INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN
DEPARTAMENTO DE INFORMÁTICA
PROYECTO FIN DE CARRERA

CONTROL DE LOS ENTORNOS DE SISTEMAS RFID

Autor: Carlos Cobos Moreno
Tutor: Miguel Ángel Ramos González
Leganés, Octubre de 2013

Autor: Carlos Cobos Moreno
Tutor: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente:_____
Vocal:_____
Secretario:_____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

"La tecnología RFID será el asunto más importante desde que Edison nos dio la bombilla incandescente"

Rick Duris

AGRADECIMIENTOS

Si solo tuviera la posibilidad de incluir dos nombres en este apartado, esos serían Sebas y Agustín, mis padres, no hay palabras suficientes para agradecer, ni hay medida para explicar todo el cariño y apoyo recibido por su parte. A mi hermana Beatriz y a su inmenso corazón, aunque físicamente lejos, en lo importante siempre está muy cerca. A mi hermano Jose Antonio, por ser siempre un ejemplo de creatividad, alegría y superación. Y como no, sobre todo a los pequeños Marcos, Emma, Victoria, Claudia y Lola.

Por supuesto a Jaime, Alvaro y Javi, por hacer de mi paso por la universidad una etapa inolvidable, y por ofrecerme su verdadera amistad. No puedo olvidarme del mejor equipo de fútbol que ha pasado por esta universidad el "Gallego´sTeam" y todos sus integrantes.

Gracias a Miguel Angel mi tutor, por su total disponibilidad en todo momento, su paciencia, esfuerzo y todo lo que me ha permitido aprender de él en sus asignaturas y especialmente en este proyecto.

Luis Morales, gracias por compartir dos de las cosas más valiosas que alguien tiene, su tiempo y sus conocimientos, me considero afortunado por ello.

Gracias a Shihan Jesus Talán, porque aunque pase el tiempo, hay enseñanzas que no se olvidan.

RESUMEN

Hoy en día todos somos conscientes de la rápida y constante evolución de los sistemas de comunicación en nuestra sociedad, hemos visto por ejemplo como en apenas dos décadas la tecnología relacionada con la telefonía móvil ha evolucionado y lo sigue haciendo año a año.

En el campo de los sistemas de identificación y comunicación podemos incluir RFID, una tecnología que está llamada a crecer considerablemente en los próximos años. Las razones por las que es fácilmente predecible que será una opción importante a tener en cuenta por parte de la industria, es su amplio abanico de aplicaciones, y las características que ofrece. De estas características la que supone una diferenciación sobre las demás es su aparente invisibilidad, eficiencia y rapidez en los procesos de identificación, gracias a la utilización de ondas de radio y un software que da soporte a este tipo de comunicación. Sin embargo por la misma razón, en ocasiones es percibido como un potencial riesgo de cara al usuario y algunos sectores de la industria.

En el presente proyecto se realiza un profundo análisis de estos sistemas de identificación, poniendo especial atención en los riesgos y amenazas potenciales sobre la seguridad y la privacidad de los usuarios. Se hará un estudio de las metodologías más importantes en torno a estos sistemas de identificación y los marcos legales y normativos prestando especial atención a los vigentes en la Unión Europea y específicamente en España.

El objetivo es hacer un análisis profundo sobre la seguridad y la privacidad de esta tecnología y proporcionar un medio de evaluación de cara a los posibles riesgos que potencialmente pueden afectar a un sistema RFID.

ABSTRACT

Today we are all aware of the rapid and constant evolution of communication systems in our society, we have seen in just two decades the technology related to mobile telephony has evolved and continues to do so every year.

In the field of identification and communication systems can include RFID, a technology that is destined to grow substantially in the coming years. The reasons why it is easy to predict that it will be an important option to be considered by the industry, is its wide range of applications, and the features it offers. From these characteristics it represents a differentiation on the other is its apparent invisibility, efficiency and speed in the processes of identification, through the use of radio waves and software that supports this type of communication. But for the same reason, it is sometimes perceived as a potential risk to the user and some sectors of the industry.

In the present project is a thorough analysis of these identification systems, paying special attention to the risks and potential threats to security and user privacy. There will be a study of the most important methodologies around these identification systems and legal and regulatory frameworks with particular attention to those in force in the European Union and specifically in Spain.

The goal is to make a deep analysis on the safety and privacy of this technology and provide a means of assessment concerning potential risks that can potentially affect an RFID system.

CONTENIDO

TABLA DE ILUSTRACIONES

CAPÍTULO 1. INTRODUCCIÓN Y OBJETIVOS

Ya en la Segunda Guerra Mundial se utilizaban para diferenciar ante un posible ataque a los aviones amigos y enemigos, desde entonces los sistemas de Identificación por Radio Frecuencia (RFID) han sufrido un progresivo avance hasta nuestros días. Es sobre todo en las dos últimas décadas cuando el mercado se fijó en esta tecnología por su gran potencial, mezclando interesantes atributos para la actividad empresarial, unido a la gran variedad de aplicaciones que puede aceptar, y que hoy por hoy todavía no se han llevado a cabo.

Esta tecnología cubre todo tipo de campos, y su atractivo se centra en la variable capacidad de datos que puede manejar, la posibilidad de interconexión con otras tecnologías, y la enorme mejora que supone respecto a otros sistemas de identificación, además de ofrecer la posibilidad de poder monitorizar a distancia y simultáneamente el número que se desee de estos dispositivos.

Son muchos los puntos fuertes como vemos a favor de los sistemas RFID, pero una de mis funciones en este proyecto será centrarme en los posibles vacíos, vulnerabilidades, flaquezas y riesgos que presentan, sobre todo respecto a la seguridad propia de estos sistemas, y lo que supone directa e indirectamente para el usuario, existiendo en muchas ocasiones un riesgo real o potencial para su privacidad. Todos estos temas son vistos y estudiados desde el punto de vista técnico informático, ya que esta tecnología asienta sus bases aparte de en la radio frecuencia, en un software, y una infraestructura informática que permite todo el proceso.

El interés que han suscitado estos sistemas, sacando a la luz en ocasiones polémicas noticias sobre riesgos, o curiosas aplicaciones como por ejemplo sofisticados sistemas anti robos en neumáticos la hacen de alguna forma estar en el punto de mira de los más escépticos. En ocasiones esta tecnología ha sido injustamente tratada y objeto de falsas noticias de gran impacto, como el polémico chip sanitario que se implantaría en Estados Unidos, sin ninguna base oficial ni legal del propio gobierno. Todo ello despertó mi curiosidad, y me llevó a intentar analizarlo desde el punto de vista técnico, y a adentrarme en profundidad en estos sistemas y sus aplicaciones.

El objetivo general de este proyecto, es dar a conocer de forma clara, tanto el funcionamiento, y los tipos de sistemas más utilizados, así como sus estándares. En otra parte se explicarán las principales aplicaciones y futuros proyectos, y sobre las principales prácticas que se llevan hoy en día y teniendo en cuenta las

características técnicas de los sistemas, hacer un análisis de los riesgos sobre todo relacionados con la seguridad y privacidad del usuario, atendiendo a las normativas y metodologías más importantes, especialmente a las que afectan a la Unión Europea, específicamente en España.

CAPÍTULO 2. SISTEMAS RFID

2.1 HISTORIA, ANTECEDENTES Y FUNDAMENTOS DE RFID

2.2 HISTORIA DE LOS SISTEMAS RFID

Al contrario de lo que se pueda pensar, a pesar de ser una tecnología más o menos "reciente", no tiene un origen ni descubridor claro. Sí se puede decir que ha surgido por la combinación y avance de otros campos de la tecnología. En décadas estos sistemas han pasado de ser objeto de algunos artículos de revista a formar parte de nuestras vidas.

Algunos consideran padre de los dispositivos RFID a Leon Theremin que al final de la Segunda Guerra Mundial, se dice que inventó el primer dispositivo como forma de espionaje en 1945. Pero no es cierto que el dispositivo inventado por Theremin sea un dispositivo RFID, ya que el sistema era de escucha encapsulado pasivo, solo era capaz de percibir sonido, y no tenía parte activa tal como entendemos en un sistema de estas características.

Lo que si es cierto es que esta tecnología está directamente relacionada con la Segunda Guerra Mundial como antes se comenta. Hay constancia que desde 1939 el ejército británico ideó un sistema de emisión y recepción de señales de radio para distinguir sus aviones de los enemigos. Para ello colocaron antenas en los aviones que respondían a una señal emitida a una distancia de hasta 40 kilómetros.

La idea era detectar las naves propias, que respondían a la señal de las enemigas de las cuales no se obtenía ninguna respuesta. A este sistema se le dio en sus inicios el nombre de IFF (Identify Friend or Foe, identificación amigo o enemigo), en el que está basado el sistema actual de control de aviación comercial y privada. Es la primera referencia clara que se tiene del uso de RFID.

Uno de los antiguos sistemas de los que hemos hablado anteriormente IFF:

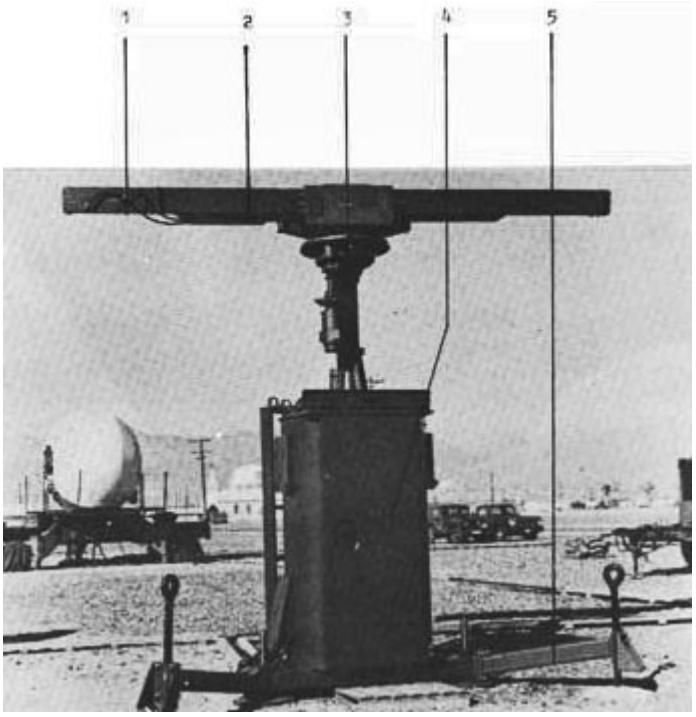


Ilustración 1: Sistema IFF.

1. Control por radio
2. Antena
3. Unidad conducción

4. Procesador datos
5. Outtrigger

En los años 50 los sistemas de radio y radar siguieron desarrollándose y con ellos el RFID. Los sistemas de radiofrecuencia implicados en transmisiones de largo alcance tuvieron un fuerte impulso en su desarrollo. Hubo trabajos que influyeron directamente en el avance, estos son "Application of microwave homodyne "(F.L. Vernon) y "Radio transmission systems with modulatable passive responder" (D.B Harris).

La década de los 60 fue la época de consolidación de los sistemas de identificación por radiofrecuencia. Su uso en supermercados como sistema de seguridad antirrobos supuso su consolidación. El sistema constaba con un único bit de información, lo único que se lograba saber es si la etiqueta era detectada o no dentro del radio de acción del lector. En caso de ser detectada, se activaba una alarma, ya que los lectores se colocaban a los lados de los clientes que abandonaban el establecimiento. A pesar de su sencillez resultó un sistema económico y efectivo, lo que supuso su expansión.

En el siguiente decenio, 1970-1980 se vieron implicadas varias instituciones como Los Alamos Scientific Laboratory, o el sueco Microwave Institute Foundation. En los sucesivos años se probaron sistemas en el sector transportes dedicados al rastreo de automóviles como el utilizado en el puerto de New York y New Jersey. Por aquellos años no llegó a entrar en el mercado del campo logístico, ya que no estaba tan consolidada su aplicación. El desarrollo técnico se disparó y el número de empresas dedicadas a la tecnología RFID creció notablemente, las aplicaciones más destacables y explotada en la década fue la usada en el seguimiento de ganado, vehículos y automatización industrial) todos ellos sistemas basados en microondas y sistemas inductivos en Europa.

Los años 80 fue la época en que fructificaron todos los estudios realizados anteriormente. Por un lado en Estados Unidos el desarrollo fue por el campo del transporte, accesos y como antes mencionamos en ganado, por parte de Europa el interés fue sobre todo en el campo industrial y en el control de animales a corto alcance.

A partir de 1990 en EEUU el uso sobre todo fue utilizado en el control electrónico para el pago de peaje en autopistas, ejemplos son los de Oklahoma y Houston. En Europa el uso fue de sistemas de microondas e inductivos para control de accesos y billetes electrónicos.

Y esto fue el principio de lo que después se fue extendiendo a otros campos y países:

-Texas Instruments desarrolla un sistema de encendido de automóvil.

-Philips crea un sistema de encendido, control de combustible, y control de acceso al vehículo.

-Los billetes electrónicos y accesos a autopistas se extienden por todo el mundo (África, Australia, Asia).

-En Dallas se desarrolla un solo tag para acceder al campus universitario, garajes municipales, y autopista.

El éxito en estos años es debido al desarrollo de equipos con más memoria, más pequeños, con más alcance y costes más baratos. Todo ello permitió su introducción en nuevos segmentos económicos.

2.3 QUE SON LOS SISTEMAS RFID

Después de hacer un repaso a la historia que permitió el desarrollo de esta tecnología, pasamos a hacer una explicación básica y clara sobre lo que es un sistema RFID.

La tecnología de identificación por radio frecuencia (RFID) permite que un objeto sea identificado automáticamente mediante una onda emisora que va incorporada en el propio objeto y que transmite los datos que lo identifican por radiofrecuencia. En la mayor parte de los casos la identificación es unívoca.

Como está documentado en el capítulo anterior, el primer uso claro del que se tiene constancia fue en la Segunda Guerra Mundial, para diferenciar a los aviones amigos de los enemigos. Más tarde se fue extendiendo hacia ramas cada vez más comerciales como ocurrió en la década de los 70 en EEUU cuando varias empresas importantes del sector.

Esta transformación ha tenido como consecuencia la tecnología RFID que conocemos hoy en día, y que engloba a los sistemas que tienen como característica general, identificar objetos mediante ondas de radio.

Lo que hace a esta tecnología tan útil es su posibilidad de auto-identificación, gracias a que el objeto a identificar tiene una emisora de radio. Todo ello unido al nivel de desarrollo actual, los costes más abaratados, y la evolución de las emisoras que cada vez van siendo más pequeñas, hasta el punto en el que nos

encontramos actualmente en que pueden ser adheridas al objeto a identificar en forma de adhesivo. Esto facilita la identificación de casi cualquier objeto.

Estos transpondedores o microemisoras , (que también llamaremos tags o etiquetas) son las que permiten que el objeto sea identificado a una distancia variable. Hay varios parámetros que condicionan aspectos como son la distancia de recepción, velocidad de transmisión, capacidad de información emitida y fiabilidad que depende directamente de la etiqueta y sus características como es la antena, la frecuencia de emisión, o el tipo de chip usado.

2.4 FUNCIONAMIENTO

Los pasos básicos que sigue el funcionamiento de la tecnología RFID son los siguientes:

1. Grabado en la etiqueta de información y datos identificativos del objeto al que va adherida.
2. Emisión de señal de radio generada por la etiqueta (difiere la forma en que lo hace dependiendo del tipo de etiqueta).
3. Un lector físico recibe la señal y la transforma en datos y transmite la información a la aplicación que se encarga de gestionar el RFID (también llamada middleware).

Más a fondo podemos explicarlo diciendo que los lectores RFID controlan la escritura y lectura de datos e información que está almacenada en un tag (etiqueta) generando en algunos casos de forma "autónoma" (nos referimos a la ausencia de cables u otras fuentes externas) un campo de radiofrecuencia en torno a la antena, y proporcionando energía al tag en caso de ser pasiva. Además el campo es también un medio de transferencia de datos de la etiqueta al lector.

El campo de radiofrecuencia del lector es modulado por el tag. Así el lector puede detectarlo. El lector se enciende y apaga siguiendo una secuencia que es captada por el tag registrándola a la vez en su memoria de una forma muy parecida a la que se graba una secuencia de unos y ceros en un medio magnético. Por último el lector recibe y envía a una aplicación la información que contiene el tag, en la que se encuentran las características del producto y es procesado según esté definido en cada aplicación.

Las cualidades que caracterizan al sistema RFID es su mayor capacidad de almacenamiento de datos junto a la alta velocidad de identificación y una recepción de datos exacta e inmediata.

2.4.1 ETIQUETA, TAG O TRANSPONDER.

En primer lugar explicar de dónde procede el término transponder ya que es bastante esclarecedor y resume bastante bien la propia función de la etiqueta:

El término transponder deriva de las dos palabras inglesas TRANSmitter/resPONDER, es decir una etiqueta es a la vez transmisor y de alguna manera contestador o respondedor.

Las partes básicas de un tag, son las siguientes:

- Memoria no volátil donde almacenar datos, generalmente suele ser una EEPROM.
- Memoria ROM, en ella se almacenan las instrucciones básicas como temporizadores o controladores de flujo de datos.
- Opcionalmente algunas incluyen memorias RAM donde se almacenan datos referentes a la comunicación con el lector.
- Una parte esencial es la antena que detecta el campo que ha sido diseñado previamente por el desarrollador de la aplicación, y del que extrae la energía necesaria para su comunicación con dicho campo.
- Componentes electrónicos para procesar la señal de la antena y para el proceso de datos, como filtros, buffers y otros.
- Información para ser utilizada en modo lectura, o modo lectura/escritura.

