elementos caso 2. Fuente Oxígeno Empresarial

Caso 3

En este caso cada lector debería ser instalado en cada aula que se quisiera localizar al alumno. El precio se encarecería considerablemente. En este caso sólo se toma el sistema RFID de largo alcance dado que no sería posible de manera práctica detectar las entradas y salidas del alumno con otro tipo de sistema En la tabla figura el precio unitario del lector.

	Caso 3
	Rfid uhf (€)
Lector	2000
Tag	4000
Sofware	2000
Servidor	3000
Otros: cableado…	2000
Router wifi	100
Sinóptico: Pc+ pantalla 32”	800

Tabla 3.17.-Coste elementos caso3. Fuente: Oxígeno Empresarial

Caso 4.

	Caso 4
	Rfid uhf (€)
Lector	2000
Tag	4000
Sofware	1500
Servidor	3000
Otros: cableado…	2000
Router wifi	100
PDA	400

Tabla 3.18.- Costes caso 4. Fuente: Oxígeno Empresarial

Caso 5

	Caso 5	
	Rfid hf (€)	Rfid uhf (€)
Lector portátil	900	1800
Tag	500	500
Sofware	1000	1000
Servidor	3000	3000
Otros: cableado…	2000	2000
Router wifi	100	100
Antena antirrobo	2000	2000

Tabla 3.19.- Costes caso 5.- Fuente Oxígeno Empresarial

4 Trabajo de desarrollo realizado

En el presente apartado se describen los desarrollos realizados y que han servido para el contraste de la factibilidad técnica y económica esperados de los estudios teóricos y de la vigilancia tecnológica.

4.1 Descripción de prototipos realizados

4.1.1 Control de asistencia a congresos

Los congresos presentan un elevado interés al control de asistencia por razones de seguridad (aglomeración de personas, personalidades, imagen, etc.) y de eficiencia (reducción del personal necesario).

En los congresos suele darse la dificultad para el control de tener unos picos de asistencia muy elevados en términos de personas que han de acceder por unidad de tiempo.

Se ha desarrollado un sistema que se ha probado en 3 congresos (2 de ellos internacionales) en Gijón.

Las ventajas de este sistema son:

- Alto volumen de tránsito: pueden pasar varias personas a la vez y no necesitan esperar para sacar su identificador de la cartera o acercarla a un lector sino que son identificadas a su paso con tal de que lleven el identificador “a la vista”. Esto se ha conseguido con una identificación tipo tarjeta colgada del cuello como es frecuente en este tipo de eventos.
- Realimentación en tiempo real a la organización de la asistencia con respecto a la esperada, etc. Esto permite graduar las esperas al inicio de charlas, etc.
- Información sobre personas que están dentro con nombres y apellidos ante posibles emergencias.
- Comprobación de que alguna persona ha llegado ya. Muy importante en el caso de Speakers, etc.
- Bajo coste del identificador (identificadores desechables tipo dipolo en pegatina).

- Información de bienvenida a cada visitante en su propio idioma a su paso por el pórtico mejorando la imagen de control y de organización eficaz y moderna.

El sistema se basaba en la utilización de RFID en frecuencia UHF 860MHz según el protocolo de EPC Gen 2 con identificadores desechables. La conexión entre el lector y el midleware se realizó a través de Wifi para facilitar el acceso a los datos desde un punto de control alejado.

Ilustración 82.- Punto de acreditación en congreso

El sistema funciona de la siguiente manera: Los participantes en la conferencia se inscriben a través de internet. La primera vez que llegan al lugar del congreso se les imprime una etiqueta RFID con sus datos. En la entrada al edificio del congreso se instalan las antenas de RFID ocultas en columnas promocionales (ver figura 6.20) por donde los asistentes pasan y son detectados apareciendo en una pantalla un mensaje de bienvenida particularizado a cada nombre y según la nacionalidad del asistente tal y como muestra la figura siguiente. El fondo de la pantalla va alternando fotografías de lugares típicos y bellos del entorno para conseguir un efecto óptico más agradable. Además se incluyen logos de la organización y mensajes.

Ilustración 83.- Pantalla de bienvenida al paso de dos visitantes.

El sistema detecta la entrada y salida de los asistentes (diferenciándolas según el estado anterior del visitante: dentro o fuera) y permite a la organización conocer la presencia de personas en particular, personas que han llegado con respecto al número de inscritos, etc. durante el evento.

Tras el evento, se proporciona a la organización un resumen estadístico interesante para la reflexión y análisis sobre el desarrollo del congreso y preparación de otros (puntualidad, porcentaje de asistencia frente a inscripción total o por nacionalidades, horas de salida de los participantes, asistencia a diferentes jornadas del evento, etc.)

Ilustración 84.- Punto de control oculto en columnas promocionales.

4.1.2 Control de accesos – combinación tecnologías RFID y Biométricas

La empresa O_2E ha implementado un sistema para el control a los accesos de las diferentes áreas de la Fundación Centro Tecnológico Prodintec en Gijón combinando la tecnología RFID junto con la biometría. Dicha Fundación gestiona el Centro Tecnológico Prodintec en el que frecuentemente se desarrolla conocimiento en colaboración con otras empresas por lo que la protección de este conocimiento y su estanqueidad es clave para que la Fundación pueda cumplir los compromisos de confidencialidad que voluntariamente suscribe con las empresas con que colabora. Por otra parte, la Fundación, tiene entre sus objetivos de gestión la consecución de las mejores prácticas en Prevención de riesgos laborales con lo que la información eficaz de la localización de las personas en tiempo real es un activo importante. Con el fin de dar satisfacción a estos requisitos manteniendo una utilización cómoda y ágil por parte del personal de la fundación se ha concebido y desarrollado el sistema descrito.

Ilustración 85.- Visualización en tiempo real de la situación de las personas en el edificio.

El sistema de control de accesos combina la auto-identificación biométrica por medio del reconocimiento de iris con el uso de tarjetas RFID: una vez verificada biométricamente la identidad de una persona, la tarjeta asignada a ella es válida hasta el evento de caducidad de la validación biométrica. Este evento está programado para el final de cada día. Esta tarjeta da al usuario acceso a las diferentes zonas en que se divide la empresa.

Ilustración 86.- Cámara de reconocimiento de iris en primer plano sobre la columna y antenas RFID ocultas en falso techo.

El sistema está configurado para que, al comenzar el día los trabajadores deban validar su identidad en el dispositivo de reconocimiento de iris. De no hacerlo, su tarjeta será inválida a efectos de la apertura de los accesos aunque si lo sigue siendo a efectos de localización.

El proceso de identificación biométrica se realiza en el hall de entrada para proteger el lector biométrico de posibles vandalismos o de las inclemencias climatológicas. El acceso al hall de entrada, definido con un perfil de seguridad bajo, se realiza con una tarjeta RFID autorizada en el sistema pero no necesariamente validada biométricamente.

El usuario a partir de la validación biométrica, tendrá acceso a las áreas que le permita el administrador del sistema según el perfil al que le asigne y podrá entrar en ellas de forma cómoda y ágil dado que las puertas se abren al estar cerca de ellas. No necesitará nuevas validaciones biométricas.

El sistema genera un informe para el recuento y apoyo al proceso de evacuación que se genera de forma inmediata en caso de emergencia Este hecho, toma especial relevancia en materia de seguridad no sólo desde el punto de vista de que personal ajeno a la empresa pueda entrar sino como medio de seguridad en prevención. Si algo ocurriera en la empresa, se sabría el número de trabajadores que se encuentran en tiempo real en la compañía y cuál es su ubicación en ese momento. Además, es posible consultar en todo momento la ubicación de una persona o trazar sus movimientos y se dispone de un sinóptico gráfico que muestra en una pantalla en el hall las fotografías de las personas que están en cada estancia. Este sinóptico gráfico es también accesible en red lo que permite una localización cómoda de las personas ante llamadas telefónicas, contactos no programados, etc.

La tecnología utilizada para el sistema biométrico es el reconocimiento de iris de Panasonic mientras que el sistema RFID utiliza receptores y tags activos UHF de 440MHz con activación a 125KHz de SHS. Estos tags, con el fin de aumentar la vida útil de las baterías que equipan, permanecen en estado de bajo consumo energético salvo que entren en la zona de influencia de una antena que los "despierta" energizando la bobina de los identificadores con una frecuencia de 125kHz. Una vez activados los identificadores trabajan en la frecuencia de 440MHz para su comunicación con la antena alimentados por su batería y, una vez la comunicación ha sido satisfactoria, la antena del lector les envía una señal para que vuelvan al estado de "letargo" no abandonándolo hasta que entran en la zona de una nueva antena.

Tras 3 meses de análisis y pruebas, fundamentalmente buscando la ubicación más adecuada de los componentes del sistema RFID, el sistema quedó instalado en Julio de 2009 y actualmente se encuentra en funcionamiento.

Desde el punto de vista de la eficacia, se han comprobado los siguientes hechos:

- ✓ La fiabilidad del sistema no permitiendo el acceso a personal no autorizado ha sido total. No se han conocido casos de falsa aceptación.
- ✓ El sistema de localización permite ha arrojado una eficacia del 99,7%. Esta eficacia se ha medido contrastando durante un periodo de 2 meses de forma sistemática las personas que presentan un error de localización al final del día cuando el edificio está vacío y que aparecen en el sistema como presentes en el mismo. Se considera la prueba suficientemente representativa de la capacidad de localización en tiempo real y se ha escogido este método de prueba por lo viable que resulta un análisis fiable.
- ✓ El confort del usuario es elevado, si bien existen dos factores que presentan, al punto actual, una oportunidad de mejora:

- ✓ El tiempo que el sistema tarda en comandar la apertura de una puerta varía normalmente entre 1 y 5s. Esta variación se debe a la suma de los retardos de detección de la tarjeta, comprobación de identidad validada y permisos, envío de orden de apertura y respuesta del mecanismo de apertura.
- ✓ La vida útil de las tarjetas de identificación ha sido en un número de casos significativo mucho más breve de lo inicialmente previsto y su fin se ha dado en algunos casos de forma imprevisible: de forma repentina la tarjeta deja de comunicarse efectivamente.

Es muy interesante resaltar que se ha comprobado, gracias a los análisis de fiabilidad de localización, que con una frecuencia de aproximadamente un 0,3% se dan errores humanos en la utilización del sistema, fundamentalmente olvido de las tarjetas. Este hecho confirma la idoneidad de un sistema de localización y control de accesos que reduzca al mínimo posible la intervención del usuario con el fin de maximizar su eficacia.

4.1.3 Seguridad – control de EPIs

La utilización adecuada y rigurosa de los EPIs (Equipos de Prevención Individual) adecuados y en correcto estado de conservación es una de las claves de una prevención de riesgos eficaz. Ésta es una tarea compleja ya que la motivación del trabajador a veces no es suficiente para evitar olvidos, cuidar la revisión del buen estado de los equipos, etc.

Se ha desarrollado un prototipo de control de EPIs apoyándose en tecnología de identificación por radiofrecuencia para el apoyo de la gestión. Se basa en la identificación de los distintos EPIs con chips de identificación por radiofrecuencia pasivos en la gama UHF que son detectados al paso del trabajador por un punto de control a ubicar en la pasarela de acceso al punto de trabajo.

El punto de control dispone de un haz óptico que actúa como barrera de control de paso que levanta una alarma sonora, visual y en el sistema (para su registro y procesado posterior, envío por email, etc.) en caso de que se cruce en los siguientes supuestos:

- No portar identificación RFID válida
- No disponer de autorización para entrar en la zona controlada
- No llevar todos los EPIs necesarios

La identificación de los diferentes tipos de equipos con tag RFID es algo que no puede resolverse con un único tipo de identificación. Hay que tener en cuenta las condiciones de utilización (temperaturas extremas, ambientes corrosivos, humedad, polvo, golpes, rozaduras, etc.) su fijación duradera y, como es lógico, el coste del conjunto identificador + fijación.

Se hicieron pruebas con los siguientes tipos de EPIS:

- Casco
- Protector auditivo
- Calzado de seguridad
- Gafas de protección
- Pantallas de protección
- Guantes
- Equipos de filtrado
- Botiquín
- Extintor

Ilustración 87.- Varios equipos de protección individual

Los resultados fueron satisfactorios y se presentó recientemente el prototipo en la Feria Laboralia 2011 celebrada en Valencia.

Las principales conclusiones de las pruebas del prototipo fueron:

- ✓ El sistema es suficientemente rápido como para no suponer una pérdida de productividad en el tránsito a los puntos de trabajo.
- ✓ El sistema, por su diseño, falla por el lado de la seguridad en caso de que algún identificador se encuentre apantallado o dañado.