La memoria incluida en las etiquetas, en su mayoría una EEPROM (Electrically erasable programable read-only memory), memoria solo permite modo lectura, es programable y se puede borrar electrónicamente. En ocasiones los datos vienen grabados de fábrica y otras veces existe la posibilidad de incluir datos relevantes para el usuario.

2.4.1.1 CLASIFICACIÓN ETIQUETAS SEGÚN FUENTE DE ALIMENTACIÓN

La energía utilizada por los tags es medida en microvatios Mw. Para hacernos una idea de la magnitud de esta medida, un microvatio es igual a una millonésima de vatio (10^-6). Este tipo de medida es también utilizada en instrumentación médica, instrumentos científicos y en receptores de radio y radar. También los dispositivos incluidos en calculadoras solares y relojes son medidos con Mw.

Los tags se dividen en dos grandes grupos dependiendo de la fuente de la que obtienen la energía:

- **ACTIVOS:** algunos dispositivos necesitan más energía que no puede obtenerse a partir del campo magnético generado por el lector, por lo que incluyen unas baterías adicionales. Como consecuencia estas etiquetas tienen un alcance mayor, necesariamente no necesitan que el lector inicie la comunicación. El coste se ve aumentado hasta en 5 veces más que las etiquetas pasivas y su vida útil es limitada. Los dispositivos que funcionan con ultra alta frecuencia (UHF) pueden ser activos o pasivos, mientras que los que funcionan en baja frecuencia y alta frecuencia son pasivos (LF y HF).Ejemplo de estos dispositivos son algunos de los utilizados en el seguimiento de ganado, donde las etiquetas son adheridas a la oreja del animal, o estómago.

Ilustración 2: Animales y RFID

- **PASIVOS:** estos dispositivos se alimentan de la energía del campo energético generado por el lector, no tienen capacidad autónoma para crear una señal de salida. El circuito integrado es alimentado por la señal de frecuencia emitida por el lector y emitir así una respuesta aprovechando la energía entrante.

  Los tamaños de estos dispositivos pueden variar desde los 0.15 mm al tamaño de una tarjeta postal, dependiendo en gran medida del tamaño de la antena.

  Su periodo de vida es "ilimitado" pudiendo ser reactivadas con el paso de los años.

  Las frecuencias en las que trabajan se encuentran entre la baja frecuencia (LF) y alta frecuencia (HF), los dispositivos que funcionan en ultra alta frecuencia (UHF) pueden ser tanto activos como pasivos.

Ilustración 3: Etiqueta RFID

COMPARACIÓN ENTRE LOS DOS MODELOS

- El nivel de intensidad de la señal que se necesita para una etiqueta activa y una pasiva es completamente distinto. Las etiquetas activas necesitan señales de muy baja potencia ya que generan de forma autónoma su respuesta mientras que las pasivas necesitan una potencia por parte del lector señales del orden de 1000 veces más alta que las activas. Por tanto si tenemos un sistema integrado con etiquetas pasivas necesitaremos lectores con capacidad de crear señales potentes.
- Las etiquetas pasivas son incapaces de iniciar una comunicación, al contrario de las activas, esto supone una gran diferencia, ya que las etiquetas activas pueden ser programadas para enviar datos en momentos determinados por ejemplo dependiendo de ciertas modificaciones externas sin esperar una señal del lector.
- La distancia entre lector y etiqueta es mucho menor en las etiquetas pasivas siendo la distancia máxima unos pocos metros, mientras que las activas pueden entablar comunicación con un lector a cientos de metros. Los factores de la distancia dependen en gran medida de la potencia del lector y el tamaño de la antena.
- Las etiquetas activas permiten abrir un campo de aplicación por ejemplo en proyectos que requieran hacer un seguimiento de factores ambientales, en los que se desee tener constancias de cambios puntuales sobre una variación externa, por ejemplo cambios de temperatura. La razón es la autonomía energética de la etiqueta activa para generar una señal, con una pasiva también se podría implementar pero teniendo un sistema en el que el lector periódicamente entablara comunicación con la etiqueta para recibir posibles datos nuevos.
- La tecnología RFID permite que las etiquetas almacenen datos e información enviada por el lector, sin embargo, las etiquetas pasivas no suelen disponer de muchas funciones de procesamiento debido a la limitación energética. Además generalmente este modelo de etiquetas no

suelen contar con un extenso espacio de memoria. Esta diferencia afecta al tratamiento de errores de transmisión, ya que las etiquetas activas al contar con mayor capacidad de procesamiento pueden incluir protocolos más complejos de seguridad.

CONCLUSIÓN

Las prestaciones ofrecidas por las etiquetas activas son mucho más amplias que las ofrecidas por los dispositivos pasivos. La autonomía energética, la distancia de lectura, y su mayor capacidad de procesamiento la harán una mejor elección en casos en que se necesiten datos de los que se desconozca su frecuencia de modificación y sean captados por la propia etiqueta, además de procesos de lectura a mayor distancia. Dependiendo de la estructura y el fin de nuestro sistema completo, unas etiquetas cumplirán mejor con los objetivos de nuestra aplicación final. Las etiquetas pasivas aunque menos potentes y de menor capacidad de memoria, suponen una solución muy eficiente para el almacenamiento de objetos, realización de inventarios e identificación, todos los casos en que solo se necesite la identificación y la comunicación de datos estáticos.

2.4.1.2 CLASIFICACIÓN DE TAGS SEGÚN LA FRECUENCIA Y VELOCIDAD DE TRANSMISIÓN

Ya hemos clasificado las etiquetas según su fuente de alimentación. A continuación se hará teniendo en cuenta la frecuencia en la que pueden ser leídos los distintos tipos de tags.

Pero antes de pasar a ver los distintos tipos, es importante comentar la relación que existe entre las altas y bajas frecuencias, velocidad de operación, e impacto económico. A mayor frecuencia, más velocidad de transferencia de datos (lectura), y por tanto más sofisticación y aumento de coste en las etiquetas.

Más adelante hablaremos ampliamente de la IEC (International Electrotechnical Comission). Es importante mencionar esta entidad porque es la que regula el proceso denominado normalización de radiofrecuencia, es decir el establecimiento de unas normas generales en todo el mundo sobre la asignación de frecuencias y otras funciones en general.

Hay que tener en cuenta cuando se asignan rangos de frecuencia para no interferir en cualquier otra operación de transmisión, tales como otros sistemas parecidos, u otros tan usados como la televisión, radio, e incluso podemos hablar de riesgo en de interferencia en transmisiones de seguridad nacional como la policía, o en el mundo de la industria.

El hecho de que cada vez se amplíe más la normalización en el uso de otros servicios que incluyen la radio en su uso, hace disminuir las disponibles para RFID.

Estos son los distintos tipos de tags según el rango en que pueden ser leídos:

- **LF (low frequency):** se considera baja frecuencia al rango que se encuentra entre 120 KHz – 134 KHz. El uso más extendido entre este tipo de etiquetas es para acceso a emplazamientos como edificios.

- **HF (High Frequency):** el rango establecido como alta frecuencia se sitúa en los 13.56 MHz. Este rango es muy usado en funciones relacionadas con el sector médico e industrial, así como en la rama científica en general, conocida en inglés como ISM (Industrial – Scientific – Medical). Una de sus características es que las etiquetas que operan en esta frecuencia son planas de unos 100mm generalmente como máximo.

    - **Ventajas:** no presentan problemas en la comunicación en presencia de agua, en general se caracterizan por su facilidad para ser leídas.
    - **Desventajas:** el alcance de lectura es muy limitado, estamos hablando de unos 35 centímetros aproximadamente.

- **UHF (Ultra High Frequency):** Su rango se encuentra entre los 868 MHz – 956 MHz. Este rango es conocido por su uso por parte delos aparatos telefónicos inalámbricos y algunos móviles. El fin al que van destinadas las etiquetas que operan en este rango es la cadena de suministro.

    - **Ventajas:** Una de las más grandes que presentan, es que tienen como característica la capacidad de ser leídas simultáneamente a la vez, en grandes cantidades. Otra ventaja es la distancia de lectura, mayor a 3 metros.
    - **Desventajas:** Al contrario de las etiquetas de alta frecuencia no pueden funcionar cuando se encuentran entre una alta concentración de líquidos, esto incluye la presencia de seres vivos y recipientes contenedores.

- **Microondas (microwave):** es el rango de 2.45 GHz.

2.4.2 LECTOR

Hay distintos tipos de lectores, su complejidad o simplicidad van en concordancia con el tipo de transponder que tienen que comunicarse. Los lectores funcionan enviando una señal de radiofrecuencia en un radio de acción determinado. El objetivo es detectar todas las etiquetas que se encuentran dentro de ese radio y entablar comunicación.

Antes de pasar a clasificar los tipos de lectores que existen, hablaremos de factores importantes que afectan a estos dispositivos RFID.

Como hemos visto, los lectores RFID son dispositivos capaces de entablar conversación con los tag, todo ello mediante señales de radio.

El lector debe hacer frente a funciones típicas de sistemas de radio y a su vez también tareas más propias de sistemas radar, comunicaciones pasivas y whireless.

Como características generales los lectores deben ser eficientes, flexibles y exactos. El diseño de estos sistemas tiene como objetivo detectar ofreciendo la mayor fiabilidad posible las etiquetas situadas en un radio determinado. Es decir de forma eficiente mediante ondas de radio de un determinado rango de frecuencia, determinar exactamente las etiquetas que están a su alcance y entablar una comunicación activa/pasiva (flexible) con ellas. Además los lectores se caracterizan por ejercer un bajo ruido de radiación.

Los factores más importantes relacionados con los lectores son los siguientes:

1. **Selectividad:** como sabemos estamos rodeados de señales procedentes de muy distintas naturaleza a nuestro alrededor. Como es obvio nuestro lector tendrá que ser capaz de detectar la señal emitida por el tag, para ello tendrá que escoger de entre numerosas señales que se encuentran en el mismo entorno, algunas de ellas parecidas a la del tag, o incluso más fuertes.

2. **Operatividad:** en un medio donde haya un alto número de lectores RFID, esta norma no es una ley obligatoria pero si recomendable, ya que así permitimos su funcionamiento evitando interferencias con otros lectores. Para poder seguir el estándar del que más tarde hablaremos, el EPC Global, es necesario estar de acuerdo con esta norma.
3. **Sensibilidad:** depende de la calidad del lector, el rango en el que sea capad de detectar señal. El rango común en el que se suelen encontrar los lectores captando señales es de [-80 dBm, -115 dBm]. Si la calidad del lector es alta puede llegar a captar señales de hasta -90 dBm.
4. **Normativas:** Las normativas suelen variar entre países y sobre todo entre continentes. En Europa se permite utilizar estos sistemas entre 865,6-867,6 MHz como rango de frecuencia. El rango de potencia en el lector está fijado en 2 W . En Europa la entidad encargada de regular estos rangos es ETSI (European Telecommunications Standard Institute).
5. **Dinamismo:** un lector no sería eficiente si solo pudiera interactuar con una sola etiqueta, tenemos que pensar que en su rango de acción, estará actuando de forma simultáneamente con un número variable de tags. Además el rango de potencias entre los tags con los que se comunique es posible que varíe ampliamente.
6. **Fiabilidad frente a distintos fabricantes:** es otra de esas normas no obligatorias pero bastante útiles a la hora de operar con componentes de otros fabricantes. Es la EPC de nuevo la que ofrece una certificación que posibilita esto.

2.4.2.1. ASPECTOS GENERALES

En los sistemas lectores de RFID, podemos diferenciar dos elementos que lo componen, en ocasiones, van por separado, pero en el caso de lectores portátiles forman parte del mismo aparato:

- Controlador
- Antenas

Controlador

Este componente tiene como función regular la generación de potencia por parte del lector.

Normalmente está conectado a una red o un procesador de datos, en el primer caso por medio de una conexión TCP/IP, en el segundo por un puerto serial.

El dispositivo es utilizado para controlar las distintas potencias para que un mismo lector pueda leer etiquetas de distinto tipo, ya que las etiquetas activas y pasivas no funcionan con las mismas potencias, y si en un mismo sistema tenemos los dos tipos de etiquetas, debemos ser capaces de tener lectores preparados para entablar la comunicación.

Antena

Estos dispositivos son los encargados de crear un campo tridimensional de acción (haz).

Son el elemento esencial entre la etiqueta y lector (transmite la potencia y recibe la señal de la etiqueta).

Básicamente, la diferencia entre los distintos tipos de antena son estas:

- **Acción corta/larga**, dirigidas a ser usadas dependiendo de la amplitud sobre la que queramos operar.
- **Densidad alta/baja** de campo, la elección de una u otra dependerá del tipo de productos a utilizar y del número a leer simultáneamente.

2.4.2.2. CLASIFICACIÓN LECTORES SEGÚN SU FUNCIÓN DE TRANSMISIÓN

Según esta clasificación encontramos dos tipos de lectores:

- Sistemas de bobina simple
- Sistemas interrogadores

Sistemas de bobina simple

Estos lectores RFID se caracterizan por el envío de información y además la transmisión de energía.

Sus características diferenciadoras en cuanto a coste con respecto a los otros es que es más económico, en cuanto a funcionalidad, estos sistemas tienen un menor radio de alcance para detectar y leer tags.

Sistemas interrogadores

Los lectores interrogadores, a diferencia de los anteriores, cuentan con dos bobinas (los sistemas de bobina simple solo una).

Una de las bobinas está destinada al envío y transmisión de energía, y la otra para información (datos).

Como se dice, los sistemas interrogadores, debido a su mayor sofisticación son más costosos, pero a cambio tienen un mayor punto de acción, ya que su alcance es mucho mayor.

Además es importante indicar que debe haber una concordancia entre la sofisticación y complejidad del transponder y la del lector.

Tendremos problemas de comunicación, eficiencia y sobrecoste en nuestro sistema completo RFID, si nuestros lectores no están adaptados o no son capaces de leer toda la información que manejan nuestros transponder.

También será innecesario poseer lectores en nuestro sistema que sean capaces de realizar funciones mucho más complejas de lo que nuestros tags son capaces de contener, si nuestro objetivo a corto o medio plazo no es ampliar las capacidades funcionales de nuestros transponders.

2.4.3. MIDDLEWARE

Es el nombre que recibe el software de conexión, su función es la de unir una aplicación destinada a la interactuación y comunicación con otras aplicaciones software, hardware, o red.

La importancia del middleware reside en la facilidad que aporta al desarrollador, evitando el estudio y desarrollo a bajo nivel entre las aplicaciones que es necesario interconectar.

En el caso de las aplicaciones relacionadas con los sistemas RFID, es un hecho muy importante ya que disponemos de componentes heterogéneos que necesitamos comunicar además de por medio de las funciones que ya conocemos (ondas electromagnéticas), por medio de aplicaciones que sean capaces de alguna forma de controlar, notificar, además de dar una interfaz y soporte a la comunicación y a todo aquello que está ocurriendo, entre los componentes. Dicho de una forma más técnica es el medio por el que se conecta el hardware con los sistemas centrales.

Específicamente, en los sistemas RFID se debe poner especial atención en la conexión de los procesos referentes a la comunicación y que se realizan de forma continua. Concretamente se pretende tener un control lo más amplio, directo y eficaz sobre los lectores. Se considera un middleware eficiente en este tipo de sistemas a aquel que nos permita la monitorización, implementación, control, emisión y configuración directa a los lectores a través de una interfaz común, teniendo control incluso sobre el "encendido y apagado" de los lectores que estén dentro de nuestro alcance.

En ocasiones, algunos proveedores permiten aplicaciones plug-and-play, son aquellas que permiten a un dispositivo informático conectarse a un controlador o computadora sin configuración previa. En nuestro caso esto significa que podemos activar en nuestro sistema un nuevo lector sin una configuración previa.

2.4.4 OPERADOR

El operador será la persona ya sea física o jurídica, también puede ser una autoridad pública, un servicio o un organismo cualquiera que de forma individual o conjunta con otros organismos o personas determinará los fines para los que se usa un sistema RFID. Además deberá especificar los medios de los que servirá el sistema y el organismo o persona para hacer funcionar la aplicación, refiriéndose tanto a las partes de que consta el sistema, dando especial importancia también a los controladores y mecanismos para tratar los datos, especialmente si éstos son referentes a personas, a través de un programa o aplicación RFID.

Es una figura importante en la implementación y desarrollo de los sistemas ya que obviamente es el representante directo de la actividad que se lleva a cabo, será el responsable a nivel legal, y es por eso que recae sobre esta figura la tarea de aplicar las medidas necesarias, mejoras continuas, y revisiones periódicas para evitar fraudes, amenazas y otros perjuicios a posibles terceros como los usuarios.

Su figura está bien definida en las recomendaciones de la Comisión Europea, así como las tareas que debería llevar a cabo en los sistemas RFID durante el proceso de diseño, implementación y mantenimiento.

2.5. REGULACIÓN Y ESTANDARIZACIÓN

Anteriormente se ha citado la función que tiene el Middleware en general y específicamente en la tecnología RFID, que es la de permitir la interoperabilidad entre los distintos dispositivos que forman un sistema. Para lograr este mismo fin, pero a un nivel más alto es necesario que exista una serie de regulaciones generales para todos los sistemas y dispositivos, que eviten la interferencia entre productos RFID de distintos fabricantes.

Antes también se expuso los distintos tipos de bandas utilizadas en la tecnología y sus distintas aplicaciones y hablamos entre otras de la banda de alta frecuencia **HF (High Frequency),** que en un principio fue la única banda aceptada mundialmente para trabajar en RFID antes de estandarizar su uso, llegó a convertirse en estándar ISO.

La regulación y la estandarización están marcadas por la competición entre las dos entidades que citaremos a continuación.

- ISO
- EPC

Además es importante citar la IEC, debido a su relevancia en la elaboración de normas específicas.

2.5.1 ESTANDARIZACIÓN ISO EN TECNOLOGÍA RFID

2.5.1.1 ORGANIZACIÓN ISO

La organización ISO (International Organization for Standardization), traduciendo sus siglas es la organización internacional de estandarización, el mayor desarrollador mundial de estándares. Los estándares internacionales dan las especificaciones del estado del arte, servicios y buenas prácticas, ayudando a la industria a ser más eficiente y eficaz. Todo ello desarrollado por un consenso global ayudando así a eliminar las posibles barreras del comercio internacional.

Como se ha dicho, la organización se dedica al desarrollo de Estándares Internacionales. Desde que fue fundada en 1947 han publicado más de 19 000 Estándares Internacionales cubriendo la mayoría de los aspectos de negocios y tecnología. Desde el cuidado de alimentos a aparatos tecnológicos, desde la agricultura a la atención médica, podemos decir por tanto que los Estándares Internacionales tienen repercusión directa en nuestras vidas.

Los miembros que lo forman se dividen en tres niveles:

- Miembros titulares: influyen en el desarrollo de normas ISO y participan y votan en las decisiones políticas y técnicas de ISO.
- Miembros Correspondientes: observan el desarrollo de las normas ISO, y asisten a reuniones de política de calidad. Pueden adoptar y vender Normas Internacionales ISO a nivel nacional.
- Miembros subscritos: están al tanto de los desarrollos pero no participan en ellos, no pueden vender ni adoptar normas ISO.

Las nacionalidades distintas de las que proceden los miembros son 164, y colaboran un total de 3335 organismos técnicos en el cuidado de elaboración de normas. Más de 150 personas trabajan a tiempo completo en la central que actualmente se encuentra en Ginebra (Suiza).

El inicio de la organización se remonta a 1946, cuando los delegado de 25 países se reunieron en el Instituto de Ingenieros Civiles de Londres, allí decidieron crear una organización internacional con el fin de "facilitar la coordinación internacional y unificación de las normas industriales". En 1947 la organización ISO comenzó oficialmente su actividad.

Por último, como curiosidad saber que el acrónimo elegido además de representar sus siglas, proviene también de la palabra de origen griego "isos" que significa "iguales".

2.5.1.2 ESTÁNDARES ISO MÁS UTILIZADOS EN RFID

Existen 58 normas ISO específicas directamente de la tecnología RFID. Hay que especificar que los estándares relacionados con RFID llevan una complejidad añadida ya que esta tecnología opera y está relacionada en muchas ocasiones con datos confidenciales de tipo económico (pagos electrónicos) o datos de identificación.

Podríamos separar los estándares ISO sobre RFID en los siguientes grupos:

- Protocolo de comunicación entre lectores y etiquetas.
- Organización de datos en el intercambio de información.
- Pruebas a superar para cumplir con los requisitos del estándar.
- Normas en la utilización las aplicaciones con RFID.
- Seguridad y privacidad de los datos.
- Normas relacionadas con los rangos de frecuencias a utilizar.

En uno de los capítulos más adelante se estudia en profundidad algunas de las normas ISO, especialmente las relacionadas con la seguridad y privacidad de los datos.

2.5.2 INTERNATIONALELECTROTECHNICALCOMMISSION (IEC)

Es importante nombrar a la Comisión Electrotécnica Internacional, ya que es una organización que colabora y en muchas ocasiones desarrollan paralelamente normas con la organización ISO.

El campo de especialización de esta Comisión es la realización de normas sobre tecnologías y aspectos relacionados con la electrónica, y cualquier campo relacionado con lo eléctrico.

Es importante también mencionar que en muchas ocasiones veremos a lo largo de la memoria normas mencionadas como ISO/IEC lo que supone una referencia a esta Organización, y significa que las dos Comisiones habrán desarrollado conjuntamente una norma.

Más adelante serán mencionadas normas IEC que están relacionadas con el uso de distinto rango de frecuencias.

2.5.3. ESTANDARIZACIÓNY REGULACIÓNEPCEN TECNOLOGÍA RFID

2.5.3.1. COMIENZOS DE LA EPC

Todo comenzó debido a problemas con la distribución de un lápiz de labios (Color Moist Hazelnut Nº 650 de Oil of Olay) en 1997 en la marca Procter & Gamble. El éxito fue tal que era imposible mantenerlo en mercado, el problema residía en que las existencias en almacenes se agotaban, pero había existencias sin circular debido a la insuficiencia de los códigos de barras.

En busca de una solución, el responsable llamado Ashton, fue puesto en conocimiento de una emergente tecnología de identificación, llamada RFID, que estaba siendo utilizada con éxito en funciones de pago en carreteras y también identificación y acceso a instalaciones, entre muchas otras. La empresa vio en esta tecnología la solución a su problema, y rápidamente se puso en contacto con investigadores involucrados en la identificación por radiofrecuencia, algunos de ellos en ese momento ocupados con la tarea de investigar la miniaturización de esta tecnología. Tras unas reuniones para intentar buscar una solución óptima al problema de los lápices labiales, se llegó a la idea de colocar un chip a cada lápiz con un número identificativo único, con el que poder rastrear de una de manera eficiente el inventario. Enseguida gracias a este caso se hizo notar el potencial de esta tecnología en la cadena de suministro y otras aplicaciones.

Así en 1999 con fondos de Procter & Gamble, Gillette y la entidad Uniform Code Council, quedó fundado el Centro de Auto-Identificación en Massachussets. El director fue el propio Ashton, gestor de la empresa de lápiz de labios que dio a conocer la tecnología ante su problema de inventario. El propósito del centro fundado era la investigación y desarrollo de RFID con una visión dirigida a la cadena de suministro y con la idea de identificar a un objeto independientemente de donde se encontrarse, tener una visión global.

Cuando en 2003 el centro contaba con 103 empresas e instituciones asociadas el Auto-ID Center fundado en 1999 transfirió su tecnología a EPC Global, contando con el respaldo de otras asociaciones y prestigiosas empresas como Accenture o Pepsico. Como objetivo estaba el impulsar la adopción de este sistema de forma global y asociar las tecnologías existentes con Internet y RFID, reforzando y haciendo más eficiente el modelo de cadena de suministro.

2.5.3.2. FUNCIONES EPC

Como organización internacional de RFID, se encarga principalmente de los estándares de código de producto electrónico y su uso. Esta entidad colabora además con EAN y UCC cuya función es regular el código de producto internacionalmente en Europa y Estados Unidos. Estas organizaciones llevan años gestionando estándares a nivel global.

Con los estándares que regula y aplica, esta organización persigue facilitar la eficiencia, eficacia, estandarización, regulación y exactitud de la automatización, labores de seguimiento y seguridad con la denominada "visibilidad mejorada", proporcionando un entorno estandarizado para facilitar el intercambio de información.

Todo ello tiene como fin principal mejorar la expansión, mejorando los procesos de detección de demanda y acelerando dichos procesos. Entre otro de sus objetivos está la continua mejora de los procesos directamente físicos como la recepción, registro, clasificación, etc.

Las principales organizaciones que promueven los sistemas RFID y a su vez los estándares y especificaciones en cuanto a las etiquetas son Wal-Mart y el Departamento de Defensa de EEUU.

2.5.3.3 CÓDIGOS EPC

Como las siglas indican, EPC (Electronic Product Coda) es un código con función similar al código universal de producto de los códigos de barras, en los códigos de la EPC encontramos información sobre el fabricante, producto, versión y número de serie, además identifica artículos únicos.

Un código EPC sirve para identificar un producto que existen en la Red EPC Global. A continuación un análisis de los códigos EPC (Notación Hexadecimal):

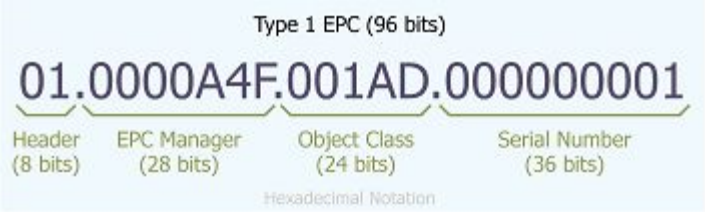


Ilustración 4: Código EPC

- Header: identifica la longitud, tipo, estructura, versión y generación de EPC. Longitud: 8 bits.
- EPC Manager: identifica la compañía con dicho número. Longitud: 28 bits.
- Object Class (Clase de objeto): parecido a una unidad de mantenimiento de existencias. Longitud: 24 bits.
- Serial Number: campo con la especificación del tipo o clase del objeto que va a tener la etiqueta. Longitud: 36 bits.

Opcionalmente se pueden añadir más campos dependiendo de la información que deseemos codificar.

CAPÍTULO 3. APLICACIONES DE SISTEMAS RFID

Aunque el uso de la tecnología RFID cada vez está más extendido en la industria española, hay que decir que el nivel de uso es por el momento incipiente aunque con un gran potencial como estamos comentando.

Según los estudios realizados por la ONTSI (Observatorio Nacional de las Telecomunicaciones y de la SI), y que a continuación se procede a analizar los datos obtenidos por el observatorio comparando lo obtenido en 2010 y 2012.

En 2010 observamos como el 0,8 % de las Microempresas utiliza la tecnología RFID en su actividad empresarial. En el 2012 se repite el mismo dato para las microempresas con un 0,8 % de uso.

Notamos un incremento en el caso de las empresas que tienen a partir de 10 trabajadores, en el caso del año 2010, el 3,1 % incorporaba la tecnología RFID para el desarrollo de su actividad, mientras que en el estudio del 2012 vemos que es el 6,1 %.

Un dato relevante de este estudio, es también conocer cuál es el sector que más interés muestra por el momento por este sistema de identificación. El transporte y el almacenamiento son los negocios que más uso hacen de RFID, con un 4,4 % de sus microempresas haciendo uso de ello.

En cuanto a los motivos de uso más frecuentes en 2012 según las microempresas que lo usan son los siguientes:

- El 77,1 % lo usa como parte de control de proceso de producción, gestión y prestación del servicio.
- El 44,6 % para controles de acceso e identificación de personal
- El 27,8 % para prevención de falsificación, control de robos, y otros usos de seguridad.

3.1.ACTUALES APLICACIONES.

Según el estudio mencionado antes, podemos clasificar las principales aplicaciones, que en general han tenido éxito allí donde la identificación eficaz, rápida y barata supone un beneficio para la actividad de la empresa.

Dicho esto, los sectores donde tiene más éxito:

- Toda aquella actividad en la que sea importante la identificación de objetos únicos, como es la venta de artículos. La finalidad puede ser desde evitar robos, a controlar el stock, o la relación de la mejor del comercio respecto a ese producto.
- En el transporte público, en los accesos.
- En el seguimiento de mascotas, para contemplar desde los datos del propio animal, y hacer su seguimiento, así como los datos del dueño en caso de pérdida del animal.
- Uno de los usos más conocidos, es el de pago de peajes automático. Entrando en detalles más técnicos, para cobros exactos se utiliza la banda UHF (Ultra High Frequency), para evitar así el uso de monedas o billetes y automatizar el proceso completamente.
- En las bibliotecas, facilitando el proceso de catalogación, ordenación y seguridad frente a intentos de robo. El tipo de etiquetas más utilizado en bibliotecas es el de sistemas pasivos UHF.
- En el sector sanitario, para el seguimiento y control de medicamentos y otras mercancías que es necesario controlar e identificar, como es el caso de los bancos de sangre.

3.2.FUTURAS(O POSIBLES) APLICACIONES.

Además de todas las aplicaciones implantadas y utilizadas, existen otras que se encuentran en desarrollo y que presentan un alto potencial para su adopción por parte de las empresas:

- Pagos a través del aparato de teléfono móvil, a través de la tecnología conocida como NFC (Near Field Communication), este sistema permite que un móvil obtenga los datos de una etiqueta RFID, con lo que podemos pagar directamente el artículo acercando el aparato telefónico al punto de información RFID.
- Ya existen países en que se utiliza el pasaporte electrónico (todos los países de la Unión Europea), en el que se almacena en un chip RFID toda la información del sujeto, huella dactilar, fotografía, y demás datos que identifican al ciudadano.
- Activación y funcionamiento de vehículos y maquinaria, esta aplicación está pensada para hacer funcionar tanto vehículos como maquinaria industrial, en caso de detectar cierto chip RFID.

3.3 TECNOLOGÍAS RELEVANTES RESPECTO A RFID

ALIEN TECHNOLOGY

El proveedor Alien Technology Corporation es líder en productos RFID que tienen como destinatario clientes globales como el gobierno en Estados Unidos, venta al por menor, manufactura, farmacéuticas, industria, transporte, etc.

Alien Techonology además posee un proceso de fabricación que tiene patentado (FSA). Mediante este proceso fabrica etiquetas EPC en grandes cantidades y con un coste reducido.

Además ofrece su gama de lectores RFID para una alta variedad de aplicaciones, entre las que están la gestión de la cadena de suministro, logística, control de fraude como por ejemplo falsificaciones, mejora de gestión de inventarios en la cadena de suministro, y otros.

Cabe destacar que es uno de los miembros activos de EPC Global.

CAPÍTULO 4. COMPARATIVA CON OTROS SISTEMAS EXISTENTES

A continuación se hace un repaso de las tecnologías que se encuentran en el mismo grupo que RFID. Son los denominados de "identificación automática". Algunos de ellos son ampliamente conocidos por el usuario. Por sus características, son candidatos en un futuro próximo a ser sustituidos por los sistemas RFID, debido a las mejoras que incorporan los sistemas de radiofrecuencia, en cuanto a prestaciones, operatividad y precio.

4.1 OTROS SISTEMAS EXISTENTESCON FUNCIONES PARECIDAS

En este apartado se exponen los sistemas comparables en su función, o fines (identificar automáticamente objetos o sujetos) a los RFID.

4.1.1. CÓDIGO DE BARRAS

Es el sistema más extendido de identificación, podemos verlo en la mayoría de objetos por ejemplo en el sector de envasado de líquidos para el comercio alimenticio. Las partes de las que consta son las siguientes:

- Código formado por barras y espacios paralelos
- Lector óptico láser
- Sistema informático que procesa la secuencia numérica o alfanumérica.

- En general las diferencias con los sistemas RFID son las siguientes, siendo la más significativa la limitación por parte de los códigos de barras para ser leídos:
- Limitación en la lectura. Para leer un código de barras hay que tener el lector láser directamente proyectado hacia el código.
- La lectura simultánea con un mismo lector es inviable.
- Una de las diferencias más importantes es que no sirve para identificar objetos únicos, sino tipos de objetos o grupos.
- Se enfrenta a un riesgo alto de ser dañado, y por tanto sin funcionar, ya que requiere de lectura directa, y va adherido en la superficie de los objetos.

4.1.2. SMART CARDS

Son las llamadas tarjetas inteligentes que tienen capacidad de almacenamiento de datos y capacidad de procesamiento. Van integrados en un componente parecido al de las tarjetas de crédito.

Dos de sus características más importantes y destacables es su grado de seguridad bastante alto, y su coste es bastante rentable.

Ilustración 5: Chip Smart Card

Respecto a RFID podemos encontrar los siguientes inconvenientes:

- Las Smart Cards requieren un lector directo.
- No podemos obtener simultaneidad en cuanto a la lectura de varios objetos que estén dentro de nuestro alcance.

4.1.3. SISTEMAS DE IDENTIFICACIÓN POR BIOMETRÍA

Algunos ejemplos de esta tecnología son los sistemas de reconocimiento por huella dactilar, por reconocimiento facial, reconocimiento ocular, por la forma de la oreja, por voz, o incluso por el patrón que seguimos en nuestra forma de escribir.

La información que se obtiene de nuestro cuerpo se almacena de forma numérica para luego ser comparados a la hora de identificar.

Existe una tasa de error en cuanto a la seguridad en cuanto a la identificación del sujeto correcto.