4.1.4 Seguridad: inspecciones y revisiones

Uno de los pilares de la actividad preventiva es la comprobación de que los medios y condiciones de trabajo se mantengan en correcto estado. Normalmente la información relativa a estas actividades de control se gestiona en papel, traspasándose en una gran parte de los casos a soporte informático para su archivo, análisis estadístico, etc.

Esta actividad suele tener asociadas en mayor o menor medida estas problemáticas:

- **Tiempo excesivo empleado por los técnicos** en cumplimentar partes de trabajo
- Dificultades para cumplimentar los partes correctamente por **falta de luz, lluvia,** etc.
- Partes cumplimentados con **poco rigor** o en lotes tiempo después de la actuación
- Tiempo de **transcripción de los partes** de trabajo **al sistema informático**
- **Errores de interpretación** de los escrito en los partes
- **Olvidos en revisiones**
- **Tiempo empleado en planificar y comunicar** rutas de inspección
- **Actualización y distribución de instrucciones de trabajo** de partes
- **Personal inspector difícilmente controlable**
- **Etc.**

Con herramientas de movilidad (PDA, smartphones, tablet-pc, etc.) se posibilita la introducción de datos directamente en soporte informático por parte del técnico. Esto trae consigo las siguientes ventajas:

- ✓ **Reducir los tiempos de cumplimentación** de documentación que emplean los técnicos de mantenimiento y **garantizando** además la **realización de las inspecciones sobre los equipos**.
- ✓ **Eliminar** la necesidad de **informatizar manualmente** los partes de mantenimiento
- ✓ **Disponer de información en tiempo real** (según cobertura) sobre el desarrollo de los trabajos, tiempos de ejecución, etc. **facilitando la supervisión de los mismos.**
- ✓ **Facilitar la recogida de información** de los técnicos en circunstancias adversas **(lluvia, oscuridad, etc.)** mediante un interfaz sencillo de utilizar y con la posibilidad de añadir **fotografías, notas de voz.**
- ✓

Ilustración 88.- Identificador RFID para su remachado sobre metal.

Se ha desarrollado una solución sobre PDA que permite, además ligada a la identificación RFID de los lugares o equipos minimizar el tiempo de cumplimentación de los protocolos y asegurar que el técnico ha realizado el protocolo en la fecha y lugar registrados.

La solución puede trabajar tanto con equipos HF como UHF, este último con mayores costes pero con una mayor flexibilidad desde el punto de vista de la ubicación de los identificadores.

Ilustración 89.- Ejemplo de lista de comprobación de extintores sobre PDA

Las PDA utilizadas permiten la conexión al servidor mediante GPRS o wifi además de mediante cable lo que permite al técnico una total libertad de actuación. La toma de fotografías y registro de notas de voz es un valor añadido que los métodos tradicionales no permiten aprovechar.

Además, el sistema registra las actividades realizadas de forma que cada vez que un técnico realiza una inspección o identifica un equipo con su PDA se registra como un "fichaje" del técnico permitiendo conocer su posición, desplazamientos en el día, etc. y mostrarlo en un mapa en la web. La posición se recaba de la propia PDA si lleva módulo GPS o de las coordenadas asociadas al activo RFID.

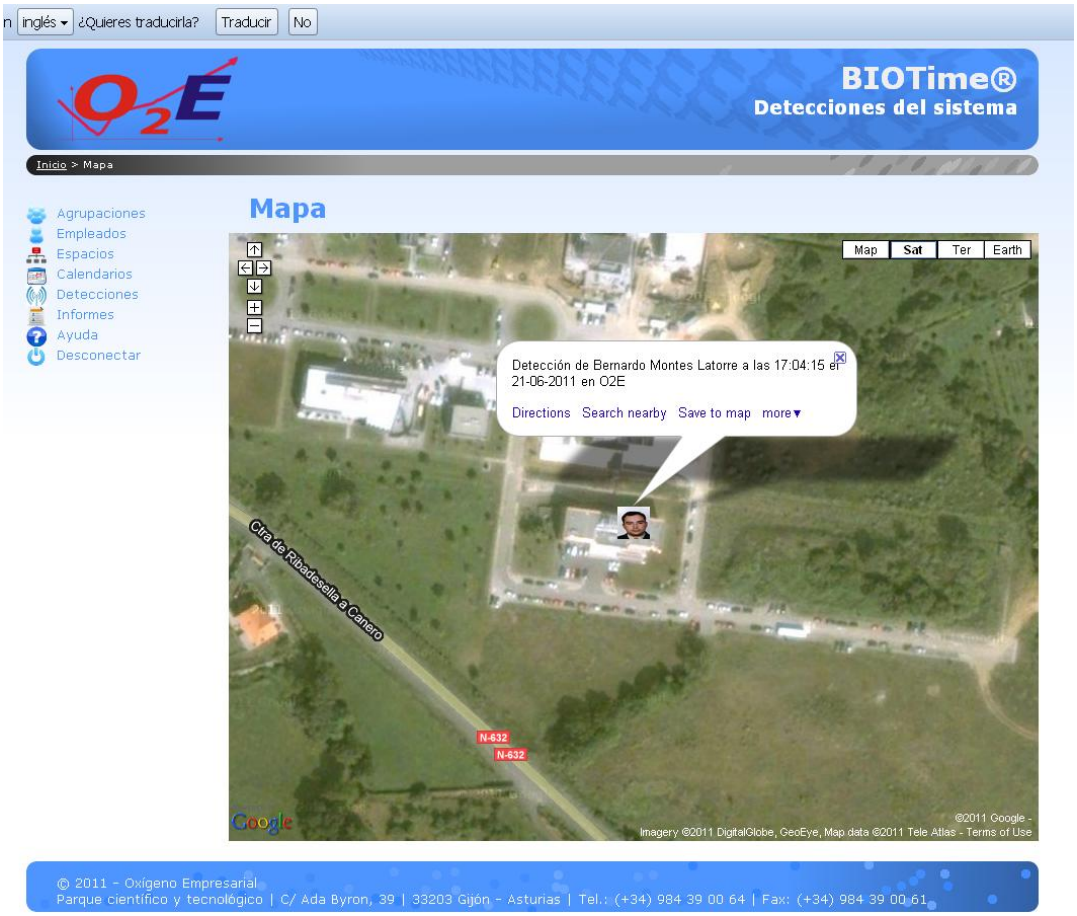


Ilustración 90.- Visualización web de una detección georeferenciada.

Ilustración 91.- PDA industrial con conectividad GPRS, cámara y wifi corriendo aplicación de O2E para la inspección en campo de la actividad del Oso pardo cantábrico.

4.1.5 Seguridad: control de presencia y accesos en obra civil

Las grandes obras suponen una enorme dificultad para el control de presencia y acceso (grandes extensiones, ausencia de perímetros controlados o cerramientos, multitud de trabajadores, entorno de intemperie). Por otra parte, la identificación de las personas es especialmente en estos casos para fines de gestión de nóminas (control de absentismo) como para una eficaz prevención de riesgos (control de formación adecuada, altas en seguros sociales, formación preventiva recibida, etc.).

Ilustración 92.- Aplicación para control de presencia en movilidad.

Con este problema en mente se está trabajando en una solución que permita resolver dicho problema utilizando dispositivos móviles dotados de reconocimiento biométrico, lectura RFID y comunicación GPRS o satélite con un servidor central al que reportar las detecciones e incidencias y del que recabar los datos necesarios sobre los individuos (filiación, documentación actualizada, formaciones recibidas, etc.)

Las conclusiones que se han verificado de la experiencia son:

- ✓ Reducción de costes de inspección, ya que permite un trabajo mucho más eficaz de los listeros (agilidad en la comprobación de la identidad, etc.) o su eliminación mediante la utilización de dispositivos portátiles en combinación con restricciones físicas del acceso donde sea posible.
- ✓ Mayor eficacia de la actividad preventiva: control simultáneo de los niveles formativos, filiaciones, etc.
- ✓ Eliminación de la picaresca (personas que se hacen pasar por otras para ocultar absentismos, sustitución de trabajadores por otros sin regular, etc.)
- ✓ Es importante cuidar la sencillez del interfaz de usuario para evitar un rechazo por el miedo natural que aún una parte de la población tiene a la utilización de equipos informáticos en su trabajo.

4.1.6 Control de asistencia en centros docentes

Con la llegada del Plan de Bolonia se ha acentuado el interés del control de asistencia de los alumnos en los centros docentes. La valoración de la asistencia como uno de los ingredientes básicos de la evaluación de los alumnos crea una oportunidad de mejora frente a los centros tradicionales tal y como se ha comentado.

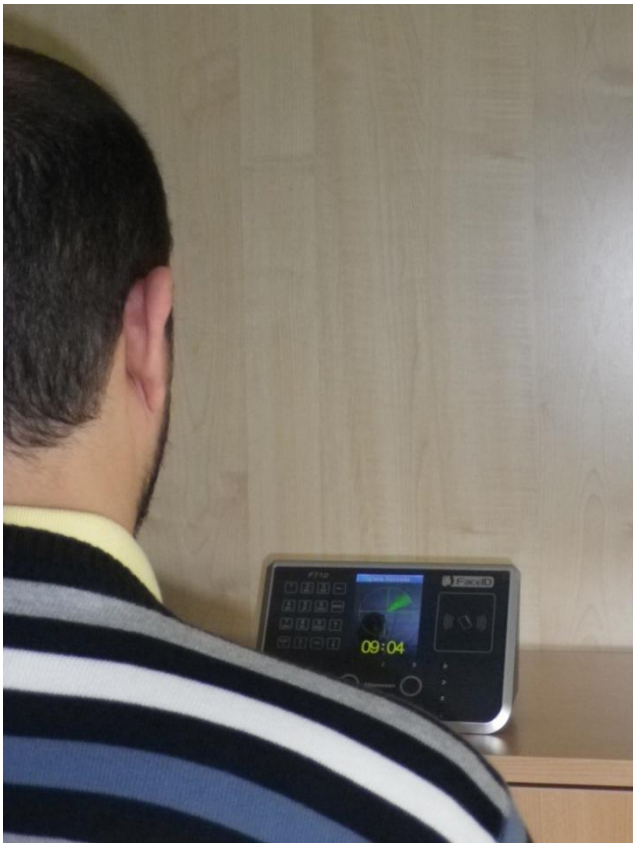


Ilustración 93.- Identificación en terminal biométrico facial en aplicación de control de asistencia a centros docentes.

Se ha desarrollado un sistema basado en biometría por reconocimiento facial que permite a los alumnos registrar su acceso a clase de forma muy rápida y cómoda. El profesor puede posteriormente visualizar los datos desde su despacho, casa o dispositivo móvil así como exportarlos para su tratamiento o importación en el sistema de gestión de la Universidad.

El dispositivo de reconocimiento facial utilizado trabaja obteniendo imágenes del individuo en el espectro de infrarrojos simultáneamente desde dos cámaras. Esto permite hacer una reconstrucción tridimensional del rostro y se parametrizan las distancias y posiciones relativas de puntos especialmente relevantes de la cara: pómulos, línea de frontera de la nariz, etc.

Ilustración 94.- Entorno de usuario de la solución para control de asistencia en centros docentes.

El sistema se utilizó en el curso 2011 en la Universidad de Oviedo, asignatura de Soldadura con 188 alumnos matriculados con excelentes resultados:

- ✓ Ahorro del tiempo de revisión y transcripción de firmas al listado de asistencias por parte del profesor, permitiendo visualizar asistencias o "no asistencias", puntualidad, etc.
- ✓ Ahorro de tiempo para los alumnos
- ✓ Control riguroso de la asistencia y puntualidad sin posibilidad de picarescas.

Es interesante resaltar que en el curso citado había dos alumnos gemelos que han sido distinguidos sin problemas. Los alumnos y alumnas con cabello muy largo tenían problemas inicialmente ya que es importante no tener pelo por la cara para una identificación exitosa. Una vez claro esto no presentaron tampoco ningún problema.

Los tiempos de identificación comenzaron en unos 15s por persona en las primeras sesiones y bajaron al entorno de unos 6” de media. El registro de una persona nueva suele llevar entre unos 30” y un minuto.

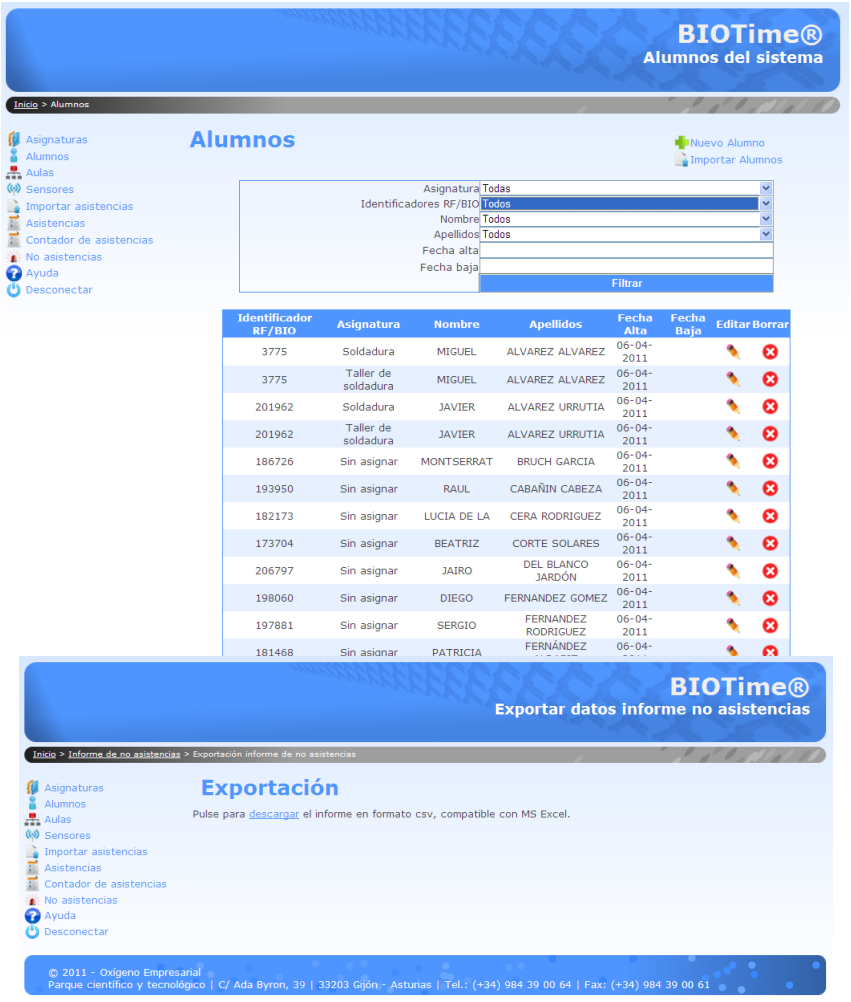


Ilustración 95.- Visión en pantalla de un informe y ventana de exportación.

El dispositivo de reconocimiento utilizado es muy ligero de peso y manejable lo que permite su utilización portátil controlando el acceso al aula y al laboratorio en que se realizaban las prácticas con un solo equipo.

Las conclusiones del proyecto realizado fueron:

- ✓ El sistema es suficientemente ágil y fiable
- ✓ Se ha adaptado bien a los casos problemáticos definidos a priori que pudieron probarse (gemelos, cabello largo, cambios de imagen, etc.)

- ✓ No ha habido rechazo por parte del alumnado. Al contrario, en la encuesta realizada veían como muy positiva su utilización para dar mayor justicia al sistema de evaluación y recomendaban su utilización en los exámenes.
- ✓ El ahorro de tiempo para el profesor alcanza las expectativas
- ✓ De todos los alumnos, uno ha tenido problemas de identificación por nerviosismo. Es minoritaria pero ya se había experimentado con otros sistemas que hay personas que se sienten incómodas ante los dispositivos biométricos.

5 Conclusiones y extensiones

Conclusiones

El presente trabajo ha arrojado las conclusiones que se detallan a continuación. El grado de interés del tema ha quedado patente tras el desarrollo del trabajo y la dificultad prevista para su estudio se ha corroborado puesto que las tecnologías están en continua evolución impulsadas por la industria que es, lógicamente, limitadamente permeable a mostrar sus avances o fracasos. Además la agilidad del desarrollo tecnológico es tremenda, habiendo aparecido soluciones que han desplazado ya a algunas otras en el tiempo transcurrido entre el inicio y final de los trabajos.

- ✓ **Validación de la adecuación de las herramientas de autoidentificación a las personas y de su creciente grado de implantación a nivel global.**

  El estudio de casos de implantaciones y resultados ha demostrado que la autoidentificación de personas tiene una implantación creciente tanto desde el punto de vista vertical (número de implantaciones de una aplicación determinada) como en el horizontal (nuevas aplicaciones y soluciones que van apareciendo).

  En muchísimas aplicaciones el control manual ha sido erradicado por la autoidentificación valiéndose de una u otra tecnología: control de presencia y accesos en centros de trabajo, cajeros automáticos, etc. Las aplicaciones emergentes (centros docentes, cuidados de personas, eventos deportivos y culturales, etc.) van viendo como la aplicación de las técnicas de autoidentificación crece inexorablemente.

- ✓ **Tecnología RFID de proximidad: madura y útil en multitud de aplicaciones**

  La tecnología RFID de proximidad es, por implantación, la dominante en el sector del control de personas en centros de trabajo. Ha desbancado a las tarjetas de banda magnética por su mayor seguridad, duración y comodidad de uso y sólo en algunas aplicaciones se ve superada por las tarjetas inteligentes (chip) cuando los requisitos de seguridad o almacenamiento son muy elevados.

Los lectores y tarjetas de proximidad son muy económicos y robustos y están disponibles en multitud de configuraciones (intemperie, sobremesa, bajo coste) constituyéndose a día de hoy en una "commodity". Es una tecnología madura y totalmente probada que hasta hace muy poco era la elección clara en sistemas de control de accesos.

- ✓ **Tecnología RFID de largo alcance: en fase de incipiente madurez, con un gran potencial en un marco temporal intermedio**

Como se ha venido demostrando en eventos deportivos la tecnología RFID de largo alcance permite la identificación de un gran caudal de paso de individuos. Sus aplicaciones en control de presencia son interesantes en ciertas aplicaciones donde llevar un identificador es todavía aceptable y donde sus elevados costes pueden absorberse.

Su aplicación a personas puede quedar reducida con el tiempo a los casos en los que una identificación rápida y masiva sea necesaria o donde la tecnología esté ya presente para el control de materiales, vehículos, etc. beneficiándose de dicha infraestructura.

A largo plazo está llamada a desaparecer cuando la identificación biométrica sea suficientemente rápida y trabaje fiablemente a distancia.

- ✓ **Biometría – solución de presente en muchas aplicaciones. ¿Solución de futuro para la totalidad?**

El reconocimiento biométrico es la gran revolución del momento actual. Sus ventajas, principalmente:

  - Comodidad de uso, no es necesario portar una tarjeta
  - Eliminación de los costes de gestión de tarjetas
  - Eliminación de la picaresca de suplantación de identidad, etc.,

La están haciendo merecedora de cada vez un mayor interés y de un mayor grado de implantación.

Cuando los avances tecnológicos lo permitan, se constituirá en la herramienta universal de identificación de personas. Para ello han de salvarse los siguientes inconvenientes:

- ✓ Identificación a distancia
- ✓ Identificación "simultánea" de individuos
- ✓ Dificultad de utilización por parte de un porcentaje de la población

Los dos primeros avances necesarios enumerados aún tardarán probablemente muchos años en producirse pero, el interés de la tecnología y el continuo avance de la capacidad de proceso de los equipos lo convierten en algo previsiblemente factible en el futuro.

- ✓ **Biometría – ¿qué tecnologías tienen mayor grado de madurez y resultan más interesantes en el presente y previsión de futuro?**

De entre las tecnologías biométricas disponibles, se considera la huella dactilar la gran dominadora en la actualidad por su gran implantación y su reducido coste aunque presenta los siguientes problemas:

- o Inseguridad: es fácil robar la identidad de una persona y falsear un lector.
- o Sensibilidad a la suciedad, daños superficiales en la yema de los dedos, etc.
- o Higiene: es un potencial foco de contagio de gripe, etc.

Otras tecnologías como el reconocimiento de iris, los mapas vasculares o el reconocimiento facial están avanzando considerablemente tanto en prestaciones, fiabilidad y sencillez de uso como en costes y, con ello, en grado de implantación. Es previsible que en un plazo corto-medio desplacen a la huella dactilar en todo tipo de aplicaciones.

De entre ellas, muy probablemente la que tenga un mayor desarrollo en cuanto a capacidad de detección de individuos a distancia sean la del reconocimiento facial o del reconocimiento de iris ya que técnicamente resulta más fácil la captación de datos a distancia que en los otros casos en los que además, las manos pueden ir ocupadas, flexionadas, etc. dificultando dicha captura.

- ✓ **La prevención de riesgos: un campo maduro tecnológicamente y aún poco explorado**

  Se ha visto que desde el punto de vista de la potenciación de la gestión del comportamiento como disciplina clave en la prevención de riesgos laborales las herramientas de autoidentificación tienen un papel potencial por su facilidad para mejorar el control y la realización "automática" de auditorías de comportamiento.

- ✓ **Centros docentes – excelente campo de aplicación de la biometría**

  El trabajo de investigación del estado del arte y experiencias realizado completado con el trabajo de campo desarrollado en Asturias a través de las encuestas corrobora el potencial de las herramientas de autoidentificación y, muy especialmente de las biométricas, en el campo de la docencia.

  Pese a que hay diversidad de opiniones en la comunidad docente, es cada día mayor la tendencia a potenciar el trabajo continuo de los alumnos y su evaluación como uno de los factores de éxito del sistema educativo del futuro, tal y como recomienda el Plan de Bolonia. La asistencia a clase es uno de los pilares de este modelo docente y las tecnologías biométricas por su sencillez de implantación (no requieren entrega y control de tarjetas), fiabilidad, rapidez suficiente y, sobre todo, invulnerabilidad a la picaresca de la suplantación de identidad se constituyen como solución ideal de futuro.

- ✓ **Tecnologías de autoidentificación que prevalecerán**

  De forma global, del estudio realizado, se desprende que las tecnologías de autoidentificación actuales que prevalecerán en el futuro serán:

  Código de barras. Por su bajísimo coste y sencillez seguirá siendo útil en identificación de productos, especialmente en la venta al por menor.

  RFID. El RFID de largo alcance complementará al código de barras en la gestión de la cadena de suministro (a nivel agrupación) y además será idóneo para identificación de vehículos, herramientas, EPIS, etc.

  Biometría. En la identificación de personas su evolución ha de ser la de seguir robando cuota de implantación al resto de tecnologías de forma continua y acabar imponiéndose en la totalidad de aplicaciones.

Extensiones

Con el presente trabajo se cree que se han evaluado las posibilidades de la tecnología en su estadio actual y en el desarrollo esperable a corto plazo.

Ha resultado muy interesante ver cómo evolucionan las tecnologías y cómo está de cerca de la realidad la identificación biométrica masiva involuntaria: identificar a las personas fiablemente y sin su intervención voluntaria.

Esta tecnología presenta problemas desde el punto de vista de la privacidad que no son distintos de los de las cámaras de video-vigilancia por lo que esto no ha de ser un obstáculo.

Las aplicaciones de este salto tecnológico serían amplísimas: aeropuertos, colegios, carreras populares, eventos, etc. A día de hoy estas situaciones se atacan con la tecnología RFID que quedaría entonces obsoleta.

El camino previsto para este desarrollo ha de venir trazado por el avance en dos disciplinas distintas:

- ✓ La identificación de alta velocidad
- ✓ La identificación a distancia

De ellas la primera está madurando muy rápidamente y es natural que en un plazo de tiempo corto se disponga de tecnologías suficientemente rápidas. La segunda presenta a día de hoy el mayor reto. Se está lógicamente trabajando en identificación gestual, facial, etc. y en la combinación de varias para conseguirlo. Se concluye del presente trabajo que sería un campo de interés para un nuevo trabajo de tesis doctoral una vez la tecnología haya madurado lo suficiente.

Bibliografía

Alton Towers: Your Day RFID video capture system. [En línea] [Citado el: 12 de marzo de 2010.] http://touch.schematic.com/2009/01/alton-towers-your-day-rfid-video-capture-system/.

What is a Contact Memory Button (CMB)? [En línea] [Citado el: 15 de abril de 2010.] http://www.macsema.com/buttonmemory.htm.

Ahrcanum. VeriChip RFID Human Implant Identifies H1N1 Swine Flu, Can it Track You Too. [En línea] [Citado el: 10 de marzo de 2010.] http://ahrcanum.wordpress.com/2009/09/22/verichip-rfid-human-implant-swine-flu-tracking/.

arjun. electricalandelectronics. [En línea] [Citado el: 10 de marzo de 2010.] http://electricalandelectronics.org/2008/11/17/what-is-a-verichip/.