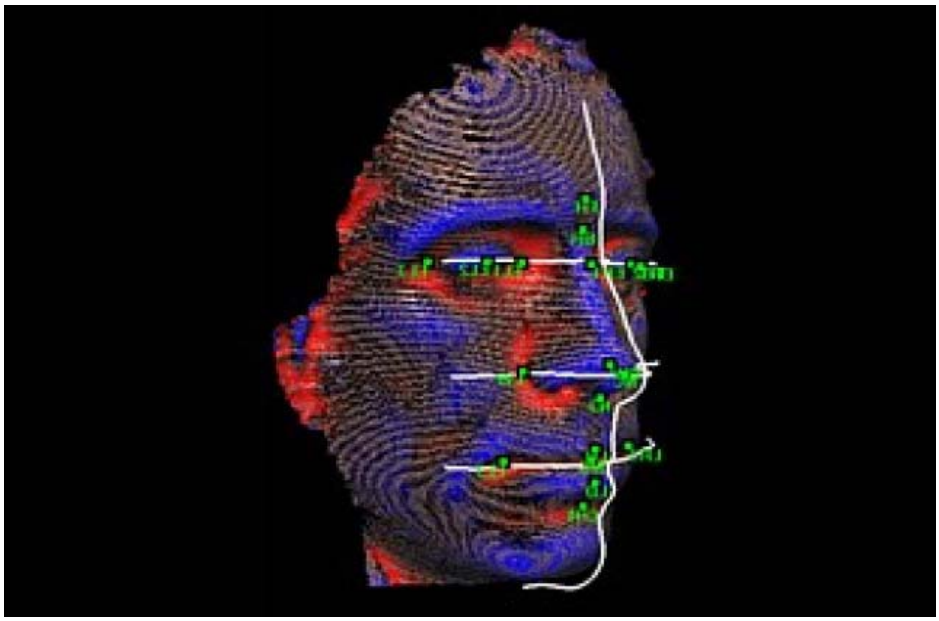


Ilustración 6: Sistemas Biometría

En cuanto a la tecnología por radiofrecuencia presenta las siguientes diferencias generales:

- Su forma de identificación sirve para identificar sujetos únicos, personas o animales, pero no es viable para el caso de objetos.
- Los costes son más altos, debido a la sofisticación del modelo de identificación.
- Necesita contacto directo para comparar los parámetros de comparación

4.1.4. OCR IDENTIFICACIÓN POR RECONOCIMIENTO ÓPTICO DE CARACTERES

Este sistema fue utilizado por primera vez en los años 60. Se basa en la lectura e identificación de objetos por un lector óptico.

El proceso consiste en pasar un texto a imagen escaneada, cuyo fin es ser interpretada y procesada por un sistema. Estos sistemas son capaces de interpretar imágenes en variados formatos como JPEG o archivos PDF.

Lo que se logra mediante el proceso es interpretar los caracteres que contienen la imagen o documento introducido en el sistema.

Entre las aplicaciones más generales y extendidas, se encuentran las lecturas de matrículas en casos de control de tráfico, o en el sector bancario, la lectura de cheques y facturas.

4.2.COMPARATIVA (BENEFICIOS E INCONVENIENTESDE LA TECNOLOGÍA RFID)

El objetivo de haber expuesto estas tecnologías en comparación con RFID, es porque la identificación por radiofrecuencia es potencialmente y en algunos casos, un hecho, sustituta de otras tecnologías de identificación.

Por ejemplo, basado en datos estadísticos, la tecnología RFID está llamada a sustituir al código de barras, el motivo principal, es el ahorro en costes materiales y personal. Además presenta una mayor eficiencia como comentábamos, ya que sus posibilidades de simultaneidad en identificación es mucho mayor.

En el caso de Reconocimiento Óptico de Caracteres (OCR), presenta mejoras en todos los aspectos, siendo la principal diferencia la reducción de los altos costes de OCR. Hay ciertas excepciones en los que el sistema Óptico de Reconocimiento seguirá siendo utilizado, y es debido a especificaciones en su uso, como el caso de los radares en carreteras.

En el caso de los sistemas Biométricos, es posible la sustitución por RFID, solo en aquellos casos, en los que no haga falta una nivel de seguridad extremo, y que si pueden aportar estos sistemas.

Respecto a las tarjetas inteligentes, la principal mejora que presenta la identificación por radiofrecuencia es la autonomía energética para funcionar. Las tarjetas necesitan del contacto directo con un lector que aporte la electricidad necesaria para poder ser útil, lo que no ocurre en el caso de las etiquetas y lectores RFID.

CAPÍTULO 5. CONTROL EN SISTEMAS RFID

En este apartado el principal objetivo es identificar las áreas generales sobre las que existe un mayor riesgo relacionado con estos sistemas, centrándose el análisis sobre todo en seguridad y privacidad.

También se realizará una identificación de los posibles tipos de riesgos, y sus consecuencias. Además se expondrán casos reales (y potencialmente posibles), sus consecuencias y posibles medidas, así como el verdadero alcance de posibles fallos y usos malintencionados.

El interés específico en campos como la seguridad y privacidad, es que en estos sistemas es especialmente importante mantener un marco que asegure la ausencia de amenazas en la medida de lo posible. La razón es que estos datos en muchas ocasiones no se encuentran únicamente almacenados en una aplicación, y por lo tanto más fácilmente controlable, sino que en muchos casos encontraremos que el propio dispositivo que porta el cliente (etiquetas, tarjetas, objetos con tags adheridas), almacenan datos privados (datos directamente del cliente, o relacionados con el mismo), y mediante políticas, normativas y metodologías se ha de asegurar que esos datos y por tanto el propio cliente no se encuentran en riesgo.

5.1.RIESGOS EN EL USO RFID

De la misma forma que esta tecnología supone un avance y progreso para muchos tipos de negocios y actividades empresariales, como hemos repasado anteriormente, abre una serie de riesgos que van inherentes a su condición de nueva tecnología en estos campos.

Especialmente existen distintos tipos de usos o actividades en las que existe un mayor riesgo y que deberán ser tratados de forma especial.

- Por una parte hemos hablado de las empresas que están adoptando el modelo de identificación por radiofrecuencia para sistemas de gestión en general, como puede ser en cadenas de montaje, almacenamiento, y actividades relacionadas con la seguridad, y gestión de personal.
- También nos encontramos con usos donde tratamos con datos que pueden significar de algo riesgo para un uso malicioso, son los casos en los que el uso de RFID va dirigido a actividades como soporte a control de accesos, usuarios de carácter particular como puede ser el ámbito sanitario o venta de productos. Podemos intuir que el tipo de datos manejados es demasiado sensible como para permitir que existan grandes riesgos de manipulación de datos dirigidos a otras actividades que las enunciadas.

Como podemos ver tenemos usos muy diferentes para esta tecnología, pero a la hora de clasificar los riesgos, lo haremos en dos grupos como veremos en los apartados siguientes.

Podemos agrupar por una parte los riesgos relacionados con la seguridad, en los que nos encontraremos problemas con averías o ataques que estén relacionadas directamente con el servicio. Especialmente localizaremos un riesgo para la

seguridad cuando encontremos una alteración del servicio, una interrupción, una alteración que suponga con fines maliciosos como un fraude.

El otro grupo que identificamos como un riesgo a tener en cuenta y controlar al máximo es el relacionado con la privacidad. En estas actividades incluiremos todas las actividades en las que haya un intento, o un uso inapropiado de datos personales, procesos que están relacionados con los servicios dirigidos a usuarios, lo que puede desencadenar graves repercusiones en las empresas que dan soporte a los servicios de usuarios.

En los siguientes capítulos estudiaremos los verdaderos riesgos, tanto para la seguridad, privacidad, y el impacto que tienen directamente sobre los humanos, y cuál es el control del entorno adecuado para asegurar o reducir al máximo los riesgos citados.

5.1.1.RIESGOS EN LA SEGURIDAD

Existen varios tipos de amenazas que están directamente relacionados con los sistemas RFID, algunos de ellos van dirigidos a explotar con fines malintencionados los posibles vacíos por ejemplo a nivel de middleware o en otros casos se ayudan de la capacidad de estos sistemas para usar las ondas de radio para comunicarse entre las distintas partes de un sistema completo.

Entre las amenazas más importantes se encuentran:

ATAQUE POR DENEGACIÓN DE SERVICIO

Estos ataques se caracterizan por pasar fácilmente inadvertidos por parte de los usuarios, por su relativa facilidad para ser llevados a cabo, y su dificultad para ser evitado.

En los siguientes casos, se explica la forma en que se puede dar este ataque en RFID:

- **CASO 1**: Un atacante o intruso puede "matar" las etiquetas que intervienen en la cadena de suministro, en un almacén, o en un establecimiento con el fin de dañar el negocio, o evitar la salida de un determinado elemento al mercado.
- **CASO 2**: Un atacante destruye o elimina físicamente etiquetas adheridas a los objetos. El fin general es evitar el seguimiento del objeto, el propósito puede ser evitar ser detectado ante un robo, o ante la eliminación del objeto.
- **CASO 3**: Un atacante blinda la etiqueta para evitar su lectura.
- **CASO 4**: Un atacante podría tener un generador de señal de largo alcance tan potente que hiciera interferencia entre el lector/interrogador y la etiqueta evitando así su lectura. La consecuencia más probable es que el lector lanzara una alarma ante la imposibilidad de leer la etiqueta.
- Como vemos en alguno de los posibles casos, hay que ser conscientes que los sistemas RFID como todos los que tienen un soporte físico, son vulnerables ante su destrucción o daño directamente físico. En el caso de las etiquetas de radiofrecuencia está el añadido de estar adheridas a los objetos que identifican, facilitando de alguna forma su posible deterioro intencionado.

ATAQUE DE COLISIÓN

El ataque por colisión viola la forma en que un lector identifica de forma única una etiqueta para su comunicación. La colisión de etiquetas ocurre cuando más de uno de los tags responden ante el interrogatorio del lector al mismo tiempo.

Si no existe ningún tipo de protocolo entre el lector/interrogador y las etiquetas no es posible llevar a cabo una eficiente forma de lectura, y ésta se torna imposible.

La forma que tiene de actuar el atacante, es haciéndose pasar por una o más etiquetas en el momento en que el lector lanza la consulta a las etiquetas, creando así un conflicto.

Funciona de forma parecida a un Ataque de denegación de servicio (conocido como ataque DoS, que de forma resumida, bloquea un servicio y lo hace inaccesible, sobrecargando los recursos computacionales de la víctima.

DESINCRONIZACIÓN

Esta amenaza trata sobre la posibilidad de perder la sincronización entre el servidor, o base de datos y una etiqueta RFID, que puede tener como resultado la inutilidad de la etiqueta.

Como hemos visto existen dos tipos de operaciones entre el lector/interrogador y la etiqueta: lectura y escritura.

Este tipo de ataque está más relacionado con la operación de lectura, especialmente con la actualización de datos y su escritura en la etiqueta, es decir tiene como objetivo la destrucción del proceso en sí. El atacante puede realizar la desincronización desestabilizando la conexión entre la etiqueta y el lector, o directamente sobrecargando, destruyendo o manipulando la red que los conecta.

REPLAY

Los ataques de repetición tienen como fin colapsar los recursos informáticos de lector y la etiqueta.

Como ejemplo, en un posible caso, podría existir un ataque contra un lector RFID, el atacante podría obtener acceso a la identidad de una etiqueta de anteriores comunicaciones y luego replicar esa identidad o la comunicación al interrogador que anteriormente consultó y recibió una respuesta de dicha comunicación, colapsando así el sistema.

HOMBRE EN MEDIO (MAN-IN-THE-MIDDLE)

Este ataque conocido por sus siglas en inglés como MIM, es una forma de ataque denominada de escucha activa en la que el atacante hace conexiones independientes con etiquetas, interrogadores/lectores RFID, y el sistema de almacenamiento y transmite e intercambia mensajes entre ellos, haciendo creer al sistema que las distintas partes están hablando directamente entre ellos, cuando en realidad, toda la comunicación o conversación está siendo controlada por el atacante.

Para que sea considerado un ataque de este tipo, el atacante debe ser capaz de interceptar los mensajes que van entre las dos víctimas e introducir nuevos, esto si es posible en algunos sistemas RFID.

El ataque solo acaba siendo satisfactorio por parte del atacante cuando éste es capaz de hacerse pasar por cada punto final a satisfacción del otro.

ROBO

No es un riesgo específico de los sistemas RFID, pero uno de los riesgos de estos sistemas como comentamos anteriormente junto con el riesgo de ser destruidos, es que al estar adheridos a objetos, o los lectores colocados en algunas ocasiones en lugares específicos y fijos, es que pueden ser robados o retirados.

ACCESO/BORRADO/MODIFICACIÓN NO AUTORIZADO DE DATOS

El acceso no autorizado a la eliminación o modificación en un equipo se produce cuando un atacante modifica, añade, elimina o cambia el orden de los datos.

Esta amenaza a la seguridad está considerada como una de las más graves si atendemos a sus posibles consecuencias como el posible ataque al pasaporte de un ciudadano, y la manipulación de su identidad y datos personales, o a la identidad

de un producto en la cadena de suministros, o a la intervención en operaciones comerciales ocasionando pérdida en los ingresos.

Los casos más grave por ejemplo en la seguridad de los ciudadanos puede darse con la denegación de la entrada en un país a un ciudadano al que le han manipulado la identidad en un pasaporte. Y visto desde otro punto de vista, si alguien logra adoptar la identidad de otra persona para realizar actividades que afecten a su reputación, pérdida financiera o actividades delictivas mediante esta forma de fraude.

Se ha observado un problema específico con el comando "kill" que puede ser peligrosa en poder de un atacante contra las etiquetas, en los casos en que no se ha seguido una política de contraseña correcta, o directamente no se ha aplicado contraseña.

El potencial negativo de este comando en manos de un atacante con la posibilidad de matar etiquetas abarca consecuencias como el desvío de productos, por medio de la pérdida de seguimiento o robo de ellos, hasta la quiebra de la empresa si es llevado a cabo a gran escala. Obviamente depende del nivel de dependencia que la empresa tenga de la tecnología RFID.

CLONACIÓN DE ETIQUETAS RFID

La mayoría de etiquetas que se utilizan en el mercado no poseen características de protección anti-clonación de forma explícita. Además no existen normas que obliguen a los mecanismos de lectura e interrogatorio a autenticar la validez de las etiquetas que escanean. El proceso de identificación funciona de forma que una etiqueta emite su respuesta promiscuamente y el lector tiene una forma predeterminada de aceptar dicha respuesta. Vemos como de esta forma existe una vulnerabilidad frente a la clonación de etiquetas.

El atacante puede obtener los datos esenciales de una etiqueta, de forma bastante simple escaneando o accediendo a la base de datos de la etiqueta adecuada.

Este problema se puede ver potenciado por la forma o método que se haya utilizado para asignar identificadores a las etiquetas. Si es de forma aleatoria, es más complicado para el atacante hacerse con los números de identificación, pero si por el contrario es de forma secuencial, es mucho más sencillo obtener los identificadores conocido uno.

GUSANOS, VIRUS Y CÓDIGO MALICIOSO

El software infeccioso, más comúnmente conocido como virus, puede ser usado para manipular, divulgar o evitar de forma maliciosa la comunicación entre las distintas partes de un sistema RFID (etiquetas, lectores, conexiones de red).

ATAQUE AL CANAL CON INFORMACIÓN INDIRECTA

Es un ataque basado en la información obtenida de la implementación física de un sistema cifrado, en lugar de la obtención por medio de fuerza bruta o puntos débiles en los algoritmos. Estos casos pueden ser fugas de información, el consumo de energía del sistema, fugas electromagnéticas, o incluso el sonido pueden proporcionar una fuente adicional de información que puede llegar a ser usada por los atacantes para romper el sistema. Es cierto que requiere un alto nivel técnico del funcionamiento del sistema interno y criptográfico.

ATAQUE ENMASCARADO

Este ataque ocurre cuando un atacante se hace pasar a todos los efectos como un usuario autorizado en el sistema. Son diversas las formas de las que puede afectar a los sistemas RFID, un uso malintencionado puede ser la intrusión en el sistema con el fin de espiar y obtener los datos sobre la cantidad de artículos y sus tipos en el inventario de una empresa, o los más graves como la intrusión en los datos que pertenecen a la intimidad de una persona.

Como hemos comentado anteriormente es fácil emular la identidad de una etiqueta, lo cual supondría una forma de enmascaramiento, si el lector/interrogador no es capaz de diferenciar una identidad verdadera de un intruso que emula o clona la identidad de una etiqueta.

ANÁLISIS DE TRÁFICO/SONDEO/EXPLORACIÓN

El análisis de tráfico, es el proceso de interceptar y examinar los mensajes con el fin de poder deducir información basándose en los patrones de comunicación extraídos de ese análisis.

En el caso de los sistemas RFID , puede ser utilizado para conocer la ubicación de las etiquetas y los interrogadores, así como la frecuencia con que se produce la comunicación.

Este tipo de ataque puede llevarse a cabo incluso cuando los mensajes son encriptados y no es posible descifrarlos.

Es fácil deducir que dependiendo del volumen de tráfico, y análisis realizado depende el tamaño de la amenaza y más se puede deducir del tráfico analizado.

Las consecuencias directas en un entorno RFID pueden llevar al atacante a saber la ubicación, el tipo de etiquetas y lectores, las conexiones de red existentes y el sistema de almacenamiento de datos.

ESPIONAJE RF

Esta amenaza se refiere a la acción de escuchar en secreto sin el consentimiento del escuchado.

El componente diferenciador de RFID es el uso que da a la radio frecuencia para poder comunicarse entre las distintas partes de un sistema completo, más específicamente entre etiqueta y lector. La señal generada por radiofrecuencia es susceptible de ser espiada.

El problema más grave ocurre cuando el atacante conoce las especificaciones sobre la codificación de la señal, sería el paso previo para poder ejecutar directamente otros ataques como la suplantación, el ataque por replay, o de seguimiento.