Bengo. Kriptópolis. *Logran clonar el chip subcutáneo de Verichip.* [En línea] [Citado el: 19 de marzo de 2010.] http://www.kriptopolis.org/logran-clonar-el-chip-subcutaneo-de-verichip.

Best, Jo. Japan school kids to be tagged with RFID chips. [En línea] [Citado el: 8 de marzo de 2010.] http://news.cnet.com/Japan-school-kids-to-be-tagged-with-RFID-chips/2100-1012_3-5266700.html.

Bormart. *La tecnología rfid y su problemática en protección de datos.* [En línea] [Citado el: 12 de marzo de 2010.] http://www.borrmart.es/articulo_redseguridad.php?id=200&numero=15.

Boulat, Alexandra. 2002. National Geographic - A life Revealed. [En línea] National Geographic, 2002. [Citado el: 15 de 05 de 2011.] http://ngm.nationalgeographic.com/2002/04/afghan-girl/mccurry-photography.

Carrasco, Eva Gotor. 2009. *Estado del arte en tecnologías RFID.* 2009.

CiberHabitat. *Identificación biométrica con huellas digitales.* [Online] [Cited: marzo 23, 2010.] http://www.ciberhabitat.gob.mx/hospital/huellas/apliaciones.htm.

CiberHabitat. *Identificación biométrica con huellas digitales.* [En línea] [Citado el: 23 de marzo de 2010.] http://www.ciberhabitat.gob.mx/hospital/huellas/apliaciones.htm.

Collins, Jonathan. Rfid Journal. *Sweden Switches to E-Passports.* [En línea] [Citado el: 19 de marzo de 2010.] http://www.rfidjournal.com/article/articleview/1942/1/1/.

Consentino, Luis. *Control de accesos. Elementos de identificación.*

Cosgrove-Mather, Bootie. CBS news. *Japanese Kids Get Radio ID'd.* [En línea] [Citado el: 15 de marzo de 2010.] http://www.cbsnews.com/stories/2004/10/11/tech/main648681.shtml.

CR80 news. *Indian school Keeptrack of students with RFID.* [En línea] [Citado el: 9 de marzo de 2010.] http://www.cr80news.com/2010/02/03/indian-school-keeptrack-of-students-with-rfid.

CSO. BioGiltz, llave biométrica para discapacitados . [En línea] [Citado el: 5 de abril de 2010.] http://www.csospain.es/BioGiltz,-llave-biometrica-para-discapacitados/seccion-tecnolog%C3%ADas/articulo-195372.

Cuellar Fernández, Arturo. Seguridad Integral en la Empresa.

DiscoverRFID. *Texas desarrolla un sistema de evacuación de emergencia basado en RFID.* [En línea] [Citado el: 8 de abril de 2010.] http://www.discoverrfid.org/es/que-es-posible/sentirse-seguro/sistema-de-evacuacion.html.

Dougman, John. John Daugman - . *Professor of Computer Vision and Pattern Recognition* . [En línea] University of Cambridge. [Citado el: 15 de 05 de 2010.] http://www.cl.cam.ac.uk/~jgd1000/.

Editors, EgovAsia. Enterprise Innovation. *County jail uses RFID wristbands to monitor detainees.* [En línea] [Citado el: 23 de marzo de 2010.] http://www.enterpriseinnovation.net/content/county-jail-uses-rfid-wristbands-monitor-detainees.

2010. El internet de las cosas "revolucionará las relaciones entre objetos y personas". [En línea] 22 de marzo de 2010. [Citado el: 6 de Junio de 2010.] http://www.europarl.europa.eu/news/public/story_page/039-70542-067-03-11-906-20100312STO70527-2010-08-03-2010/default_es.htm.

2005. *EPC UHF Clase 1 Generación2.* s.l. : RFID magazine, 2005.

Ética y controversias en informática. *¿Será Posible Que La Tecnología RFID Rastree Todos Tus Movimientos?* [En línea] [Citado el: 22 de marzo de 2010.] http://mlarracuente.wordpress.com/2009/02/27/%C2%BFsera-posible-que-la-tecnologia-rfid-rastree-todos-tus-movimientos/.

Fennig, Chris. 2005. *INTERFERENCIA EN LECTORES RFID.* s.l. : ODIN technologies, 2005.

Finger Vein Authentication: White Paper.

García, C. 2010. Los funcionarios de Justicia ya fichan con su huella dactilar. *La Voz de Asturias.* 2010.

Gardner, David. Global CIO. *RFID Chips Implanted In Mexican Law-Enforcement Workers.* [En línea] [Citado el: 22 de marzo de 2010.] http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=23901004.

Gema A.B.S. [En línea] [Citado el: 13 de marzo de 2010.] http://www.gemaabs.com/index.php?option=com_content&task=view&id=45&Itemid=131&lang=es.

Gutierrez, David. U.S. School District to Begin Microchipping Students. [En línea] [Citado el: 9 de marzo de 2010.] http://www.naturalnews.com/023445.html.

Impact of Artificial "Gummy" fingers on fingerprint systems. **Matsumoto, Tsutomu, y otros. 2002.** Yokohama National University : Rudolf L. Van Renesse, 2002, Vols. Optical Security and Countefeit Deterrence Techniques IV. Proceedings of SPIE, Vol. 4677. 0277-786x/02/.

Industria-IT.com. *La empresa australiana Wtek crea un sistema RFID de localización de mineros.* [En línea] [Citado el: 8 de abril de 2010.] http://www.industriait.com/articulo/_la_empresa_australiana_wtek_crea_un_sistema_rfid_de_localizacion_de_mineros_48.

Marcelo Davila Vargas, Fernando. Sistema biométrico de identificiación de personas mediante el análisis de los patrones del iris, aplicado al control de accesos de áreas restringidas.

Masaki Watanabe, Toshio Endoh, Morito Shiohara, and Shigeru Sasak. 2005. Palm vein authentication technology and its applications. *Fujitsu Laboratories.* 2005.

Mayné, Jordi. 2009. *Sistemas de auto-identificación.* 2009.

Montes, Bernardo. *"Impacto de la tecnología RFID en los modelos de negocio actuales y nuevas oportunidades de negocio.*

O. Foley, Mary. Su recurso de seguridad. *Chips RFID y su privacidad.* [En línea] [Citado el: 22 de marzo de 2010.] http://www.yoursecurityresource.com/es/articles/rfid/index.html.

Palao, Juan. [En línea] [Citado el: 22 de marzo de 2010.] http://palaoc.blogspot.com/2009/10/tecnologia-rfid.html.

Panasonic. [En línea] http://www.panasonic.com/business/security/bm-et300_demo/iris.html.

Pérez Cortés, Juan Carlos. *Parámetros biométricos de seguridad.* s.l. : Instituto Tecnológico de Informática, Universidad Politécnica de Valencia.

Portillo, Javier. 2003. Sistemas de identificación biométrica. 2003.

Portillo, Javier, Bermejo, Ana Belén y Bernardos, Ana M. *Tecnología de identificación por radiofrecuencia (RFID) Aplicaciones en el ámbito de la salud.* s.l. : Fundación madri+d para el Conocimiento.

PositiveID. [En línea] [Citado el: 10 de marzo de 2010.] http://www.positiveidcorp.com/about-us.html.

PositiveID. [En línea] [Citado el: 10 de marzo de 2010.] http://investors.positiveidcorp.com/releasedetail.cfm?ReleaseID=446070.

PositiveID. [En línea] [Citado el: 10 de marzo de 2010.] http://investors.positiveidcorp.com/releasedetail.cfm?ReleaseID=447181.

PrisionPlanet. *Baja Beach Club in Barcelona, Spain Launches Microchip Implantation for VIP Members.* [En línea] [Citado el: 15 de marzo de 2010.] http://www.prisonplanet.com/articles/april2004/040704bajabeachclub.htm.

Privaris. *SmartWatch SecurePass Wireless Biometric Authentication of Vehicle Occupants.*

Privaris white paper. *Achieving Universal Secure Identity Verification with.* [En línea] [Citado el: 6 de abril de 2010.]

Puigbò, Jaume. RFID MAGAZINE. *¿Cómo está evolucionando la RFID?* [En línea] [Citado el: 16 de abril de 2010.] http://www.rfid-magazine.com/opinion/index.php?id=867.

R. Modesti, Mario. Sistemas de códigos de barras . [En línea] [Citado el: 14 de abril de 2010.] http://www.profesores.frc.utn.edu.ar/industrial/sistemasinteligentes/UT6/Bar_Code.pdf.

RFId Activa+ RFID pasiva=Hospital del futuro. **Francés, Paloma.** s.l. : RFID magazine.

RFID gazette. *Combining RFID and Biometrics For Security.* [En línea] [Citado el: 6 de abril de 2010.] http://www.rfidgazette.org/2006/07/combining_rfid_.html.

RFID Takes Attendance—and Heat. **O'Connor, Mary Catherine. 2005.** s.l. : RfidJournal, 2005.

RfidSpain. *Akrocard lanzó nuevas tarjetas de identificación híbridas que utilizan tecnología sin contacto y un chip de contacto.* [En línea] [Citado el: 11 de marzo de 2010.] http://www.rfid-spain.com/articulo/69622/rfid/otros/akrocard-lanzo-nuevas-tarjetas-de-identificacion-hibridas-que-utilizan-tecnologia-sin-contacto-y-un-chip-de-contacto.

RfidSpain. *El hospital costa del sol utiliza fid en las pulseras de los pacientes para reducir el peligro de errores.* [En línea] [Citado el: 11 de marzo de 2010.] http://www.rfid-spain.com/articulo/69600/rfid/hospitales-y-clinicas/el-hospital-costa-del-sol-utiliza-rfid-en-las-pulseras-de-los-pacientes-para-reducir-el-peligro-de-errores.

RfidSpain. *Una escuela publica de taipei utiliza rfid para controlar la entrada y salida de los niños.* [En línea] [Citado el: 9 de marzo de 2010.] http://www.rfid-spain.com/articulo/35681/rfid/educacion/una-escuela-publica-de-taipei-utiliza-rfid-para-controlar-la-entrada-y-salida-de-los-ninos.

RfidSpain. *La prisión estadounidense Hardin County Jail utiliza pulseras RFID para gestionar la información de los reclusos.* [En línea] [Citado el: 11 de marzo de 2010.] http://www.rfid-spain.com/articulo/69709/rfid/otros/la-prision-estadounidense-hardin-county-jail-utiliza-pulseras-rfid-para-gestionar-la-informacion-de-los-reclusos.

Rhode Island Governor Vetoes Restrictions on RFID. **Swedberg, Claire. 2009.** s.l. : RfidJournal, 2009.

Ross, Gary. *Biometrics: A self-service viewpoin.* s.l. : NCR Corporation Inc.

Sabater Suau, Bartolomé. *Marketing RFID.*

Scheeres, Julia. Three R's: Reading, Writing, RFID. [En línea] [Citado el: 7 de marzo de 2010.] http://www.wired.com/science/discoveries/news/2003/10/60898#Replay.

Tedjasaputra, Adi. RFID and Children: The World is Not Enough. [En línea] [Citado el: 8 de marzo de 2010.] http://rfid-asia.info/2006/08/rfid-and-children-world-is-not-enough.htm.

Teoría y aplicación de la informática. [En línea] http://www.jeuazarru.com/docs/biometria.pdf.

Torrealba, Enrique. *Avances en técnicas biométricas y sus aplicaciones en seguridad.*

Treelogic RFID. [En línea] [Citado el: 23 de marzo de 2010.] http://rfid.treelogic.com/noticias/noticia3.html.

Using RFID.com. *Biometrics and RFID combined for access control.* [En línea] [Citado el: 5 de abril de 2010.] http://www.usingrfid.com/news/read.asp?lc=u27452rx393zl.

Walker, Chris. School puts a chip on pupils. *FreePress.* [En línea] [Citado el: 10 de abril de 2010.] http://www.doncasterfreepress.co.uk/free-press-news/School-puts-a-chip-on.3391369.jp.

WorldNetDaily. *Employees get microchip implants.* [En línea] [Citado el: 10 de marzo de 2010.] http://www.wnd.com/news/article.asp?ARTICLE_ID=48760.

WorldNetDaily. *Employees get microchip implants.* [En línea] [Citado el: 10 de marzo de 2010.] http://www.wnd.com/news/article.asp?ARTICLE_ID=48760.

ANEXOS

- ✓ Encuesta realizada a Centros Docentes Asturianos
- ✓ Resultados validación sistema control asistencia congresos
- ✓ Estudio aplicación RFID al control de EPIs

ANEXO I .- ENCUESTA REALIZADA A CENTROS DOCENTES ASTURIANOS

DATOS GENERALES

1.-Tipo de centro

- ☐ Público
- ☐ Privado
- ☐ Concertado
- ☐ Otros

2.-Tipo de estudios impartidos

- ☐ Infantil 0-3
- ☐ Infantil y primaria
- ☐ Secundaria
- ☐ Bachiller
- ☐ FP
- ☐ Otros

3.- ¿El centro posee biblioteca?

- ☐ Sí
- ☐ No

3.1.-¿Se encuentra gestionada mediante algún tipo de programa informático?

- ☐ Sí. ¿Cuál?
- ☐ No

3.2 Grado de satisfacción con el programa.

- ☐ Muy bueno
- ☐ Bueno
- ☐ Aprobado
- ☐ Regular
- ☐ Necesita mejorar
- ☐ Ns/Nc

4.- ¿Las tareas administrativas se encuentran gestionadas mediante algún programa informático?

- ☐ Sí. ¿Cuál?
- ☐ No

4.1 Grado de satisfacción con el programa.

- ☐ Muy bueno
- ☐ Bueno
- ☐ Aprobado
- ☐ Regular
- ☐ Necesita mejorar
- ☐ Ns/Nc

CONOCIMIENTOS DE LA TECNOLOGÍA

1.- ¿Sabe que son los sistemas de auto-identificación?

- ☐ Sí
- ☐ No
- ☐ Ns/Nc

2.-¿Conoce algún ejemplo de sistema de auto-identificación?

- ☐ Sí. ¿Cuál/es?
- ☐ No
- ☐ Ns/Nc

3.-¿Conoce el sistema RFID?

- ☐ Sí
- ☐ No
- ☐ Ns/Nc

4.- ¿Conoce alguna de sus aplicaciones?

- ☐ Sí. ¿Cuál/es?
- ☐ No
- ☐ Ns/Nc

IMPLANTACIÓN DEL SISTEMA

1.- Califique como (4) muy interesante/ (3) interesante/ (2) práctico/ (1) no necesario las siguientes ventajas que puede ofrecer la implantación del sistema de auto-identificación en el centro docente:

	4	3	2	1
Localización en tiempo real del alumno dentro del centro				
Posibilidad de enviar mensajes al teléfono móvil de los padres para indicar si su hijo ha salido o no del centro				
Control de acceso a diferentes áreas del centro				
Identificación automática del alumno sin necesidad de pasar lista				
Control de activos en bibliotecas de manera automatizada				

2.- ¿Le interesaría implantar estas características en el centro de docencia?

- ☐ No interesa
- ☐ Sólo si es gratuito
- ☐ Interesa
- ☐ Ns/Nc

3.- ¿Dónde le parece más eficaz que el alumno lleve la etiqueta identificadora?

- ☐ Tarjeta identificadora
- ☐ Pulsera
- ☐ Collar
- ☐ Cosido en los uniformes
- ☐ Otros

SUGERENCIAS

Si tiene alguna sugerencia o duda, sobre alguna posible mejora en los centros docentes que se pueda realizar mediante la auto-identificación automáticas por favor, escríbala en las líneas posteriores

AGRADECIMIENTO

Gracias por su colaboración

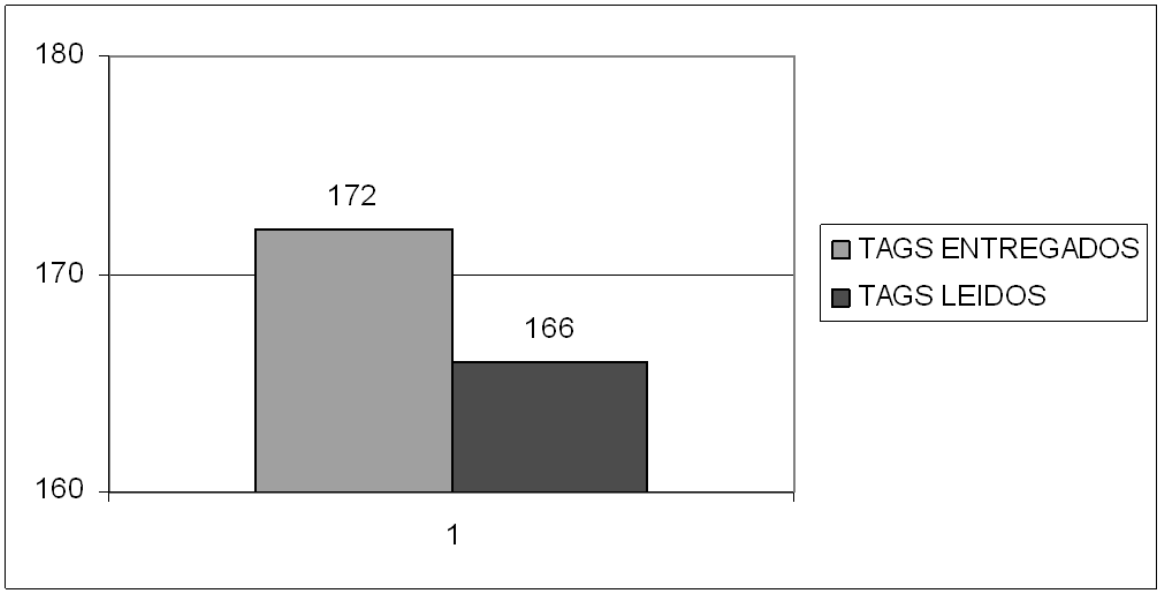
ANEXO II.- Conclusiones análisis fiabilidad congreso Rapid Manufacturing 08 (primera experiencia en congresos)

Congreso Rapid Manufacturing 08.

Conclusiones sobre fiabilidad de detección del sistema RFID utilizado

El siguiente gráfico muestra la comparación entre los tags entregados a asistentes y los tags leídos.

Asumiendo que los 6 entregados entraran efectivamente en la zona de congresos (es posible que no hubiese sido así) la fiabilidad en detección del sistema se estima en un 97%. Esta fiabilidad es menor que la esperada y se atribuye a que se observo que en muchos casos las identificaciones no eran llevadas de acuerdo a las instrucciones sino en carteras o bolsos lo que dificulta su detección.



ANEXO III .- EXPERIMENTACIÓN DE LA UTILIZACIÓN DE LA TECNOLOGÍA RFID DE LARGO ALCANCE PARA EL CONTROL DE EQUIPOS DE PROTECCIÓN INDIVIDUAL (EPIs)

1.- PLANTEAMIENTO

La experimentación se ha planteado en dos fases. En una primera fase se realiza una experimentación inicial de las tecnologías, en las que se juega con variables de carácter ambiental, y que pretenden mostrar si dichas tecnologías son viables bajo ciertas condiciones.

En caso afirmativo, se pasará a la segunda parte de la experimentación, donde se realizarán las pruebas bajo condiciones reales de ubicación y colocación de identificadores, con las variables que han dado mejores resultados en la primera fase.

2.- EXPERIMENTO INICIAL DE TENOLOGÍA

Para realizar la comprobación de la tecnología se han diseñado dos experimentos, uno para cada tipo de tecnología a probar. A continuación se detalla el proceso seguido para cada prueba.

2.1.- UHF

Se han dispuesto 4 antenas en la parte superior de un pórtico (a 3m de altura) de ancho variable, siempre a una distancia equidistante entre ellas y proporcional a la anchura del pórtico para cubrir la máxima distancia posible. Las pruebas se realizarán con tres anchos distintos, de 2, 5 y 9 metros.

También se realizarán en distintos ambientes como entorno, en este caso se ha probado en interiores y en exteriores, en este último tanto en húmedo como en seco. Para simular la lluvia se ha utilizado un pulverizador de agua. Antes de realizar la pasada por el pórtico, se pulverizaba agua en el espacio entre las antenas y los identificadores para realizar una correcta simulación.

También se ha probado con materiales que pueden ser comunes en la identificación tanto de personas como de EPIs, como puedan ser metales, ropa, o PVC (utilizado a modo de material plástico genérico). Para los elementos de metal se han utilizado identificadores especiales para metales, ya que de lo contrario el ratio de lecturas sería siempre del 0%.

Los identificadores se han dispuesto sobre cada material en grupos de 5 y de 20, para realizar las pasadas con el número de identificadores que corresponda.

A continuación se presenta el detalle de los distintos experimentos realizados en los que no se ha obtenido un 100% de lecturas. Para cada experimento se ha realizado 10 repeticiones.

Ancho	5	Entorno	Exterior (h)
Material	Ropa	**Nº tags**	20
	Tags leídos	**% Leídos**	**% No leídos**
1	18	90,00%	10,00%
2	20	100,00%	0,00%
3	20	100,00%	0,00%
4	20	100,00%	0,00%
5	20	100,00%	0,00%
6	20	100,00%	0,00%
7	20	100,00%	0,00%
8	20	100,00%	0,00%
9	19	95,00%	5,00%
10	20	100,00%	0,00%
	Total	**98,50%**	**1,50%**

0-1: Detalle experimento 26 UHF

Ancho	5	Entorno	Exterior (s)
Material	Ropa	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	5	100,00%	0,00%
2	5	100,00%	0,00%
3	5	100,00%	0,00%
4	5	100,00%	0,00%
5	4	80,00%	20,00%
6	5	100,00%	0,00%
7	5	100,00%	0,00%
8	5	100,00%	0,00%
9	5	100,00%	0,00%
10	5	100,00%	0,00%
	Total	**98,00%**	**2,00%**

Figura 0-2: Detalle experimento 27 UHF

Ancho	5	Entorno	Exterior (s)
Material	Ropa	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	20	100,00%	0,00%
2	20	100,00%	0,00%
3	20	100,00%	0,00%
4	20	100,00%	0,00%
5	19	95,00%	5,00%
6	19	95,00%	5,00%
7	20	100,00%	0,00%
8	20	100,00%	0,00%
9	20	100,00%	0,00%
10	20	100,00%	0,00%
	Total	**99,00%**	**1,00%**

Figura 0-3: Detalle experimento 28 UHF

Ancho	5	Entorno	Exterior (h)
Material	PVC	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	5	100,00%	0,00%
2	5	100,00%	0,00%
3	5	100,00%	0,00%
4	5	100,00%	0,00%
5	5	100,00%	0,00%
6	5	100,00%	0,00%
7	5	100,00%	0,00%
8	5	100,00%	0,00%
9	5	100,00%	0,00%
10	4	80,00%	20,00%
	Total	**98,00%**	**2,00%**

Figura 0-4: Detalle experimento 31 UHF

Ancho	5	Entorno	Exterior (h)
Material	PVC	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	20	100,00%	0,00%
2	20	100,00%	0,00%
3	20	100,00%	0,00%
4	20	100,00%	0,00%
5	20	100,00%	0,00%
6	18	90,00%	10,00%
7	20	100,00%	0,00%
8	20	100,00%	0,00%
9	20	100,00%	0,00%
10	20	100,00%	0,00%
	Total	**99,00%**	**1,00%**

Figura 0-5: Detalle experimento 32 UHF

Ancho	5	Entorno	Exterior (s)
Material	PVC	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	20	100,00%	0,00%
2	20	100,00%	0,00%
3	20	100,00%	0,00%
4	20	100,00%	0,00%
5	20	100,00%	0,00%
6	20	100,00%	0,00%
7	19	95,00%	5,00%
8	20	100,00%	0,00%
9	20	100,00%	0,00%
10	20	100,00%	0,00%
	Total	**99,50%**	**0,50%**

Figura 0-6: Detalle experimento 34 UHF

Ancho	5	Entorno	Interior
Material	PVC	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	19	95,00%	5,00%
2	20	100,00%	0,00%
3	20	100,00%	0,00%
4	19	95,00%	5,00%
5	20	100,00%	0,00%
6	20	100,00%	0,00%
7	20	100,00%	0,00%
8	20	100,00%	0,00%
9	20	100,00%	0,00%
10	20	100,00%	0,00%
	Total	**99,00%**	**1,00%**

Figura 0-7: Detalle experimento 36 UHF

Ancho	9	Entorno	Exterior (h)
Material	Metal	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	4	80,00%	20,00%
2	4	80,00%	20,00%
3	5	100,00%	0,00%
4	5	100,00%	0,00%
5	5	100,00%	0,00%
6	4	80,00%	20,00%
7	5	100,00%	0,00%
8	5	100,00%	0,00%
9	5	100,00%	0,00%
10	5	100,00%	0,00%
	Total	**94,00%**	**6,00%**