5.1.1.1 CASO REAL

El riesgo en la seguridad principalmente radica en la posible vulnerabilidad de los mecanismos de seguridad en los sistemas RFID.

Como ejemplo pondré una noticia de las posibles vulnerabilidades de estos sistemas:

Clonación de tarjetas con RFID

Demuestran como clonar tarjetas de crédito de forma inalámbrica, tal como mostró la investigadora de seguridad Kristin Paget en el congreso ShmooCon 2012 que se celebra en Washington, clonando una tarjeta de crédito con tecnología de pago sin contacto (RFID) y permitiendo que la copia pueda ser usable al menos una vez, utilizando el siguiente material:

-lector de tarjetas RFID (50$ en eBay)

-grabador de tarjetas (300$)

El lector fue usado para obtener los datos de la tarjeta de un voluntario del público que se ofreció, y en la que figura el CVV de un solo uso que se emplea para autenticar los pagos sin contacto directo. Una vez obtenidos los datos, paso a crear un duplicado de la tarjeta mediante el grabador de tarjetas, y el software de pago sin contacto de un teléfono móvil iPhone se "donó" 15$ con la tarjeta copiada. Con el fin de evitar cualquier tipo de problema, le entregó al voluntario un billete de 20$ a cambio de su ofrecimiento.

Es alarmante pensar que podría ocurrir si este tipo de acciones se llevaran a cabo en un lugar público con acceso a múltiples dispositivos de este tipo, como por ejemplo en un recinto deportivo o un medio de transporte.

Fuente: Forbes 2012

5.1.2. RIESGOS EN LA PRIVACIDAD

Como está comentado anteriormente existen ciertos riesgos respecto a esta tecnología, es por esto que debe haber una acción conjunta entre los encargados de desarrollarla, como por parte de las empresas proveedoras, así como los fabricantes, las entidades internacionales y gobiernos a la hora de marcar objetivos comunes que tengan como fin ofrecer un entorno seguro que garantice la libertad y seguridad de los usuarios de RFID.

Es preciso decir que al igual que existe un gran desarrollo y un potencial uso masivo de esta tecnología, también existen detractores (asociaciones tanto jurídicas y de ciudadanos) en contra de la identificación por radiofrecuencia, alegando que suponen una amenaza para la privacidad y los derechos humanos.

Hasta ahora hemos citado a lo largo de los capítulos las mejoras y opciones que presenta esta tecnología, sus ventajas respecto a las demás, pero el objetivo principal de este estudio es la presentación de sus riesgos y presentar posibles formas de atajarlos. Uno de los puntos débiles de la radiofrecuencia utilizada con fines identificativos es la polémica que arrastra desde su expansión en nuestro entorno, por los riesgos que potencialmente puede presentar para la privacidad. Podemos presentar varios puntos que en principio alarmaron en cuanto a riesgos se refiere:

- Posibilidad de lectura de etiquetas a distancia sin notificación a un posible portador de la etiqueta
- Posible rastreo, y conocimiento de identidad en caso de que el usuario utilice etiquetas RFID con tarjetas.
- Desconocimiento por parte del comprador o usuario final de un producto de la utilización por parte del producto de etiquetas y su incapacidad por tanto para eliminarla si así lo desea.

Una de los puntos que más preocupan sobre las etiquetas es su funcionamiento una vez el producto está en manos del consumidor. En ocasiones la etiqueta una vez el producto ha sido vendido sigue funcionando, lo que puede suponer un posible rastreo, con múltiples fines como el interés por los hábitos del consumidor, vigilancia o riesgo de robo por al usuario.

Existen medidas contra algunos tipos de ataques, pero no significa la erradicación de contramedidas para anularlas. Por ejemplo como medida para anular el ataque a distancia sobre etiquetas con información confidencial o susceptible de ser atacada y manipulada, existe la medida de utilizar etiquetas de corta distancia. Como reacción los ataques pueden ser ejecutados con antenas de mayor potencia (alta potencia).

Pasamos a analizar los posibles riesgos, la dimensión de estos, sus posibles soluciones, y las legislaciones ya creadas. El análisis se plantea dividido en bloques:

- Cadena de suministros.
- Acciones y prácticas por parte de los gobiernos.
- Acciones y prácticas por parte de instituciones y asociaciones empresariales.

5.1.2.1 RIESGOS EN LA PRIVACIDAD EN LA CADENA DE SUMINISTROS

Hemos hablado de las posibilidades de hacer un seguimiento al cliente una vez el producto está en sus manos y desconozca que contiene una etiqueta RFID, dificultando así su eliminación. Algunas fuentes lo citan así:

"***1.*** *Utilizando números de serie RFID permanentes, un artículo proporciona información a los fabricantes sobre una persona. Cuando los artículos se revenden o regalan, pueden trazar y dar a conocer la red social de una persona."*

Fuente: "RFID Oportunidades y riesgos"

Es cierto que esto podría pasar, si se cumplieran ciertas condiciones. Si existiera una infraestructura formada por lectores y detectores, a nivel internacional, o simplemente de una forma implantada y generalizada, se podría hacer un rastreo completo de un producto siempre que contuviera su etiqueta RFID. La situación actual es que algo así no podría ocurrir ya que el alto coste de tener instalada una estructura que sostenga el proceso hace que no exista, y además esta tecnología no se encuentra en un nivel de implantación tan alto que justifique este tipo de red de detección, que permita la lectura de una etiqueta en cualquier punto del planeta.

Además el riesgo está focalizado en las propias etiquetas, es obvio y ha sido expuesto anteriormente que son mucho más potentes que otros sistemas de identificación como los códigos de barras. Cómo sabemos las etiquetas guardan información relevante y de riesgo, pero no son las etiquetas las que suponen el riesgo, sino las aplicaciones informáticas destinadas a recopilar la información de los productos y que ofrecen la vía para acceder a esos datos.

También es cierto que al ser una tecnología nueva, supone un aliciente más para levantar alarmas sobre su riesgo en cuanto a seguridad se refiere. Si nos fijamos existen múltiples empresas que trabajan con nuestros datos confidenciales a diario. Por ejemplo cada vez que pagamos con una tarjeta bancaria, se está realizando un proceso por el cual nuestros datos personales y económicos están circulando desde una caja, cajero, tienda, hasta la central de los datos.

Hay una serie de recomendaciones, o buenas prácticas que se recomiendan a los proveedores que están implicados en la cadena de suministros, a grandes distribuidores y a minoristas:

- Aviso al consumidor de la inclusión de un tag RFID en el producto, y de sus posibles riesgos
- Como comentábamos, los tags es recomendable deshabilitarlos una vez está en manos del consumidor, algo que no ocurre siempre.
- Generalmente se recomienda colocar la etiqueta en el envoltorio o recubrimiento del producto, siempre que sea posible.
- Es altamente aconsejable colocar la etiqueta en un lugar localizable y facilitar su separación del producto.

Como hemos mencionado algunos de los riesgos está relacionado con el alcance de la señal, y las posibles infraestructuras con fines malintencionados frente a estos sistemas. Pero los sistemas de corto alcance pasa a ser un riesgo cuando todos los artículos que son detectados están relacionados con una base de datos unificada de algún modo cada vez que la persona pasa cerca de un dispositivo lector.

Al igual que comentábamos anteriormente en este apartado, todo depende de la estructura formada informáticamente alrededor del consumidor, como sabemos actualmente no existen tales medios que supongan una amenaza palpable o generalizada para ellos. La manipulación de datos conlleva intrínsecamente un riesgo al igual que en otros sistemas de identificación y gestión de datos de algún modo críticos.

Ejemplo que pone de manifiesto los puntos mencionados, es el de la tienda de alimentos Grocery (Estados Unidos), muestra en sus pantallas anuncios que se ajustan a tus gustos y tendencias a la hora de consumir. Esto se consigue de la siguiente forma, mediante la etiqueta RFID y la tarjeta de crédito, las consecutivas

ocasiones en que visitas la tienda eres reconocido, junto con el historial de compras, personalizan los anuncios que en principio se ajustan a tus anteriores compras.

La infraestructura para llevar a cabo esto requiere un alto nivel de sofisticación, por un lado la base de identificación RFID y código de barras, y por otra parte un sistema informático que permita almacenar nuestras compras y a la vez lo relacione con los productos actualmente en venta y que están vinculados con nuestras anteriores consumiciones.

Las autoras del libro **Chips Espías**, Katherine Albrecht y Liz Mcintyre que encabezan el movimiento creado en 1999 denominado "Consumidores en contra de la invasión a la privacidad y enumeración por los supermercados", afirman lo siguiente:

"RFID nos ofrece un mundo en el que cada compra se supervisa y registra en una base de datos y cada posesión está enumerada".

Es una visión demasiado radical, pero potencialmente posible, y de nuevo caemos en el tema de las infraestructuras globales inexistentes que lo podrían permitir actualmente.

También en su libro las autoras nos refieren lo siguiente:

"Una empresa con acceso a información clasificada, tiene un registro de todo lo que usted ha comprado, de todo lo que ha poseído, de cada pieza de vestir en su armario, de cada par de zapatos. Una vez que todas las posesiones de una persona se encuentran registradas en una base de datos, es posible ubicar y supervisar al dueño por las cosas que viste, utiliza y lleva"

Desde estos sectores detractores de la tecnología RFID también se hace constar el posible riesgo de llevar encima dispositivos como tarjetas, o incluso la misma ropa que llevamos puesta, junto a lectores ocultos en los almacenes o establecimientos donde accedamos, dando información confidencial y personal sobre nuestra

identidad, preferencias y pertenencias al establecimiento donde nos encontremos en ese momento.

¿Cómo podría ser posible esto?, la respuesta no es complicada, con tags o códigos de barras y un sistema que permita identificar al cliente en la entrada del establecimiento, todo ello integrado con una base de datos donde se encuentren todo nuestro histórico de adquisiciones anteriores.

Realmente es alarmante pero, hasta qué punto no deberíamos también preocuparnos de aquellas llamadas que recibimos por teléfono de compañías con las que nunca hemos mantenido ningún contacto ni interés y ya conocen nuestros datos personales, domicilio y posibles preferencias en los productos que nos ofrecen. O también, a la hora de navegar por internet cuando recibimos anuncios cada vez más personalizados que se ajustan a nuestras preferencias y búsquedas anteriores.

IBM

Por ejemplo respecto a este tema de rastreo en la cadena de suministro, existen numerosos artículos sobre la patente que IBM en 2001 tramitó sobre rastreo e identificación de personas usando artículos con etiquetas RFID (No. 20020165758), en la que se explica de forma detallada la lectura de los números del tag en la caja y posterior almacenamiento en una base de datos. Como fin tiene la identificación precisa de la persona y usarse para la supervisión de los movimientos de esa persona a través del establecimiento u otras áreas.

De esa forma se obtendría un perfil de cada consumidor que ha tenido alguna compra en el establecimiento con los datos almacenados en las cajas registradoras a la hora de pagar como se indica anteriormente y creando una base de datos de movimientos, en la que se asociará cada compra que se haga con el código RFID del producto comprado, creando una información en la que están relacionados el cliente con sus movimientos y los productos consumidos.

Uno de los posibles fines podría ser conocer las tendencias, comportamientos y preferencias de la persona con fines comerciales en las que se pretende saber mejor el comportamiento del cliente y conseguir a fin de cuentas un mayor consumo por parte de éste. A su vez constituye un peligro y riesgo para el consumidor.

Por ejemplo se podrían deducir muchos de sus datos que pertenecen a la privacidad de una persona. Si pensamos por ejemplo en este sistema, y la compra por parte del consumidor de varios artículos relacionados con la mujer, por ejemplo maquillaje y otros productos de este tipo, podríamos deducir fácilmente que es una mujer. O si por ejemplo consta en la base de datos la compra de varios artículos de lujo, o de alto precio, podríamos decir que nos encontramos ante un consumidor con un perfil medio o alto de ingresos.

Como hemos comentado anteriormente puede parecer alarmante, pero actualmente existen campañas en torno al consumidor del mismo tipo pero por otros medios como internet o teléfono, cuyo fin es conocer mejor al consumidor

para inducirlo a un mayor consumo, de hecho es una práctica asumida por parte de la mayoría de los consumidores, son los llamados estudios de mercado.

NCR

La corporación NCR (fundada en 1884 y que formó parte de AT&T durante los años noventa) pertenece al sector de las TIC (empresas y corporaciones dedicadas a las Tecnologías de la Información y Comunicación), especializada en el campo de las industrias financieras y la venta al por menor. Entre sus principales productos se encuentran las cajas o puntos de venta en los grandes almacenes y supermercados, cajeros automáticos, lectores de cheques, tecnología relacionada con el código de barras, bases de datos a gran nivel, además de dedicarse también al mantenimiento de los productos tecnológicos.

Además NCR, tiene una división (Systemedia Corporation RFID) con la que abarca gran parte del mercado de fabricación de etiquetas RFID, adhiriéndose al estándar Gen 2 y los requerimientos establecidos por la EPCglobal.

NCR implementa el desarrollo de extremo a extremo (end to end) de sistemas RFID, siendo a lo largo de los años una de las empresas que ha trabajado en la mejora de lecturas y velocidad en sus operaciones.

La división se centra además en la mejora y eficiencia de la organización dentro de la cadena de suministro y la reducción de costes operativos. Las etiquetas Gen 2 RFID de NCR ofrecen además una mayor capacidad de datos para hacer frente a la demanda de rendimiento y requisitos.

Según las palabras del vicepresidente de ventas y marketing Keith McDonald, “NCR y su Systemedia Division son muy apreciados en el mercado como uno de los participantes clave en el avance de las tecnologías RFID en múltiples industrias” y respecto a los estándares adoptados “Gen 2 Alien requiere etiquetas de alta calidad y consistencia, y estamos seguro de la capacidad de conversión de Systemedia a este respecto”.

Sobre las divisiones creadas en NCR para el desarrollo y soporte de la tecnología RFID podemos concluir que abarca tanto hardware, tags, servicios y software incluyendo soluciones de almacenamiento de datos Teradata, para ayudar en la resolución de problemas empresariales reales, ofreciendo soluciones de consumo, intentando como resultado final tener un producto líder en la industria RFID frente al presente y futuro emprendedor que ofrece.

Cómo vemos NCR ha invertido recursos y esfuerzo al desarrollo, soporte y avance en tecnología RFID. Ahora bien, hace un tiempo, NCR ofreció una lista titulada "50 Ideas para revolucionar la tienda por medio de RFID" con una serie de ideas referentes a la evolución, objetivos y posibles aplicaciones relacionadas con RFID, y que suponen en algunos casos aspectos críticos para la privacidad:

-Idea No. 34 de la NCR: "Con RFID colocadas en las tarjetas de clientes frecuentes que los identifiquen y una base de datos con el historial de compras del mismo, los artículos podrían recibir un precio según las características de la persona que los compre."

-Comentario: Esta idea parece estar al límite de la ley, ya que podría suponer una discriminación ofrecer un precio distinto dependiendo del cliente. Además ofrecer un precio distinto, supone hacer un análisis de los gastos y otros datos privados del consumidor lo que supondría una amenaza grave a la privacidad.

Ley: Según la ley 7/1996 de 15 de enero de la Ley de Ordenación del Comercio (considerando la venta al por menor). No estaría permitida la modificación de los precios de forma particular para cada cliente.

-Idea No. 26 "La información de tarjetas de débito/crédito y de lealtad del cliente podrían colocarse en una sola tarjeta, permitiendo a los clientes aprovechar las promociones y pagar con sólo leer la tarjeta una vez"

-Comentario: en principio puede suponer una comodidad para el cliente, pero también la capacidad de acceder más fácilmente a los datos por parte del vendedor.

-Idea No. 9: “”Las cámaras de la tienda podrían programarse para girar e inclinarse automáticamente para seguir al cliente con mercancía (con etiquetas de RFID) hasta que pague por ella”.

-**Comentarios:** supondría un paso más en los sistemas de seguridad que benefician al comercio. Pero supone ciertos riesgos en la privacidad si se pudieran aplicar fuera del comercio, y supone un seguimiento personal vinculado con la etiqueta RFID que portas en el producto, lo que se encontraría peligrosamente en el límite de invasión de la privacidad. Ya que la compra de un producto podría estar vinculado con el seguimiento monitorizado.

-Idea No. 25: “El recibo estaría “en la etiqueta”, en el sentido de que la información que usualmente aparece en un recibo impreso en papel (y probablemente más información) estaría asociada con el código de RFID del artículo”.

-Idea No 29: “Devoluciones y cambios con recibos digitales”. La idea es que un artículo comprado usando RFID, podría devolverse o cambiarse sin la necesidad de utilizar recibos físicos de papel, debido a que la información que aparece o intercambia en recibos está asociada con la etiqueta RFID.

-Idea No. 32 “Precios dinámicos. La RFID puede utilizarse junto con rótulos electrónicos en las repisas para automatizar los precios, según el número de artículos que quede en las repisas…. Por ejemplo… cuando ciertos artículos tuvieran existencias bajas (por ejemplo, en Navidad) el precio podría aumentarse automáticamente.”

-**Comentario:** Al igual que otras mejoras, supone un beneficio en cuanto al comerciante, pero para el consumidor supone una desventaja, sería la regla de oferta y demanda llevada al extremo del tiempo real.