Figura 0-8: Detalle experimento 37 UHF

Ancho	9	Entorno	Exterior (h)
Material	Metal	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	20	100,00%	0,00%
2	16	80,00%	20,00%
3	19	95,00%	5,00%
4	20	100,00%	0,00%
5	20	100,00%	0,00%
6	18	90,00%	10,00%
7	20	100,00%	0,00%
8	19	95,00%	5,00%
9	18	90,00%	10,00%
10	17	85,00%	15,00%
	Total	**93,50%**	**6,50%**

Figura 0-9: Detalle experimento 38 UHF

Ancho	9	Entorno	Exterior (s)
Material	Metal	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	5	100,00%	0,00%
2	5	100,00%	0,00%
3	4	80,00%	20,00%
4	4	80,00%	20,00%
5	4	80,00%	20,00%
6	5	100,00%	0,00%
7	5	100,00%	0,00%
8	5	100,00%	0,00%
9	4	80,00%	20,00%
10	5	100,00%	0,00%
	Total	**92,00%**	**8,00%**

Figura 0-10: Detalle experimento 39 UHF

Ancho	9	Entorno	Exterior (s)
Material	Metal	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	20	100,00%	0,00%
2	18	90,00%	10,00%
3	17	85,00%	15,00%
4	17	85,00%	15,00%
5	19	95,00%	5,00%
6	20	100,00%	0,00%
7	20	100,00%	0,00%
8	16	80,00%	20,00%
9	20	100,00%	0,00%
10	18	90,00%	10,00%
	Total	**92,50%**	**7,50%**

Figura 0-11: Detalle experimento 40 UHF

Ancho	9	Entorno	Interior
Material	Metal	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	5	100,00%	0,00%
2	5	100,00%	0,00%
3	4	80,00%	20,00%
4	5	100,00%	0,00%
5	4	80,00%	20,00%
6	5	100,00%	0,00%
7	4	80,00%	20,00%
8	4	80,00%	20,00%
9	4	80,00%	20,00%
10	5	100,00%	0,00%
	Total	**90,00%**	**10,00%**

Figura 0-12: Detalle experimento 41 UHF

Ancho	9	Entorno	Interior
Material	Metal	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	16	80,00%	20,00%
2	20	100,00%	0,00%
3	19	95,00%	5,00%
4	18	90,00%	10,00%
5	20	100,00%	0,00%
6	20	100,00%	0,00%
7	17	85,00%	15,00%
8	19	95,00%	5,00%
9	20	100,00%	0,00%
10	20	100,00%	0,00%
	Total	**94,50%**	**5,50%**

Figura 0-13: Detalle experimento 42 UHF

Ancho	9	Entorno	Exterior (h)
Material	Ropa	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	4	80,00%	20,00%
2	4	80,00%	20,00%
3	3	60,00%	40,00%
4	4	80,00%	20,00%
5	3	60,00%	40,00%
6	3	60,00%	40,00%
7	3	60,00%	40,00%
8	4	80,00%	20,00%
9	4	80,00%	20,00%
10	5	100,00%	0,00%
	Total	**74,00%**	**26,00%**

Figura 0-14: Detalle experimento 43 UHF

Ancho	9	Entorno	Exterior (h)
Material	Ropa	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	14	70,00%	30,00%
2	12	60,00%	40,00%
3	15	75,00%	25,00%
4	16	80,00%	20,00%
5	15	75,00%	25,00%
6	17	85,00%	15,00%
7	14	70,00%	30,00%
8	18	90,00%	10,00%
9	15	75,00%	25,00%
10	13	65,00%	35,00%
	Total	**74,50%**	**25,50%**

Figura 0-15: Detalle experimento 44 UHF

Ancho	9	Entorno	Exterior (s)
Material	Ropa	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	5	100,00%	0,00%
2	5	100,00%	0,00%
3	3	60,00%	40,00%
4	3	60,00%	40,00%
5	2	40,00%	60,00%
6	4	80,00%	20,00%
7	4	80,00%	20,00%
8	3	60,00%	40,00%
9	4	80,00%	20,00%
10	3	60,00%	40,00%
	Total	**72,00%**	**28,00%**

Figura 0-16: Detalle experimento 45 UHF

Ancho	9	Entorno	Exterior (s)
Material	Ropa	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	11	55,00%	45,00%
2	18	90,00%	10,00%
3	12	60,00%	40,00%
4	13	65,00%	35,00%
5	12	60,00%	40,00%
6	15	75,00%	25,00%
7	15	75,00%	25,00%
8	16	80,00%	20,00%
9	18	90,00%	10,00%
10	17	85,00%	15,00%
	Total	**73,50%**	**26,50%**

Figura 0-17: Detalle experimento 46 UHF

Ancho	9	Entorno	Interior
Material	Ropa	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	3	60,00%	40,00%
2	3	60,00%	40,00%
3	3	60,00%	40,00%
4	4	80,00%	20,00%
5	3	60,00%	40,00%
6	4	80,00%	20,00%
7	4	80,00%	20,00%
8	5	100,00%	0,00%
9	4	80,00%	20,00%
10	3	60,00%	40,00%
	Total	**72,00%**	**28,00%**

Figura 0-18: Detalle experimento 47 UHF

Ancho	9	Entorno	Interior
Material	Ropa	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	9	45,00%	55,00%
2	15	75,00%	25,00%
3	13	65,00%	35,00%
4	18	90,00%	10,00%
5	17	85,00%	15,00%
6	17	85,00%	15,00%
7	18	90,00%	10,00%
8	14	70,00%	30,00%
9	13	65,00%	35,00%
10	17	85,00%	15,00%
	Total	**75,50%**	**24,50%**

Figura 0-19: Detalle experimento 48 UHF

Ancho	9	Entorno	Exterior (h)
Material	PVC	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	5	100,00%	0,00%
2	3	60,00%	40,00%
3	2	40,00%	60,00%
4	2	40,00%	60,00%
5	3	60,00%	40,00%
6	3	60,00%	40,00%
7	5	100,00%	0,00%
8	4	80,00%	20,00%
9	4	80,00%	20,00%
10	4	80,00%	20,00%
	Total	**70,00%**	**30,00%**

Figura 0-20: Detalle experimento 49 UHF

Ancho	9	Entorno	Exterior (h)
Material	PVC	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	15	75,00%	25,00%
2	14	70,00%	30,00%
3	14	70,00%	30,00%
4	15	75,00%	25,00%
5	17	85,00%	15,00%
6	17	85,00%	15,00%
7	18	90,00%	10,00%
8	12	60,00%	40,00%
9	13	65,00%	35,00%
10	15	75,00%	25,00%
	Total	**75,00%**	**25,00%**

Figura 0-21: Detalle experimento 50 UHF

Ancho	9	Entorno	Exterior (s)
Material	PVC	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	3	60,00%	40,00%
2	3	60,00%	40,00%
3	4	80,00%	20,00%
4	2	40,00%	60,00%
5	5	100,00%	0,00%
6	4	80,00%	20,00%
7	4	80,00%	20,00%
8	3	60,00%	40,00%
9	4	80,00%	20,00%
10	4	80,00%	20,00%
	Total	**72,00%**	**28,00%**

Figura 0-22: Detalle experimento 51 UHF

Ancho	9	Entorno	Exterior (s)
Material	PVC	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	17	85,00%	15,00%
2	17	85,00%	15,00%
3	13	65,00%	35,00%
4	15	75,00%	25,00%
5	16	80,00%	20,00%
6	15	75,00%	25,00%
7	14	70,00%	30,00%
8	14	70,00%	30,00%
9	11	55,00%	45,00%
10	15	75,00%	25,00%
	Total	**73,50%**	**26,50%**

Figura 0-23: Detalle experimento 52 UHF

Ancho	9	Entorno	Interior
Material	PVC	Nº tags	5
	Tags leídos	% Leídos	% No leídos
1	3	60,00%	40,00%
2	2	40,00%	60,00%
3	3	60,00%	40,00%
4	4	80,00%	20,00%
5	4	80,00%	20,00%
6	4	80,00%	20,00%
7	3	60,00%	40,00%
8	3	60,00%	40,00%
9	5	100,00%	0,00%
10	4	80,00%	20,00%
	Total	**70,00%**	**30,00%**

Figura 0-24: Detalle experimento 53 UHF

Ancho	9	Entorno	Interior
Material	PVC	Nº tags	20
	Tags leídos	% Leídos	% No leídos
1	14	70,00%	30,00%
2	12	60,00%	40,00%
3	15	75,00%	25,00%
4	14	70,00%	30,00%
5	16	80,00%	20,00%
6	12	60,00%	40,00%
7	17	85,00%	15,00%
8	16	80,00%	20,00%
9	17	85,00%	15,00%
10	14	70,00%	30,00%
	Total	**73,50%**	**26,50%**

Figura 0-25: Detalle experimento 54 UHF

En la figura 2-26 (siguiente página) se presenta un resumen de los experimentos realizados con las variables anteriormente comentadas.

Ancho	Material	Entorno	Nº tags	Leídos	No leídos
2	Metal	Exterior (h)	5	100,00%	0,00%
2	Metal	Exterior (h)	20	100,00%	0,00%
2	Metal	Exterior (s)	5	100,00%	0,00%
2	Metal	Exterior (s)	20	100,00%	0,00%
2	Metal	Interior	5	100,00%	0,00%
2	Metal	Interior	20	100,00%	0,00%
2	Ropa	Exterior (h)	5	100,00%	0,00%
2	Ropa	Exterior (h)	20	100,00%	0,00%
2	Ropa	Exterior (s)	5	100,00%	0,00%
2	Ropa	Exterior (s)	20	100,00%	0,00%
2	Ropa	Interior	5	100,00%	0,00%
2	Ropa	Interior	20	100,00%	0,00%
2	PVC	Exterior (h)	5	100,00%	0,00%
2	PVC	Exterior (h)	20	100,00%	0,00%
2	PVC	Exterior (s)	5	100,00%	0,00%
2	PVC	Exterior (s)	20	100,00%	0,00%
2	PVC	Interior	5	100,00%	0,00%
2	PVC	Interior	20	100,00%	0,00%
5	Metal	Exterior (h)	5	100,00%	0,00%
5	Metal	Exterior (h)	20	100,00%	0,00%
5	Metal	Exterior (s)	5	100,00%	0,00%
5	Metal	Exterior (s)	20	100,00%	0,00%
5	Metal	Interior	5	100,00%	0,00%
5	Metal	Interior	20	100,00%	0,00%
5	Ropa	Exterior (h)	5	100,00%	0,00%
5	Ropa	Exterior (h)	20	98,50%	1,50%
5	Ropa	Exterior (s)	5	98,00%	2,00%
5	Ropa	Exterior (s)	20	99,00%	1,00%
5	Ropa	Interior	5	100,00%	0,00%
5	Ropa	Interior	20	100,00%	0,00%
5	PVC	Exterior (h)	5	98,00%	2,00%
5	PVC	Exterior (h)	20	99,00%	1,00%
5	PVC	Exterior (s)	5	100,00%	0,00%
5	PVC	Exterior (s)	20	99,50%	0,50%
5	PVC	Interior	5	100,00%	0,00%
5	PVC	Interior	20	99,00%	1,00%
9	Metal	Exterior (h)	5	94,00%	6,00%
9	Metal	Exterior (h)	20	93,50%	6,50%
9	Metal	Exterior	5	92,00%	8,00%

		(s)			
9	Metal	Exterior (s)	20	92,50%	7,50%
9	Metal	Interior	5	90,00%	10,00%
9	Metal	Interior	20	94,50%	5,50%
9	Ropa	Exterior (h)	5	74,00%	26,00%
9	Ropa	Exterior (h)	20	74,50%	25,50%
9	Ropa	Exterior (s)	5	72,00%	28,00%
9	Ropa	Exterior (s)	20	73,50%	26,50%
9	Ropa	Interior	5	72,00%	28,00%
9	Ropa	Interior	20	75,50%	24,50%
9	PVC	Exterior (h)	5	70,00%	30,00%
9	PVC	Exterior (h)	20	75,00%	25,00%
9	PVC	Exterior (s)	5	72,00%	28,00%
9	PVC	Exterior (s)	20	73,50%	26,50%
9	PVC	Interior	5	70,00%	30,00%
9	PVC	Interior	20	73,50%	26,50%

Figura 0-26: Resumen experimento UHF

Tal y como se puede verificar en los resultados, se puede establecer un primer filtro de variables admisibles para el siguiente estudio. En el caso de un ancho de paso de 9 metros, la fiabilidad respecto a las detecciones decrece a unos niveles inaceptables, mientras que con los otros anchos de paso, el número de detecciones es perfectamente válido.

Llama la atención los porcentajes de lecturas fiables de los identificadores sobre metal. A priori debería ser un obstáculo, pero debido a la construcción interna de los identificadores específicos para el metal utilizados en esta prueba (utilizan el propio metal para amplificar aún más la señal), se consigue una fiabilidad superior.

También se puede concluir como el número de identificadores simultáneos leídos, o el entorno en el que se desarrollan las pruebas, no influyen significativamente en las detecciones.

2.2.- HF MiFare

El montaje para HF es mucho más sencillo, puesto que el corto alcance que tiene provoca que las influencias externas sobre el proceso de detección sean reducidas.

Se ha dispuesto un lector de sobremesa HF MiFare, con un alcance en condiciones normales de entre 5 y 10 cm.

Los tags HF varían en factor forma, puesto que cada vez es más habitual encontrarse con esta tecnología. La industria ha adaptado los chips a distintos tipos de etiquetas, como pueden ser tarjetas, pulseras, llaveros… En esta experimentación se tratará de comprobar si cada uno de los tipos usado en su entorno natural es fiable en cuento a detecciones o no.

A continuación se presenta el detalle de los distintos experimentos realizados en los que no se ha obtenido un 100% de lecturas. Para cada experimento se ha realizado 10 repeticiones.

Tipo	Tarjeta	**Ubicación**	Cartera
1	1	100,00%	0,00%
2	1	100,00%	0,00%
3	1	100,00%	0,00%
4	0	0,00%	100,00%
5	1	100,00%	0,00%
6	0	0,00%	100,00%
7	1	100,00%	0,00%
8	1	100,00%	0,00%
9	1	100,00%	0,00%
10	1	100,00%	0,00%
	Total	**80,00%**	**20,00%**

Figura 0-27: Detalle experimento MiFare (Tarjeta dentro de cartera)

Tipo	Pulsera	Ubicación	Junto a Reloj
1	1	100,00%	0,00%
2	1	100,00%	0,00%
3	0	0,00%	100,00%
4	1	100,00%	0,00%
5	1	100,00%	0,00%
6	1	100,00%	0,00%
7	0	0,00%	100,00%
8	1	100,00%	0,00%
9	0	0,00%	100,00%
10	1	100,00%	0,00%
	Total	**70,00%**	**30,00%**

Figura 0-28: Detalle experimento MiFare (Pulsera junto al reloj)

En la siguiente tabla se presenta un resumen de los experimentos realizados con los condicionantes del experimento.

Tipo	Ubicación	Leídos	No leídos
Tarjeta	Sin cartera	100,00%	0,00%
Tarjeta	Cartera	80,00%	20,00%
Pulsera	Junto a Reloj	70,00%	30,00%
Pulsera	Manga larga	100,00%	0,00%
Pulsera	Sudor	100,00%	0,00%
Llavero	Con llaves	100,00%	0,00%
Llavero	Sin llaves	100,00%	0,00%

Figura 0-29: Resumen experimento MiFare

Como se puede observar, salvo en dos supuestos, el resto de pruebas han resultado satisfactorias.

Las no lecturas dentro de la cartera puede deberse a que la tarjeta esté demasiado lejana del lector debido al propio grosor de la cartera. Este factor distancia puede ser definitivo también en caso de llevar dinero en monedas que pueda causar interferencias.

Con ubicar la tarjeta cerca de un lado exterior de la cartera sin nada de por medio debería ser suficiente para obtener la fiabilidad deseada.

Relativo a los identificadores de pulsera con reloj, se ha observado que en las 3 repeticiones que no se ha leído correctamente, el reloj de pulsera quedaba por encima del identificador, produciendo de esta forma un apantallamiento considerable con un elemento de metal.

Con evitar que el reloj cubra el identificador, ya sea no llevando, cambiando el identificador o el reloj de mano, o bien poniendo cuidado a la hora de efectuar la identificación, es suficiente para evitar estos problemas de no lectura.

3.- EXPERIMENTOS EN CONDICIONES REALES UHF

Una vez identificadas las condiciones más prometedoras para la tecnología UHF, se procede a realizar pruebas reales, con los identificadores ubicados sobre la persona como si fueran las condiciones normales de acceso a la zona.

Las pruebas se realizan en interiores ya que se ha comprobado que el factor entorno en este caso no debe ser tenido en cuenta.

A continuación se presenta el detalle de los distintos experimentos realizados en los que no se ha obtenido un 100% de lecturas. Para cada experimento se ha realizado 10 repeticiones.

Ancho	2	**Personas**	1
Tags/persona	5	**Total tags**	5

	Tags leídos	% Leídos	% No leídos
1	4	80,00%	20,00%
2	3	60,00%	40,00%
3	3	60,00%	40,00%
4	3	60,00%	40,00%
5	4	80,00%	20,00%
6	4	80,00%	20,00%
7	3	60,00%	40,00%
8	4	80,00%	20,00%
9	4	80,00%	20,00%
10	3	60,00%	40,00%
	Total	**70,00%**	**30,00%**

Figura 0-30: Detalle experimento 1 UHF

Ancho	2	**Personas**	2
Tags/persona	5	**Total tags**	10

	Tags leídos	% Leídos	% No leídos
1	6	60,00%	40,00%
2	7	70,00%	30,00%
3	8	80,00%	20,00%
4	7	70,00%	30,00%
5	7	70,00%	30,00%
6	6	60,00%	40,00%
7	6	60,00%	40,00%
8	6	60,00%	40,00%
9	7	70,00%	30,00%
10	7	70,00%	30,00%
	Total	**67,00%**	**33,00%**

Figura 0-31: Detalle experimento 2 UHF

Ancho	2	Personas	3
Tags/persona	5	Total tags	15
	Tags leídos	% Leídos	% No leídos
1	10	66,67%	33,33%
2	8	53,33%	46,67%
3	10	66,67%	33,33%
4	9	60,00%	40,00%
5	11	73,33%	26,67%
6	9	60,00%	40,00%
7	10	66,67%	33,33%
8	9	60,00%	40,00%
9	11	73,33%	26,67%
10	10	66,67%	33,33%
	Total	**64,67%**	**35,33%**

Figura 0-32: Detalle experimento 3 UHF

Ancho	2	Personas	4
Tags/persona	5	Total tags	20
	Tags leídos	% Leídos	% No leídos
1	12	60,00%	40,00%
2	13	65,00%	35,00%
3	12	60,00%	40,00%
4	12	60,00%	40,00%
5	12	60,00%	40,00%
6	13	65,00%	35,00%
7	11	55,00%	45,00%
8	12	60,00%	40,00%
9	14	70,00%	30,00%
10	14	70,00%	30,00%
	Total	**62,50%**	**37,50%**

Figura 0-33: Detalle experimento 4 UHF

Ancho	2	Personas	1
Tags/persona	10	Total tags	10
	Tags leídos	% Leídos	% No leídos
1	8	80,00%	20,00%
2	7	70,00%	30,00%
3	7	70,00%	30,00%
4	8	80,00%	20,00%
5	7	70,00%	30,00%
6	7	70,00%	30,00%
7	6	60,00%	40,00%
8	8	80,00%	20,00%
9	7	70,00%	30,00%
10	8	80,00%	20,00%
	Total	**73,00%**	**27,00%**

Figura 0-34: Detalle experimento 5 UHF

Ancho	2	Personas	2
Tags/persona	10	Total tags	20
	Tags leídos	% Leídos	% No leídos
1	14	70,00%	30,00%
2	15	75,00%	25,00%
3	14	70,00%	30,00%
4	13	65,00%	35,00%
5	15	75,00%	25,00%
6	14	70,00%	30,00%
7	14	70,00%	30,00%
8	13	65,00%	35,00%
9	15	75,00%	25,00%
10	14	70,00%	30,00%
	Total	**70,50%**	**29,50%**

Figura 0-35: Detalle experimento 6 UHF

Ancho	2	Personas	3
Tags/persona	10	Total tags	30
	Tags leídos	% Leídos	% No leídos
1	19	63,33%	36,67%
2	21	70,00%	30,00%
3	23	76,67%	23,33%
4	21	70,00%	30,00%
5	22	73,33%	26,67%
6	19	63,33%	36,67%
7	21	70,00%	30,00%
8	19	63,33%	36,67%
9	19	63,33%	36,67%
10	21	70,00%	30,00%
	Total	**68,33%**	**31,67%**

Figura 0-36: Detalle experimento 7 UHF

Ancho	2	Personas	4
Tags/persona	10	Total tags	40
	Tags leídos	% Leídos	% No leídos
1	27	67,50%	32,50%
2	25	62,50%	37,50%
3	27	67,50%	32,50%
4	27	67,50%	32,50%
5	24	60,00%	40,00%
6	26	65,00%	35,00%
7	26	65,00%	35,00%
8	25	62,50%	37,50%
9	25	62,50%	37,50%
10	27	67,50%	32,50%
	Total	**64,75%**	**35,25%**

Figura 0-37: Detalle experimento 8 UHF

Ancho	2	Personas	1
Tags/persona	15	Total tags	15
	Tags leídos	% Leídos	% No leídos
1	10	66,67%	33,33%
2	11	73,33%	26,67%
3	12	80,00%	20,00%
4	13	86,67%	13,33%
5	11	73,33%	26,67%
6	10	66,67%	33,33%
7	11	73,33%	26,67%
8	11	73,33%	26,67%
9	12	80,00%	20,00%
10	12	80,00%	20,00%
	Total	**75,33%**	**24,67%**

Figura 0-38: Detalle experimento 9 UHF

Ancho	2	Personas	2
Tags/persona	15	Total tags	30
	Tags leídos	% Leídos	% No leídos
1	20	66,67%	33,33%
2	22	73,33%	26,67%
3	21	70,00%	30,00%
4	22	73,33%	26,67%
5	22	73,33%	26,67%
6	22	73,33%	26,67%
7	21	70,00%	30,00%
8	23	76,67%	23,33%
9	22	73,33%	26,67%
10	20	66,67%	33,33%
	Total	**71,67%**	**28,33%**

Figura 0-39: Detalle experimento 10 UHF

Ancho	2	Personas	3
Tags/persona	15	Total tags	45
	Tags leídos	% Leídos	% No leídos
1	31	68,89%	31,11%
2	33	73,33%	26,67%
3	31	68,89%	31,11%
4	30	66,67%	33,33%
5	32	71,11%	28,89%
6	32	71,11%	28,89%
7	31	68,89%	31,11%
8	33	73,33%	26,67%
9	31	68,89%	31,11%
10	30	66,67%	33,33%
	Total	**69,78%**	**30,22%**

Figura 0-40: Detalle experimento 11 UHF

Ancho	2	Personas	4
Tags/persona	15	Total tags	60
	Tags leídos	% Leídos	% No leídos
1	38	63,33%	36,67%
2	44	73,33%	26,67%
3	39	65,00%	35,00%
4	38	63,33%	36,67%
5	42	70,00%	30,00%
6	37	61,67%	38,33%
7	45	75,00%	25,00%
8	41	68,33%	31,67%
9	32	53,33%	46,67%
10	38	63,33%	36,67%
	Total	**65,67%**	**34,33%**

Figura 0-41: Detalle experimento 12 UHF

Ancho	5	Personas	1
Tags/persona	5	Total tags	5
	Tags leídos	% Leídos	% No leídos
1	3	60,00%	40,00%
2	3	60,00%	40,00%
3	2	40,00%	60,00%
4	3	60,00%	40,00%
5	3	60,00%	40,00%
6	3	60,00%	40,00%
7	4	80,00%	20,00%
8	3	60,00%	40,00%
9	3	60,00%	40,00%
10	4	80,00%	20,00%
	Total	**62,00%**	**38,00%**

Figura 0-42: Detalle experimento 13 UHF

Ancho	5	Personas	2
Tags/persona	5	Total tags	10
	Tags leídos	% Leídos	% No leídos
1	6	60,00%	40,00%
2	6	60,00%	40,00%
3	5	50,00%	50,00%
4	6	60,00%	40,00%
5	6	60,00%	40,00%
6	7	70,00%	30,00%
7	6	60,00%	40,00%
8	7	70,00%	30,00%
9	6	60,00%	40,00%
10	5	50,00%	50,00%
	Total	**60,00%**	**40,00%**