-Idea No. 37: “Si un comprador tuviera asuntos pendientes que resolver con la tienda (por ejemplo, un video no devuelto o con fecha temprana de devolución, o un pago pendiente, el comprador podría recibir un recordatorio automático al entrar a la tienda. Esto podría hacerse por medio del teléfono móvil…si ese

dispositivo tuviera una etiqueta de RFID que identificara al comprador, o si el comprador llevara una tarjeta de comprador frecuente con etiqueta de RFID y la tienda tuviera disponible la información de contacto móvil del cliente."

-**Comentario:** en principio podría suponer una intromisión en la privacidad del consumidor. Pero mi observación es que los comercios disponen de otros métodos desde hace tiempo para llevar a cabo este seguimiento. Siempre que no se sobrepase su uso, me parece paralelo al que se hacen con simples bases de datos.

-Idea No. 41: "Advertencias sobre ingredientes a los que un comprador o miembro de la familia es alérgico o desea evitar. Si los alimentos o ropas están marcados con una etiqueta RFID que proporcione información de los ingredientes y materiales que componen el artículo, los compradores podrían recibir advertencias sobre aquellos a los que ellos o algún miembro de su familia fuera alérgico al colocarlo en sus carritos/cestas de compras equipados con lectores de RFID. Esto podría hacerse con software que comparara el contenido de los artículos seleccionados con los perfiles preparados para los compradores.. Un sistema inteligente… podría sugerir alternativas que carecieran de los componentes problemáticos e indicarle al comprador donde hallarlos."

-**Comentarios:** aunque aparentemente en beneficio del consumidor, es una forma más de hacer eficiente el servicio al consumidor, mejorarlo, y por tanto aumentar beneficios. Supone una intromisión en la privacidad del sujeto, ya que su salud, no debería ser accesible mediante un dispositivo electrónico, si el consumidor no lo decide así.

ISOGON CORPORATION

A continuación vemos otro uso en la cadena de suministros que utiliza como herramienta los sistemas RFID, y que podríamos decir, se sitúa en el límite de la privacidad del usuario.

La idea fue de Robert Barritz, presidente ejecutivo de la empresa Isogon Corporation, (que más tarde compró IBM por 250 millones de Dólares). El motivo para utilizar RFID, es que tras hacer estudios a lo largo de los años, en envío de catálogos a domicilio se descubre que entre un 80% y un 90% van directamente a los deshechos sin siquiera ser abiertos. El problema para los vendedores es que no pueden determinar quién abre y quién no el catálogo. Por ello Robert Barritz ideó una forma para determinar si un catálogo o un envío habían sido leídos. Todo esto se recoge en la patente 6,600,419 en Estados Unidos.

Más específicamente en la patente se explica cómo se asigna un número de identificación unívoco a cada hogar, y se fija en una etiqueta RFID que va unida al catálogo o envío. La etiqueta va unida a un interruptor que cuando el catálogo es abierto se desactiva la etiqueta, deja de emitir señal, y resulta ser la forma para diferenciar las que han sido abiertas de las que no. Por lo que todo envío no aceptado, o no abierto, será posible detectarlo mediante un lector RFID.

Comentario: en primer lugar, esta patente ofrece una buena idea, pero con una solución parcial, de esta forma solo puede conocerse si un catálogo ha sido abierto o no de su envoltorio, pero todavía no será posible determinar si se ha leído o no. El segundo punto que ofrece dudas es el sistema de lecturas, ya que según la potencia de las etiquetas que son rentables para el mercado y las infraestructuras existentes, sería necesario colocar lectores por las casas, o en los basureros.

Como medida regulatoria se debería informar a los receptores de dichos envíos que la publicidad, o catálogos que reciben contienen etiquetas RFID.

INTELLECTUAL PROPERTY CORPORATION

La Corporación de Propiedad Intelectual (Bell South) ha recibido la solicitud de patente que tiene por nombre "Sistema y Método Para Utilizar Etiquetas De RF Para Recopilar Datos De Recursos Postconsumo". La idea según sus solicitantes es localizar materiales que puedan ser aprovechados para su reciclaje una vez desechos, pero podemos entender el potencial que tiene un método así de localización, y la cantidad de datos extraíbles que afectan a la privacidad de los consumidores. Realmente es un punto conflictivo si analizamos los datos que más tarde se podrían procesar, archivar, utilizar y obviamente vender para su uso.

La información sobre los productos relativa al tiempo de vida desde que son comprados hasta que acaban siendo reciclados o en los deshechos podría ser de enorme valor para algunos tipos de vendedores como los mercados, industria farmacéutica, por ejemplo.

Comentario: Como ocurre en la mayoría de los casos expuestos, uno de los mayores problemas de todas estas ideas es que actualmente resulta todavía bastante costoso llevarlas a cabo, pero tienen un gran potencial, y deben ser tomadas en cuenta porque afectan directamente a la privacidad, y podrían modificar y afectar al mercado de forma importante, siendo desde mi punto de vista y desde la privacidad del usuario y consumidor una situación de desventaja.

FLINT INK y TIME Inc.

La empresa fabricante de tinta, es una de las que cuenta con más peso en esta industria en el mundo, y desde hace tiempo se conoce que está investigando y desarrollando etiquetas RFID y antenas de tinta conductora que no puedan ser diferenciadas del resto de la tinta de las revistas que publican.

La empresa publicadora de importantísimas revistas como TIME o Reader´s Digest (Time Inc.), también está interesada en hallar una forma de incluir sistemas en sus revistas para lograr datos y estudios sobre la lectura de sus productos, rastrear comportamientos y otros datos de interés.

Comentario:

Llama la atención como las corporaciones y empresas tienen un especial interés en conocer en profundidad el comportamiento del consumidor respecto a sus productos a veces sin importar los límites éticos y morales, y parecen ver en RFID gracias a su potencial de identificación y diferenciación de otros sistemas, un sistema perfecto para estos fines.

Una vez más el único límite para estas prácticas es el coste y la falta de infraestructuras para llevarlas a cabo, indiscutiblemente a medida que siga creciendo la tecnología estas prácticas se harán mucho más habituales. En este punto juegan un papel importante los gobiernos y grandes corporaciones, ya que si ven un uso que pueda ser compensado, cada vez irán avanzando más en estas infraestructuras.

OTROS USOS RELACIONADOS CON LA CADENA DE SUMINISTROS Y CON RIESGO PARA LA PRIVACIDAD DEL CONSUMIDOR.

A continuación se presentan algunos posibles usos de los sistemas RFID que podrían usar un vacío en la privacidad y seguridad de estos sistemas.

-La conocida empresa de farmacéuticos Pfizer dio a conocer que usa RFID en envases del medicamento Viagra, para luchar contra el uso de medicamentos falsos de este tipo, que se venden por varios medios incluyendo Internet.

Comentario: al margen del tipo de medicamento con el que se utilice, supone un uso con riesgo para la privacidad del paciente. Con un lector debidamente capacitado podría saberse que personas usan un determinado medicamento, y eso pertenece exclusivamente al ámbito privado de cada persona.

- Según algunas organizaciones, existe un riesgo en el uso de etiquetas RFID en los productos que compramos, y los programas lectores de RFID accesibles al público en general. Podría suponer una herramienta para delincuentes que rastrearían a potenciales víctimas que acaban de adquirir un artículo de lujo, o simplemente del interés del ladrón.

Comentario: hasta cierto punto es un riesgo real, ya que existen aplicaciones para teléfono móvil que son capaces de leer etiquetas y como vimos en una noticia, algunos expertos informáticos han logrado duplicar tarjetas con dispositivos parecidos y accesibles para todo tipo de público.

- Hay asociaciones que ven un riesgo general en el uso de lectores móviles , tales como las aplicaciones en teléfonos móviles. Ven un riesgo real en cuanto a rastreo de documentos y otros objetos de ámbito privado

Comentario: los documentos oficiales, o con información muy confidencial contienen mecanismos de seguridad que estarían preparados en principio para evitar este tipo de ataques.

5.1.2.2. RIESGO EN LA PRIVACIDAD, ACCIONES Y PRÁCTICAS POR PARTE DE GOBIERNOS

Como herramienta incipiente, RFID presenta numerosos usos futuros además del mundo del comercio y especialmente la cadena de suministros como hemos visto.

La identificación por radiofrecuencia se presenta como un modelo a tener en cuenta por parte de los gobiernos e instituciones.

A continuación se plantean los usos que se están dando por parte de algunos de ellos, futuros proyectos, siempre analizando el riesgo de la propia tecnología y el uso desde el punto de vista de la privacidad del usuario.

Como es previsible, los gobiernos ven una herramienta muy útil en este modelo de identificación, gracias a las cualidades de la radiofrecuencia, de las cuales, las más interesantes para este fin, serían el alto volumen de datos que puede almacenarse en las etiquetas, y el modelo de lectura, además de la facilidad, rapidez y capacidad de los lectores a distancia.

Centraré especial atención en el uso de esta tecnología en pasaportes y algunos de los ataques recibidos.

RFID EN PASAPORTES

Ilustración 7: Símbolo Pasaporte RFID

Los pasaportes que incluyen RFID son denominados epassport o e-pasaporte. Este tipo de pasaporte físicamente se caracteriza por combinar papel y contener información electrónica. La etiqueta que incorpora suele situarse en la contraportada y en la página central del documento de identidad.

Los detalles son tomados del documento 9303 de la Organización de la Aviación Civil Internacional (ICAO).

La información crítica y privada que identifica a cada individuo se encuentra en el microprocesador e impresa en la página principal del documento.

Como modelo de seguridad utiliza el sistema de clave pública (PKI) como método de autenticación de la información contenida en el microprocesador.

Este tipo de pasaporte es conocido como Biométrico. El campo de la biometría aplicado y estandarizado para este tipo de identificación, usa los métodos de reconocimiento facial, huella dactilar y de iris. Los tipos de identificación anteriores fueron adoptados tras evaluar varios tipos, incluido el reconocimiento de retina.

El ICAO es la institución encargada de definir el formato de los datos manejados y protocolos a seguir para el establecimiento de contacto entre lectores y receptores de datos biométricos.

Las características técnicas de los datos y componentes:

- Los perfiles biométricos son almacenados como imágenes digitales en formato JPEG o JPEG2000
- Memoria EEPROM con un mínimo de 32 kilobytes.
- Interfaz adecuada al estándar internacional ISO/IEC 14443 (la principal característica de estos estándares es la compatibilidad entre la utilización de distintos países y proveedores de pasaportes como principal objetivo).

Sistemas de protección de la información:

- Sistema aleatorio de números de identificación del microprocesador. Su función es evitar prácticas como el trazado de los microprocesadores, mediante su rastreo. Al enviar un número distinto cada vez no es posible para un atacante determinar el recorrido que éste hace.
- Protección del canal de comunicación entre el microprocesador y el lector , con cifrado de datos incluido. Además se utiliza una clave correctamente proporcionada por el lector para poder acceder a la lectura de datos. En principio un atacante no podría tener facilidad de acceso a la "escucha" si no tiene la clave correcta. A estas medidas se las denomina Control de Acceso Básico (BAC), más adelante se realiza una visión más completa.
- Autenticación Pasiva (PA). Es un mecanismo de defensa para evitar la manipulación y modificación de los datos contenidos en el pasaporte.
- Hay un fichero auxiliar en el que se guardan los valores hash y una firma digital de los archivos almacenados tales como la imagen, la huella y demás datos biométricos de primer nivel de confidencialidad. La firma digital se realiza usando una clave de firma del documento que a su vez es firmado por una clave del país.

La finalidad de estas medidas es detectar datos en el microprocesador corruptos, que hayan podido ser modificados por alguna razón entre las que puede estar un

ataque malintencionado. El lector que se ponga en contacto con el pasaporte deberá comprobar que la firma digital del pasaporte se genera por un país de confianza, para ello necesitará acceso a las claves públicas del país.

Otras de sus características:

- Para evitar la clonación de los microprocesadores del pasaporte se usa opcionalmente dependiendo del modelo de pasaporte Autentificación Activa (AA). Además contiene una clave privada que no puede ser leída ni copiada.
- Para proteger y autenticar el microprocesador y el terminal encargado de realizar la lectura se usa un protocolo conocido como Control de Acceso Extendido de forma opcional (EAC). Este protocolo se utiliza normalmente para la protección de huellas dactilares e iris. En la Unión Europea se comenzó a usar en algunos pasaportes a partir del 28 de junio de 2009.
- Métodos físicos de seguridad ante ataques. En Estados Unidos se usa una protección metálica muy fina en forma de malla para evitar lecturas o intentos de ataque cuando el pasaporte está cerrado actuando a modo de escudo.

Ataques:

- Características no detectables.
- En 2008 en la universidad Radboud sin conocer la clave determinó de qué país era un pasaporte. La forma de conseguirlo fue mediante el mensaje de error que devolvía el modelo de cada país al intentar leer indebidamente el dato biométrico que pertenece a la huella dactilar. Si se obtienen todos los mensajes de error resultantes se puede determinar donde se encuentra un microprocesador.
- Control de acceso básico (Basic Access Control BAC).
- En el año 2005 Marc Witteman muestra que los números identificativos de documento son seguros. En el año siguiente 2006 Adán Lauire creó un

programa que prueba todas las claves conocidas del pasaporte dentro de un rango dado. Por medio de los sitios en línea de reserva de vuelo, los billetes del vuelo y más información pública de este tipo existe la posibilidad de reducir el número de posibles claves.

- Autentificación pasiva (Passive Autentification PA).

Lukas Grunwald demostró que se pueden copiar datos fácilmente del microprocesador de un pasaporte biométrico en una tarjeta inteligente estándar de ISO/IEC 14443, utilizando para ello una interfaz sin contacto estándar de la tarjeta y para la transferencia de datos una herramienta simple. El pasaporte utilizado para sus ataques no tenía autentificación activa, con seguridad anti-reproducción y no modificó los datos, teniendo como objetivo no cambiar la firma criptográfica del microprocesador original, que es la válida.

Dos años más tarde en 2008 Jeroen van Beek descubrió que no todos los sistemas encargados de inspeccionar el pasaporte comprueban la firma criptográfica de los pasaportes. Llegó a esta conclusión modificando algunos datos copiados del microprocesador original, y como firma utilizó una propia de un país inexistente, lo que debería tener como resultado que el sistema de identificación advirtiera el cambio. De forma contraria a lo esperado, no se detectó esta modificación por lo que se demuestra que algunos sistemas no comprueban la firma. Además para comprobar las firmas conocidas de los países se puede usar una base de datos central, la cual es utilizada solamente por cinco países fuera del área propia. Este ataque es de los más llamativos, ya que en los datos falsos que modificó en el pasaporte, incluyó una identidad falsa con foto incluida, fingiendo pertenecer a la desaparecida figura musical Elvis Presley, y lo más grave, siendo identificado correctamente como un pasaporte de Estados Unidos.

Vídeo: https://www.youtube.com/watch?v=0u4pg_XwNk8

- Autentificación activa (Active Autentification AA)
- Utilizando algunos métodos de rastreo de clave y análisis en 2005 Marc Witteman demostró que la clave privada secreta utilizada en la autentificación puede ser recuperada. Esto en resumen puede permitir a un

usuario malintencionado copiar los microprocesadores del pasaporte que tienen esta forma de autentificación y son susceptibles de ataque.

- Más tarde en 2008 Jeroen van Beek probó como los mecanismos de seguridad opcional pueden ser inutilizados eliminando su apariencia en el fichero correspondiente al índice del pasaporte. De esta forma tan fácil un atacante puede eliminar por ejemplo los ficheros que pertenecen a la seguridad del pasaporte tales como los que permiten la anti-reproducción (autentificación activa).
- Control de acceso extendido (Extended Acces Control, EAC)

En 2007 Luks Grunwald demostró cómo se podía inutilizar un pasaporte con Control de acceso extendido activado. Se pueden modificar algunos parámetros como las fechas de bloqueo de acceso.

POSICIONES EN CONTRA

Los organismos y personas que están en contra de este tipo de pasaporte, lo hacen principalmente porque creen que supone un riesgo para la libertad civil de cada individuo, y también sobre la falta de información respecto a los microprocesadores utilizados en ellos. Todas estas protestas se fundamentan en una base, la tecnología RFID utilizada para transferir la información contenida en el documento, lo que supone un riesgo y vulnerabilidad a tener en cuenta según estos grupos. Cómo hemos visto, que un pasaporte contenga tecnología RFID permite mejorar el acceso a datos a distancia, pero también podría suponer el acceso a ella por parte de usuarios no autorizados de forma malintencionada. Esto unido a la información completamente confidencial contenida en los documentos de identidad puede ocasionar riesgos graves para los ciudadanos.

Según algunos medios de comunicación como BBC se refleja la protesta de algunos expertos, concretamente, aseguraban en 2006 que muchos expertos en seguridad en la mayoría de países donde se utilizan pasaportes biométricos, estaban muy

alarmados debido a que no consideran segura la utilización de identificación por radiofrecuencia en pasaportes.

En palabras de un especialista en seguridad, afirmaba, que el procedimiento no está bien diseñado ya que primero debería realizarse la lectura, más tarde el análisis de los datos obtenidos, y por último la comprobación y verificación de su origen y veracidad de contenidos, de forma contraria a como se hace, primero comprobando el origen, y más tarde accediendo y leyendo los datos. Asegura que no es la mejor forma de aportar el mayor nivel de seguridad a un proceso tan delicado.