Figura 0-43: Detalle experimento 14 UHF

Ancho	5	Personas	3
Tags/persona	5	Total tags	15

	Tags leídos	% Leídos	% No leídos
1	7	46,67%	53,33%
2	8	53,33%	46,67%
3	8	53,33%	46,67%
4	9	60,00%	40,00%
5	8	53,33%	46,67%
6	10	66,67%	33,33%
7	8	53,33%	46,67%
8	7	46,67%	53,33%
9	10	66,67%	33,33%
10	11	73,33%	26,67%
	Total	**57,33%**	**42,67%**

Figura 0-44: Detalle experimento 15 UHF

Ancho	5	Personas	4
Tags/persona	5	Total tags	20

	Tags leídos	% Leídos	% No leídos
1	10	50,00%	50,00%
2	11	55,00%	45,00%
3	12	60,00%	40,00%
4	11	55,00%	45,00%
5	10	50,00%	50,00%
6	12	60,00%	40,00%
7	11	55,00%	45,00%
8	11	55,00%	45,00%
9	10	50,00%	50,00%
10	11	55,00%	45,00%
	Total	**54,50%**	**45,50%**

Figura 0-45: Detalle experimento 16 UHF

Ancho	5	Personas	1
Tags/persona	10	Total tags	10

	Tags leídos	% Leídos	% No leídos
1	7	70,00%	30,00%
2	8	80,00%	20,00%
3	5	50,00%	50,00%
4	5	50,00%	50,00%
5	6	60,00%	40,00%
6	8	80,00%	20,00%
7	7	70,00%	30,00%
8	8	80,00%	20,00%
9	6	60,00%	40,00%
10	6	60,00%	40,00%
	Total	**66,00%**	**34,00%**

Figura 0-46: Detalle experimento 17 UHF

Ancho	5	Personas	2
Tags/persona	10	Total tags	20
	Tags leídos	% Leídos	% No leídos
1	13	65,00%	35,00%
2	12	60,00%	40,00%
3	13	65,00%	35,00%
4	12	60,00%	40,00%
5	11	55,00%	45,00%
6	14	70,00%	30,00%
7	13	65,00%	35,00%
8	15	75,00%	25,00%
9	11	55,00%	45,00%
10	13	65,00%	35,00%
	Total	**63,50%**	**36,50%**

Figura 0-47: Detalle experimento 18 UHF

Ancho	5	Personas	3
Tags/persona	10	Total tags	30
	Tags leídos	% Leídos	% No leídos
1	19	63,33%	36,67%
2	18	60,00%	40,00%
3	18	60,00%	40,00%
4	17	56,67%	43,33%
5	19	63,33%	36,67%
6	20	66,67%	33,33%
7	18	60,00%	40,00%
8	19	63,33%	36,67%
9	18	60,00%	40,00%
10	19	63,33%	36,67%
	Total	**61,67%**	**38,33%**

Figura 0-48: Detalle experimento 19 UHF

Ancho	5	Personas	4
Tags/persona	10	Total tags	40
	Tags leídos	% Leídos	% No leídos
1	26	65,00%	35,00%
2	22	55,00%	45,00%
3	27	67,50%	32,50%
4	26	65,00%	35,00%
5	25	62,50%	37,50%
6	22	55,00%	45,00%
7	20	50,00%	50,00%
8	26	65,00%	35,00%
9	24	60,00%	40,00%
10	21	52,50%	47,50%
	Total	**59,75%**	**40,25%**

Figura 0-49: Detalle experimento 20 UHF

Ancho	5	Personas	1
Tags/persona	15	Total tags	15

	Tags leídos	% Leídos	% No leídos
1	11	73,33%	26,67%
2	11	73,33%	26,67%
3	10	66,67%	33,33%
4	12	80,00%	20,00%
5	10	66,67%	33,33%
6	10	66,67%	33,33%
7	11	73,33%	26,67%
8	10	66,67%	33,33%
9	10	66,67%	33,33%
10	11	73,33%	26,67%
	Total	**70,67%**	**29,33%**

Figura 0-50: Detalle experimento 21 UHF

Ancho	5	Personas	2
Tags/persona	15	Total tags	30

	Tags leídos	% Leídos	% No leídos
1	20	66,67%	33,33%
2	23	76,67%	23,33%
3	21	70,00%	30,00%
4	22	73,33%	26,67%
5	18	60,00%	40,00%
6	21	70,00%	30,00%
7	19	63,33%	36,67%
8	20	66,67%	33,33%
9	22	73,33%	26,67%
10	20	66,67%	33,33%
	Total	**68,67%**	**31,33%**

Figura 0-51: Detalle experimento 22 UHF

Ancho	5	Personas	3
Tags/persona	15	Total tags	45

	Tags leídos	% Leídos	% No leídos
1	32	71,11%	28,89%
2	25	55,56%	44,44%
3	31	68,89%	31,11%
4	27	60,00%	40,00%
5	29	64,44%	35,56%
6	26	57,78%	42,22%
7	32	71,11%	28,89%
8	34	75,56%	24,44%
9	26	57,78%	42,22%
10	30	66,67%	33,33%
	Total	**64,89%**	**35,11%**

Figura 0-52: Detalle experimento 23 UHF

Ancho	5	Personas	4
Tags/persona	15	Total tags	60

	Tags leídos	% Leídos	% No leídos
1	39	65,00%	35,00%
2	33	55,00%	45,00%
3	38	63,33%	36,67%
4	39	65,00%	35,00%
5	36	60,00%	40,00%
6	38	63,33%	36,67%
7	32	53,33%	46,67%
8	39	65,00%	35,00%
9	36	60,00%	40,00%
10	37	61,67%	38,33%
	Total	**61,17%**	**38,83%**

Figura 0-53: Detalle experimento 24 UHF

En la siguiente tabla se presenta un resumen de los experimentos realizados con los condicionantes del experimento.

Ancho	Tags/persona	Personas	Leídos	No leídos
2	5	1	70,00%	30,00%
2	5	2	67,00%	33,00%
2	5	3	64,67%	35,33%
2	5	4	62,50%	37,50%
2	10	1	73,00%	27,00%
2	10	2	70,50%	29,50%
2	10	3	68,33%	31,67%
2	10	4	64,75%	35,25%
2	15	1	75,33%	24,67%
2	15	2	71,67%	28,33%
2	15	3	69,78%	30,22%
2	15	4	65,67%	34,33%
5	5	1	62,00%	38,00%
5	5	2	60,00%	40,00%
5	5	3	57,33%	42,67%
5	5	4	54,50%	45,50%
5	10	1	66,00%	34,00%
5	10	2	63,50%	36,50%
5	10	3	61,67%	38,33%
5	10	4	59,75%	40,25%
5	15	1	70,67%	29,33%
5	15	2	68,67%	31,33%
5	15	3	64,89%	35,11%
5	15	4	61,17%	38,83%

Figura 0-54: Resumen experimento UHF real 1

Como se puede observar, los resultados han sido considerablemente peores que los obtenidos en el experimento previo, a pesar de haberse realizado con las variables verificadas previamente.

Se observan varias tendencias en los resultados que pueden ayudar a concluir las razones de estos porcentajes tan bajos.

Por una parte, se observa que el porcentaje de lecturas decrece a medida que hay más personas. La primera razón obvia ante este caso es el apantallamiento de los identificadores por parte de las personas que pueden ir en grupo. Al situarse un cuerpo humano (que recordemos es en un alto porcentaje agua) entre un identificador y la antena receptora, absorbe toda la energía y la lectura no es completada.

Por otra parte, cuantos más identificadores se colocan en cada individuo, mayor porcentaje de lecturas se realizan. La causa de esta situación surge de la ubicación de los identificadores, que se fueron disponiendo en mayor medida en la parte del superior del individuo. Las causas resultan ser dos: apantallamiento dentro del propio individuo (brazos, piernas, cabeza… que se interponen entre la antena y el identificador), y la orientación de los identificadores, ya que la comunicación física entre las antenas y el identificador es altamente dependiente de la orientación del identificador respecto de la antena.

Conocidos los problemas de apantallamiento y orientación, se ha intentado evitar en la medida de lo posible disposiciones perjudiciales de los identificadores para el correcto funcionamiento de las detecciones.

Los identificadores se han dispuesto por el cuerpo teniendo en cuenta estos apantallamientos y la orientación, y se han repetido de nuevo las mismas pruebas. A continuación, se presenta la tabla resumen de la repetición del experimento.

	Tags/persona	Personas	Leídos	No leídos
2	5	1	98,00%	2,00%
2	5	2	97,00%	3,00%
2	5	3	97,33%	2,67%
2	5	4	96,50%	3,50%
2	10	1	99,00%	1,00%
2	10	2	99,00%	1,00%
2	10	3	98,67%	1,33%
2	10	4	98,75%	1,25%
2	15	1	99,33%	0,67%
2	15	2	99,00%	1,00%
2	15	3	97,78%	2,22%
2	15	4	96,17%	3,83%
5	5	1	98,00%	2,00%
5	5	2	97,00%	3,00%
5	5	3	96,67%	3,33%
5	5	4	96,00%	4,00%
5	10	1	99,00%	1,00%
5	10	2	98,50%	1,50%
5	10	3	99,00%	1,00%
5	10	4	98,50%	1,50%
5	15	1	98,67%	1,33%
5	15	2	99,00%	1,00%
5	15	3	97,56%	2,44%
5	15	4	96,67%	3,33%

Figura 0-55: Resumen experimento UHF real 2

Las diferencias con respecto al anterior son abismales, puesto que en ningún momento ha bajado del 96% de lecturas positivas.

Se siguen produciendo apantallamientos individuales debido a las partes móviles del individuo al pasar en movimiento, como por ejemplo un brazo que cruza por encima de un identificador, pero son puntuales.

También se siguen produciendo apantallamientos de identificadores más pronunciados cuando pasa bajo el pórtico un grupo de personas.

4.- CONCLUSIONES FINALES

A tenor de los resultados de la experimentación, se puede afirmar que es viable aplicar la auto-identificación con RFID a la prevención de riesgos laborales siempre y cuando se tengan en cuenta una serie de restricciones.

En relación a la tecnología UHF, es más eficiente en cuanto a productividad, en el sentido que es capaz de tratar un alto número de elementos por segundo, estando supeditado al coste elevado en equipos.

El primero de los factores a tener en cuenta en UHF es el material que se pretende identificar. Se debe tener especial cuidado con los metales, puesto que los identificadores normales no se pueden leer sobre metal, es necesario utilizar identificadores especiales. Por el contrario el coste es elevado en comparación con los normales, así que deben usarse en casos absolutamente indispensables.

Pero sobre todo, los dos factores más determinantes son la orientación de los identificadores y el apantallamiento. Los resultados de la experimentación no dejan lugar a dudas acerca de la importancia capital de estos dos aspectos. Y es aquí donde radican las principales reservas a la hora de implantar definitivamente el sistema.

Debido a estas limitaciones, no sería admisible la detección de la presencia o ausencia para evitar directamente un accidente laboral, como por ejemplo, detener el funcionamiento de una máquina, ya que como se ha visto, las detecciones son sensibles a los apantallamientos.

Tampoco sería recomendable utilizarlo en acceso a zonas sin barreras físicas, puesto que se dependería de la buena voluntad del individuo que reaccionase ante un acceso denegado (por ejemplo, ante una luz roja o un zumbador).

Sin embargo, para permitir o denegar el paso en sistemas con barrera física, la auto-identificación es perfectamente viable, puesto que si no detecta alguno de los identificadores, siempre se puede intentar volver visibles aquéllos que estén apantallados o reorientar los que no estén bien orientados, así como reintentar el paso en caso de denegación del mismo. Así, mientras no se autorice el paso, no se puede realizar el acceso a la zona.

Esto podría introducir algunos problemas de aglomeraciones en las entradas, si bien el alto porcentaje de detecciones indica que son casos aislados y fácilmente recuperables.

Precisamente por este problema de las aglomeraciones, no se recomienda utilizar HF para identificar números elevados de EPIs, ya que el individuo que quisiera

realizar el acceso a la zona, debería identificar los mismos uno a uno con la consiguiente acumulación de tiempo en el dispositivo.

Sin embargo, HF es conveniente cuando, o bien no se requiere identificar un número elevado de elementos por persona (2 o 3 elementos), o bien cuando las posibles aglomeraciones en el acceso no pueden tener lugar por el bajo número de usuarios (o son admisibles) y es fácil aproximar los EPIs identificados al lector. Debido a su alta fiabilidad y bajo coste podría ser la mejor opción en estos casos.

Aún dependiendo de las necesidades de cada implantación, generalmente una solución mixta resulta mejor en un compromiso eficiencia/coste razonable, por lo que un estudio pormenorizado de la situación requerida en la implantación se antoja indispensable para maximizar dicha relación eficiencia/coste.