Se añadía la que se supone ha sido la posición de FIDIS (Future of Identity in the Information Society), un grupo de expertos en identificación de la red en la sociedad de la información. Esta agrupación de expertos financiada por la Unión Europea en el campo de las TIC (Tecnologías de la Información y Comunicación), que según parece son bastante críticos con el uso de estos ePassport afirman que "los países europeos han forzado a los ciudadanos a usar unos pasaportes que disminuyen de forma drástica la seguridad y aumenta notablemente el riesgo de un posible robo de identidad".

Los científicos especializados en seguridad indican que no solo los ciudadanos sospechosos son la amenaza contra estos sistemas de identificación. Dirigen sus dudas hacia sistemas de verificación poco fiables, organizaciones gubernamentales corruptas o las naciones que hacen un mal uso de los sistemas electrónicos pudiendo permitir fallos en la seguridad. Por ello existen estudios sobre estos temas pero todavía sin ejecutar sobre pasaportes.

MODELO DE EPASSPORT EUROPEO Y ESPAÑOL

Con el fin de acabar con los fraudes por papel, la Unión Europea decidió adoptar el modelo biométrico, incluyendo la imagen digital y la imagen de la huella dactilar. Respecto a los modelos más antiguos de papel, supone un avance muy considerable en seguridad. La Comisión Europea fue la encargada de establecer los

parámetros técnicos de estos pasaportes. Entre los modelos europeos existen diferencias, por ejemplo en Alemania y Rumania se incluyen dos huellas dactilares en vez de una. Un dato relevante es que solo los Países Bajos tienen centralizadas todas las huellas dactilares incluidas en los pasaportes. Según la normativa europea, solo se obliga a incluir en el documento una huella dactilar. Relacionado con todo esto, el responsable de la supervisión en Europa de la protección de datos indicaba sobre el marco jurídico que "no puede abordar todos los posibles problemas relevantes ocasionados por los fallos o imperfecciones inherentes a estos sistemas biométricos".

En España este modelo de pasaporte está siendo usado desde el 28 de agosto de 2006 con un precio de 25,50 € (Mayo de 2013), incluyendo la huella dactilar de ambos dedos índices y con una caducidad de 5 años.

PERMISOS DE CONDUCIR

Según explica el propio departamento de seguridad de los Estados Unidos de América en los documentos de conducir se incluye un sistema de identificación RFID. El documento no es un simple documento que acredita a un ciudadano como conductor sino que además es un documento de identidad. Sirve como documento de acceso al país desde Canadá, México o el Caribe desde el medio que sea (tierra o mar), sin incluir el aéreo.

Justifican la utilización de RFID como un medio de hacer más fácil el cruce de la frontera.

El principal uso es como modo de envío de los datos biométricos incluidos en el documento, y la capacidad de un oficial de la frontera de poder visualizar y disponer de estos datos cuando un ciudadano se aproxime a su puesto.

Además como medida de seguridad, en el caso de que el sistema de identificación por radiofrecuencia no esté disponible, incluye un código de barras con la misma información.

PROTECCIÓN PRIVADA

Desde la agencia, aseguran que el sistema RFID solo incluye un número de identificación que une la identidad con los datos almacenados en la base de datos del Department of Homeland Security.

Como medidas extras de seguridad los portadores del documento reciben un manual de protección, transporte y uso de la licencia, aparte de un blindaje especial para evitar la lectura a distancia por parte de usuarios malintencionados.

De forma parecida al pasaporte, este modelo de identificación es un documento oficial de identidad, y ha levantado ciertas alertas por riesgos de privacidad. Como vemos se ha añadido un modo de seguridad física (el blindaje), pero la mayor preocupación es crear una legislación ajustada a este tipo de riesgos y posibles ataques.

SANIDAD

El uso más generalizado en el campo de la asistencia sanitaria se encuentra sobre todo en los hospitales. Es una aplicación que se encuentra actualmente en proceso de implementación en este sector y que permite utilizar los sistemas RFID para tareas como el seguimiento activo de partes del mobiliario o instalaciones como pueden ser las camas o los contenedores. Pero las más interesantes son las que tienen como fin identificar a los pacientes para un control más detallado de los medicamentos, o por ejemplo aumentar el seguimiento y la seguridad sobre pacientes de mayor riesgo o que necesitan más cuidados, por ejemplo los bebés y pacientes con enfermedades como demencia.

Otras aplicaciones relacionadas con la sanidad pueden ser las relacionadas con las tarjetas de seguro por ejemplo ya introducidas en Méjico, en las que figuran datos como el nombre del usuario incluyendo información relacionada con el paciente, es decir medicamentos indicados y con el que paciente se ha tratado o lo hace en la actualidad, todo ello incluido en la memoria del chip RFID.

5.1.2.3. RIESGO EN LA PRIVACIDAD, ACCIONES Y PRÁCTICAS POR PARTE DE INSTITUCIONES Y ASOCIACIONES EMPRESARIALES.

Ejemplos de posibles riesgos y hechos que han levantado las alarmas de los grupos contrarios al uso que suponga cualquier riesgo contra la privacidad:

Los expertos se unen a la oposición presentada por CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) contra el uso de RFID en colegios como medio de rastreo.

El rastreo tecnológico es "deshumanizante" y amenaza la privacidad y las libertades civiles según defienden estos grupos.

Sus protestas se deben al incipiente uso de RFID en colegios, como ocurre en San Antonio´s Northside Independent School, donde estaban probando su uso en dos campus en Agosto del 2012. En los colegios Jay High School y Jones Middle School dicen que exigirán a los estudiantes participar en el nuevo sistema de seguimiento que tiene como fin aumentar los ingresos perdidos a causa de las ausencias.

La principal preocupación de las protestas se basa en el número de identificación que contienen los chips, asegurando que se asemeja a un número de Seguridad Social para cosas. El temor a ser rastreado se basa en la capacidad de identificación de forma invisible y silenciosa de las etiquetas que pueden adjuntarse a todo tipo de pertenencias y objetos.

El plan del colegio San Antonio Northside Independent School es incorporar etiquetas RFID en las tarjetas de identificación de los estudiantes, de forma parecida a la incorporación de tags en los uniformes de los estudiantes de un colegio en Brasil. El objetivo en ambos casos es mantener la seguridad entre los estudiantes, profesores y el personal mediante una vigilancia constante.

Desde la dirección de CASPIAN protestan debido a que aseguran que RFID es usada para rastrear y tener inventario de los animales de granja, además, opinan que en los colegios se debería educar y enseñar a los alumnos como participar en una

sociedad de democracia libre, no condicionándolos y rastreándolos como ganado, y dicho esto instan a las protestas y demandas por parte de los ciudadanos.

-Algunas tarjetas de acceso a empresas incorporan una etiqueta RFID, lo cual lleva al control por parte de la empresa sobre los tiempos de trabajo, descansos, conversaciones con otras personas, o el tiempo que ha permanecido un empleado en el cuarto de baño.

-Comentario: hasta ahora no hay legislación que lo prohíba, y si la empresa decide exigir este tipo de identificación y el empleado lo acepta, no hay ningún tipo de práctica ilegal. Son comprensibles las consecuencias que pueden tener un excesivo control y el uso controvertido que puede tener una herramienta así.

5.1.2.4 OTROS RIESGOS ASOCIADOS A LA PRIVACIDAD

A continuación se enumeran los riesgos y amenazas más destacables relacionados directamente con el entorno de la privacidad en los sistemas de identificación por radiofrecuencia.

ROBO DE IDENTIDAD

Este tipo de amenaza aparece directamente mencionado en otros capítulos y es especialmente importante cuando se ve involucrado con temas tan importantes como documentos personales tales como el pasaporte.

Es una forma de fraude en la cual una persona pretende hacerse pasar por otra asumiendo su identidad. Normalmente el objetivo es acceder a recursos de cualquier tipo (materiales o informativos), también para obtener crédito de algún tipo haciéndose pasar por la persona suplantada y otros beneficios. Las víctimas de robo de identidad (se refiere a la persona a la cual su identidad ha sido asumida por el ladrón) pueden sufrir consecuencias muy adversas si él o ella son directamente responsables de las acciones del autor. Tanto las organizaciones como los individuos que son defraudados o suplantados a consecuencia de un robo de identidad también pueden sufrir consecuencias adversas y pérdidas, por lo que pasan a ser directamente víctimas de esta amenaza.

CREACIÓN DE PERFILES SIN CONSENTIMIENTO DEL USUARIO

También hemos hablado de los riesgos que puede arrastrar esta tecnología, debido al seguimiento con fines comerciales, sirviéndose de los atributos y capacidades de esta tecnología, para crear un patrón de comportamiento en el cliente, algo que está completamente reñido con su privacidad.

Existen perfiles anónimos que se utilizan en el comercio minorista de ventas específicas y publicidad, pero lo que verdaderamente supone una amenaza son los perfiles creados en torno a los usuarios con el fin de hacer un seguimiento personalizado y así conocer sus preferencias con múltiples fines, lo que supone una intrusión en el campo de la privacidad.

RASTREO

Esta es una amenaza directamente ligada a la privacidad del usuario. Tal como se ha comentado en anteriores apartados, el sistema basado en lectores y etiquetas, unido al potencial de las ondas de radio, hace de estos sistemas una herramienta muy potente, eficiente y rápida en el campo de la identificación, pero al mismo tiempo supone posibles riesgos como este. Los lectores, si son colocados en lugares o zonas estratégicas pueden grabar, y hacer el seguimiento de etiquetas que contienen identificadores que son asociados a identidades reales de personas. El problema real es cuando este rastreo se produce de manera involuntaria por parte del rastreado. Generalmente los sujetos que están bajo esta práctica deberían ser conscientes y tener notificación de ello, pero no siempre es el caso.

La diferencia con los teléfonos móviles por ejemplo, es que estos dispositivos no siempre son accesibles, y además necesitan de un consentimiento por parte del usuario generalmente mientras que las etiquetas RFID suelen ser susceptibles de lecturas y rastreos involuntarios por parte del individuo que lo porta.

EXCLUSIÓN DEL SUJETO/PROPIETARIO EN EL PROCESO DE LA DESHABILITACIÓN DE DATOS EN UNA ETIQUETA RFID

Esta amenaza está relacionada con los procesos específicos que están directamente relacionados y dependen directamente del estado activo de la etiqueta para poder tener accesos.

Por ejemplo, una práctica que se puede llevar a cabo es restringir la capacidad de los consumidores para devolver un artículo si no tiene habilitada la etiqueta.

CONEXIÓN DE INFORMACIÓN Y DATOS

Existe la posibilidad mediante diversas formas de que la información relativa a la conducta y otra información no directamente personal pueda ser conectada de alguna forma para derivar información persona.

Esta amenaza está referida a los casos donde los datos de los sistemas RFID una vez recogidos y procesados pueden de alguna forma relacionados con información la cual podría ser usada para llegar o derivar información privada y personal.

INSTRUCCIONES Y PROCEDIMIENTOS NO CONTROLADOS

El procedimiento correcto para el uso de datos debe ser consentido por el usuario desde el principio. Un problema que se presenta respecto a esto, es que el usuario se convierte en portador de dispositivos RFID, pero en muchas ocasiones no existe una interfaz disponible para ellos, por eso es necesario definir desde un principio la finalidad de los datos que se van a manejar. Cuando las etiquetas son usadas pasado el propósito inicial, los datos y la información pueden ser conectados, y la información privada y personal puede ser así utilizada de una forma incorrecta.

MINERÍA DE DATOS Y VIGILANCIA A LARGA ESCALA UTILIZADA INAPROPIADAMENTE

Esta amenaza se refiere a los casos donde un número significativo de artículos llevan etiquetas y donde las etiquetas son usadas para recoger datos en numerosos contextos. Los datos de varios sistemas RFID pueden ser agregados derivando información personal.

La combinación de sistemas RFID podría utilizarse también teniendo como resultado la capacidad de crear perfiles y hacer el seguimiento como resultado de la vigilancia.

5.2.CONTROL LEGISLATIVO

Como cualquier actividad relacionada con el comercio, en la que está involucrada la economía, y además afecta a los ciudadanos, la tecnología RFID y sus aplicaciones deben estar reguladas por un marco legal. Existen ciertos aspectos relacionados directamente con estos sistemas, por ejemplo es el caso de las frecuencias permitidas en las que operan los dispositivos, o la criticidad de los datos privados de usuarios que en ocasiones manejan, que nos indican la necesidad de una regulación legislativa que controle las normativas y usos de RFID.

Hay que tener en cuenta aspectos como los diferentes matices legislativos dependiendo del país donde este encuadrada la actividad de dichos sistemas.

Para hacer una explicación más clara de las leyes que afectan a los sistemas RFID, se tendrán en cuenta los siguientes aspectos:

- Seguridad relacionada con la criticidad de datos en cuanto a privacidad.
- Los rangos de frecuencias, aspecto que varía de unos países a otros, a veces condicionado por la utilización con fines militares.

5.2.1 LEGISLACIÓN RELATIVA A DELITOS INFORMÁTICOS

Si atendemos a la definición dada por la OCDE (Organization for Economic Co-operation and Development) elaborada por los expertos en la reunión de 1983, se entiende como delito informático el comportamiento antijurídico, no ético que no está autorizado, y que incluye todos aquellos procesos automatizados de datos y los procesos de transmisión de estos.

Como sabemos, asociados a las ventajas que proporcionan los sistemas de información, existen los conocidos "delitos informáticos". Realmente la tecnología en sí no supone una amenaza para la sociedad, lo que realmente supone un problema y un riesgo, es el grupo de personas o individuos que tienen prácticas malintencionadas relacionadas con las actividades que estas tecnologías llevan a cabo. Es fácil observar que conforme avancen los sistemas y su sofisticación, valores como la privacidad y la probabilidad de ser utilizados con un mal fin se agravarán.

Es por esto que es necesario tener un marco que regule este uso y sus posibles usos delictivos, para ello debe existir una cohesión entre el punto de vista penal, también civil o comercial, y por otra parte podría incluirse el derecho administrativo. Es necesario tener bien regulado y desde el mayor número de campos legales para poder ofrecer una eficaz defensa y protección hacia los delitos informáticos. Específicamente en los sistemas RFID es especialmente crítico y por tanto a tener en cuenta el campo de la privacidad y todo lo relacionado con los usuarios y consumidores finales, como hemos explicado en los capítulos anteriores pueden ser muy vulnerables si se da un uso incorrecto a esta tecnología.

5.2.1.1 HABEAS DATA

Con el fin de proteger a los usuarios de los posibles usos malintencionados específicamente de delitos informáticos en este caso por medio de sistemas de identificación por radiofrecuencia, existe un recurso legal denominado Habeas Data que está a disposición de todo individuo con acceso a un registro de datos sobre el propio individuo.

El verdadero riesgo no reside en los propios sistemas y partes de los mismos que lo forman sino en los posibles usos malintencionados como la manipulación e individuos dispuestos a hacer dicho uso de los datos confidenciales y privados.

La fecha que se podría marcar como punto de partida real en el comienzo de la reglamentación y expansión en el ámbito de normas de protección de datos personales sería el año 1994.A partir de este año se asigna a los Ministerios del Estado el control sobre este conjunto de normativas, leyes y normas, recayendo sobre ellos el control del uso que hacen las empresas e individuos de los datos personales. En España actualmente se aplica esta medida.

Más específicamente en España la ley en la que se reconoce el derecho de Habeas Data y protección de datos personales es la *Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal*.

La importancia de este recurso es que el individuo tiene derecho a la modificación y corrección de los datos si éstos tienen algún efecto perjudicial o son erróneos.

5.2.1.2 LEGISLACIÓN REGULATORIA DE FRECUENCIAS EN EUROPA

Por el momento no existe una corporación pública que globalice la regulación y administración de los estándares relativos a las frecuencias que deben ser utilizadas en RFID por lo que pertenece a cada país la fijación de las reglas y rangos.

Las principales corporaciones que se dedican a la asignación de frecuencias y su administración en Europa son las siguientes:

ERO (European Radiocommunications Office)

Fundada en 1991 y situada en Copenhague (Dinamarca).

Sus principales funciones son las siguientes:

- Proporcionar un centro especializado que actuará como punto central.
- Identificar áreas donde existan problemas, y nuevas posibilidades en el campo de la radio y telecomunicaciones
- Elaborar planes a largo plazo para el uso del espectro radioeléctrico en toda Europa.
- Apoyar y colaborar con las autoridades nacionales de gestión de frecuencias
- Llevar a cabo consultas sobre los temas o partes del espectro de frecuencias específicas
- Publicación de Decisiones y Recomendaciones, llevar un registro de su aplicación
- Identificar y promover las mejores prácticas en la administración de los regímenes nacionales de numeración y procedimientos de asignación de número.
- Asesoraral ECC (Electronic Communications Committee)
- Dar soporte permanente al Electronic Communications Committee (ECC)
- Publicación y distribución de las decisiones y recomendaciones del ECC.

ECC (Electronic Communications Committee)

Este organismo es el encargado de formar un comité regulatorio de la CEPT (European Conference of Postal and Telecommunications Administrations)

Sus funciones:

- Desarrollo de políticas de radiocomunicación y la coordinación de frecuencia.
- Tareas relacionadas con la regulación, asignación y utilización de frecuencias que van de los 9 KHz a 275GHz

ETSI (European Telecommunications Standards Institute)

Fundado en 1988 es el encargado principalmente de elaborar las bases de consenso en los estándares de telecomunicaciones de los países miembros.

Atendiendo a los estándares europeos podemos advertir los siguientes puntos:

- En comparación al utilizado en Estados Unidos, la banda de UHF utiliza muy baja potencia, ancho de banda y ciclo de transferencia.
- La regulación vigente de UHF permite un rango máximo para los lectores de potencia de transmisión de 500 mW en la banda de 200 kHz
- En las últimas recomendaciones el incremento de ancho de banda es aumentado en hasta 2 watts de potencia.

Información disponible en documentos EN 302 208 ,EN 300 220

5.2.1.3 LEY ORGÁNICA PROTECCIÓN DATOS DE CARÁCTER PERSONAL

Como queda mencionado en este capítulo el reconocimiento al derecho Habeas Data, queda englobado en la Ley Orgánica de Protección de Datos de Carácter Personal.

Esta ley se divide en varios artículos, algunos directamente relacionados e importantes con los posibles problemas de privacidad relacionados con RFID.

ARTICULO 5

A continuación se mencionan partes del Artículo 5 de esta ley donde se encuentran los procesos a seguir en cuanto al tratamiento de datos privados y personales, directamente aplicables sobre sistemas RFID en los que se manejen este tipo de datos.

"*Artículo 5. Derecho de información en la recogida de datos.*

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante."

En capítulos anteriores hemos hablado de los problemas relacionados con la posible obtención de datos personales no autorizada, y aquí podemos ver como la ley española obliga directamente a informar al sujeto al que pertenecen los datos.

Por tanto en productos que portarán etiquetas RFID y tratarán de extraer cierta información del cliente, obligatoriamente, dicho cliente debe ser informado de forma exacta y precisa, del tratamiento y datos que van a ser utilizados y estudiados, de otra forma se convierte en una práctica ilegal.

ARTICULO 9

Me parece importante prestar atención también al siguiente artículo referente a la seguridad, tratamiento, y requisitos que deben tener los sistemas que den soporte y contengan los datos, incluyendo así los sistemas de identificación por radiofrecuencia.

"*Artículo 9. Seguridad de los datos.*

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

Para que el almacenamiento de datos privados sea legal debe reunir una serie de requisitos mínimos que lo permitan.

ARTICULO 14 y 15

Tal como decíamos al principio del apartado, el derecho Habeas Data queda recogido en esta ley, eso significa que cualquiera tiene derecho a consultar sus datos, lo vemos reflejado en los siguientes artículos:

"*Artículo 14. Derecho de consulta al Registro General de Protección de Datos.*

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho de acceso.

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso al que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes."

5.2.1.4 REGULACIONES SOBRE LOS RANGOS DE FRECUENCIA

Estas son las restricciones aplicadas a los rangos de frecuencia, además de las especificaciones generales, llevadas a cabo para establecer un control y orden evitando así intromisiones en usos del propio estado, como pueden ser los militares.

Baja Frecuencia

Si dividimos las restricciones por rangos de frecuencia, aquellas que se encuentran en el espectro entre 125 - 134 kHz y 140 – 148,5 kHz (low frequency, baja frecuencia) en principio no necesita de licencia alguna para su utilización de forma global.

Alta Frecuencia

Las etiquetas que funcionan en un rango de frecuencia en torno a los 13,56 MHz al igual que las etiquetas de baja frecuencia no se someten a ninguna licencia especial en su uso global.

Ultra Alta Frecuencia

Sin embargo las frecuencias que se encuentran en el rango de 868 y 928 MHz, al contrario que las altas y bajas frecuencias, no pueden ser usadas de forma global debido a que existen distintos estándares, y no hay una unificación general.

Por ejemplo en Norteamérica este tipo de frecuencia puede ser utilizada entre los 900 y 928 MHz, aunque con límites en las energías de transmisión. En Europa sin embargo se puede usar sin licencia el rango que se encuentra entre 869,40 y 869,65 MHz pero también existen limitaciones en cuanto a la energía utilizada para la transmisión.

Podemos ver casos reales de incompatibilidad internacional, es el caso del estándar de ultra alta frecuencia en Norteamérica, no es válido ni aceptado en Francia, porque ese espacio está reservado para uso militar.

El tratamiento de estas frecuencias en China y Japón está sujeto a cada caso particular, teniendo que ser consultado y solicitado a los organismos locales, y con la posibilidad de ser rechazado.

Otras Regulaciones

En Europa existe una regulación sobre los deshechos que afecta directamente a los sistemas RFID. La Waste Electrical and Electronic Equipment , evita que se desechen de forma incorrecta las etiquetas de los sistemas de identificación por radiofrecuencia, más específicamente, se obliga por medio de esta regulación a separar los recipientes y cajas de las etiquetas que lleven incluidas, antes de deshacerse de las mismas.

5.3 CONTROL SOBRE NORMATIVAS

Debido a la cantidad de posibles riesgos que pueden rodear a los sistemas RFID, los organismos oficiales llevan tiempo organizando y aprobando normativas que regulen y minimicen cada vez más estas amenazas.

En lo que a nuestra zona se refiere la Unión Europea ha publicado numerosos documentos y normativas aprobadas ya que se considera importante evitar los posibles riesgos en cuanto a privacidad y seguridad relacionados con los sistemas de radiofrecuencia.

Particularmente en España estamos representados en el ámbito normativo en Europa mediante la ya estudiada Ley Orgánica de Protección de Datos de Carácter Personal.

A nivel Europeo, la Comisión Europea aprobó en 2009 el documento que tiene el siguiente título "Sobre la aplicación de los principios de privacidad y protección de datos en las aplicaciones basadas en la identificación por radiofrecuencia SEC (2009) 3200 final", y en el que quedan reflejadas recomendaciones generales sobre buenas prácticas a la hora de utilizar e implementar sistemas RFID del cual se puede extraer de forma general:

- En primer lugar en los puntos del 1 al 4 se reconoce el creciente uso de RFID, y sus actuales y cada vez más diversas aplicaciones (gestión de equipajes, gestión de pago de peajes en carreteras, sanidad, documentos de viaje, transporte, etc…), posicionándola como una tecnología a tener en cuenta debido a su actual y potencial importancia en el crecimiento económico, y en el mercado laboral.

- En los siguientes puntos, 5, 6, y 7se habla sobre el potencial de las aplicaciones RFID para el uso de datos privados de carácter personal, así como la identificación de objetos o individuos. A consecuencia de ello y de las características de este tipo de comunicación, se debe aplicar el principio de seguridad y privacidad por diseño ('security and privacy-bydesign'), siendo necesarias la percepción y constancia de estas cualidades para que sea aceptada como una opción viable para el uso público y masivo.

- En los puntos 8, 9 del comunicado se hace énfasis en la protección de datos privados, y la recomendación de aplicar los pasos sugeridos por la Unión Europea, reflejados en documentos como 'Radio Frequency Identification(RFID) in Europe: Steps towards a policy framework'.

- Más adelante se habla sobre la importancia de mantener lo más alejado posible del dominio público los datos mediante el uso de seudónimos y datos anónimos, con el fin de preservar lo máximo la privacidad, apoyándose en los acuerdos alcanzados en el 2007 por la Comisión de Comunicación reflejados en "Promoting Data Protection by Privacy Enhancing Technologies (PETs)". En 2006 esta misma comisión habla sobre la necesidad de utilizar razonablemente las certificaciones necesarias y las buenas prácticas en seguridad y privacidad.

- Antes de implementar un sistema RFID es necesario hacer una evaluación del impacto sobre seguridad y privacidad. Esta evaluación deberá ser llevada a cabo para conocer las medidas necesarias a tomar antes y durante el funcionamiento del sistema. Este control deberá ser llevado a cabo durante el ciclo de vida del sistema.

- En el comercio al por menor, deberá proporcionarse la información necesaria para determinar si las etiquetas y la utilización de los sistemas RFID realmente supone o no una amenaza a la privacidad y seguridad del consumidor.

- Desde la Unión Europea se anima a todos los países miembros a adoptar las normativas internacionales que sean compatibles con la Unión Europea tales como las desarrolladas por la Organización Internacional de Normalización (ISO), para garantizar las medidas necesarias en los comercios en que se utilice esta tecnología.

- Requiere dar una atención y tratamiento específico a los sistemas que afectan a gran parte de la población, como pueden ser los billetes usados en transporte público con tecnología RFID, o que incluyen datos críticos como pueden ser biométricos, en el caso de los pasaportes, ya que suponen información potencialmente crítica en el campo de la privacidad para los usuarios.

- Se hace especial énfasis en dar la información sobre el uso pertinente a la población que vaya a utilizar este tipo de sistemas, recayendo esta responsabilidad en las empresas o cuerpos que desplieguen esta tecnología.

- Potenciar el uso de RFID entre las empresas públicas, y las medias y pequeñas empresas (PYME) atendiendo a las capacidades y características que pueden permitir el crecimiento económico y mejorar la industria tecnológica, potenciando además el uso mayoritario y haciendo al mismo tiempo que disminuya el riesgo de ser utilizado por una minoría con fines no deseados.

- Reforzar la investigación y desarrollo en tecnologías de bajo coste, medida necesaria para lograr una mayoritaria adopción de estos sistemas en condiciones aceptables y seguras.

- Además la propia Comisión ofrece su apoyo directo e indirecto por medio de acuerdos y medidas tales como la aprobación por parte del Parlamento Europeo del programa "Competitiveness and Innovation framework Programme (CIP) established by Decision No 1639/2006/EC of the European Parlament and of the Council of 2006", que pretende facilitar el desarrollo y permite un marco mejorado para la innovación y el desarrollo basado en un crecimiento económico equilibrado.

Documentos consultados SEC(2009)3200

ESPECIFICACIONES REFERENTES A COMPONENTES DE UN SISTEMA RFID

En las recomendaciones hechas por la Unión Europea, se encuentran definiciones formales sobre las partes que contienen un sistema RFID:

- Identificación por Radiofrecuencia: Sistema comunicado por ondas de radiofrecuencia con el fin de comunicar datos y la lectura de los datos contenidos en una etiqueta.
- Etiqueta RFID: dependiendo del tipo de dispositivo, es aquel que contiene la capacidad de producir una señal de radio RFID para la lectura de sus datos, o simplemente porta datos y es leída por otro dispositivo.
- Lector RFID: dispositivo de identificación con una frecuencia de ondas electromagnéticas de radio, estimula o produce una respuesta de datos modulados en una etiqueta o grupo de etiquetas.
- Aplicación RFID: programa que procesa los datos mediante el uso de etiquetas y lectores, y que se apoya en un software y en una infraestructura de comunicación en red.
- Operador de aplicaciones RFID: es la persona física o jurídica, autoridad pública, servicio u organismo que solo o conjuntamente determina los fines y los medios de funcionamiento de una aplicación, incluidos los controladores de datos personales a través de una aplicación RFID.
- Información de Seguridad: la preservación de la confidencialidad, integridad y disponibilidad de la información.
- Monitorización: actividad realizada con el propósito de detectar, observar, copiar o grabar la ubicación, el movimiento, las actividades o estado de un individuo.

ESPECIFICACIÓN SOBRE SEGURIDAD E INFORMACIÓN CRÍTICA

El acuerdo incluye los siguientes puntos que deben llevarse a cabo en el uso de sistemas RFID respecto a la información privada que se maneja en ellos:

- Los Estados Miembros deben proporcionar un marco legal para que la industria en colaboración con las partes interesadas de la sociedad civil, pueda realizar una evaluación del impacto en la privacidad y la protección de datos.
- Los Estados deben garantizar que los operadores de acuerdo con la Directiva 95/46/CE, cumplen lo siguiente:

    1. Llevar a cabo una evaluación de las implicaciones de la implementación de la aplicación para la protección de datos personales y la intimidad, incluyendo la posibilidad de si una aplicación podría ser usada para monitorizar a un individuo. El nivel de detalle del estudio debe estar en consonancia con los riesgos detectados para la privacidad.

    2. Con el fin de garantizar los datos personales y la intimidad, deben adoptarse las medidas técnicas y de organización.

- Designar a una persona o grupo de personas responsables de la revisión de las evaluaciones y la adecuación continua de los aspectos técnicos y medidas organizativas con el fin de garantizar la protección de los datos personales y la intimidad.

- Poner a disposición de las autoridades competentes la evaluación, al menos seis semanas antes de la implementación de la aplicación.

- Una vez la evaluación está aprobada y de acuerdo con los puntos anteriores, debe implementarse de acuerdo a esos pasos.

ESPECIFICACIONES SOBRE LA SEGURIDAD DE LA INFORMACIÓN

Se avisa a los Estados Miembros de la necesidad de apoyar a la Comisión Europea, en la detección e identificación de las aplicaciones que pudieran suponer una amenaza para la seguridad de la información, implicando al público en general. Para estos casos los Estados Miembros deben garantizar que los operadores en colaboración con las autoridades nacionales competentes junto a las organizaciones de la sociedad civil, deben desarrollar nuevos planes, o aplicar los ya existentes.

Los planes existentes son las certificaciones aprobadas y compatibles con la Unión Europea, o el operador de autoevaluación como se comentaba anteriormente, con el fin de demostrar que se están aplicando las medidas necesarias de seguridad respecto a los niveles de riesgo resultantes de la evaluación.

Ilustración 8: Símbolo Internacional RFID

ESPECIFICACIONES SOBRE INFORMACIÓN Y TRANSPARENCIA EN USO DE RFID

En conformidad con las Directivas 95/46/CE y 2002/58/CE, los Estados de la Unión Europea deben garantizar que los operadores desarrollan y publican una política de información concisa, precisa y fácil de entender para cada una de sus aplicaciones. La política deberá incluir al menos los siguientes puntos:

a) La identidad y dirección de los operadores
b) Propósito de la aplicación
c) Qué datos deben ser procesados por la aplicación, especialmente si se trata de datos personales, y si la ubicación de las etiquetas será monitorizada.
d) Resumen de la evaluación del impacto sobre la protección de datos y privacidad.
e) Posibles riesgos de privacidad, si los hay, en relación con el uso de etiquetas en la aplicación y las medidas que las personas pueden tomar para mitigar estos riesgos.

Los Estados Miembros deben velar por que los operadores tomen las medidas necesarias para informar a las personas de la presencia de lectores, para ello se tomará como base un signo común en toda Europa elaborado por organismos europeos de normalización, con el apoyo de las partes interesadas. El cartel informador debe incluir la identidad del operador y un punto de contacto para las personas que deseen obtener la política de información de la aplicación.

ESPECIFICACIONES SOBRE APLICACIONES RFID USADAS EN EL COMERCIO AL POR MENOR

A continuación se recogen las recomendaciones y puntos que deben ser llevados a cabo por los comercios al por menor que entre sus actividades y aplicaciones contengan sistemas RFID:

- Una vez creado un símbolo común por los organismos europeos de normalización, con la colaboración de las partes interesadas, los operadores deben informar a las personas y usuarios de la presencia de etiquetas adheridas o incluidas en los productos.

- Mediante una evaluación se debe medir el impacto sobre la protección de la privacidad y de los datos personales. El operador debe determinar si las etiquetas colocadas o incorporadas a los productos vendidos a los consumidores a través de los minoristas que no son operadores directos de la aplicación, representan o no una posible amenaza para la intimidad o la protección de datos privados y personales.

- Se debería proporcionar al cliente o usuario de un minorista la posibilidad de una vez informado sobre la tecnología incluida en su producto y sus posibles riesgos, eliminar o desactivar las etiquetas, o como se indica si después de haber sido informado, lo desea, conservar las etiquetas activas. La desactivación de las etiquetas se entiende como el proceso que detiene las interacciones de una etiqueta con su entorno, es decir no requiere la participación activa de los consumidores. Esta desactivación por parte del vendedor debe realizarse de forma inmediata y sin coste alguno para el consumidor. Además el consumidor debe ser capaz de poder verificar esta desactivación o eliminación.

- La eliminación o desactivación de las etiquetas no será necesaria, si una vez hecha la evaluación de riesgos sobre datos personales, privacidad e intimidad concluyen con que el funcionamiento de la etiqueta tras la venta no supone una amenaza. No obstante, los vendedores deben poner a disposición del cliente una forma sencilla de desactivar los dispositivos incluidos.

- La desactivación o eliminación de las etiquetas no implica la reducción o terminación de las obligaciones legales del minorista y fabricante hacia el consumidor.

ESPECIFICACIONES Y RECOMENDACIONES A LOS ESTADOS MIEMBROS PARA LA SENSIBILIZACIÓN

Estas son las recomendaciones de la Unión Europea a sus Estados Miembros:

- En una acción conjunta entre los Estados Miembros, la industria, la Comisión y otras partes interesadas, se deberían tomar las medidas adecuadas para informar y sensibilizar a las autoridades públicas y empresas, en especial a las PYME, sobre los beneficios y riesgos potenciales asociados con el uso de RFID. Prestando especial atención a la seguridad de la información y aspectos de la privacidad.

- Con el fin de informar y sensibilizar al público en general se recomienda en una acción conjunta entre los Estados, la industria, las asociaciones de la sociedad civil, la Comisión y otras partes interesadas, identificar y dar ejemplos de buenas prácticas sobre la implementación de aplicaciones RFID.

- Además se apoya la adopción de medidas como proyectos piloto a gran escala, para aumentar la conciencia pública sobre RFID, los beneficios, riesgos y las consecuencias de su uso, como requisito previo a la adopción mayoritaria de esta tecnología.

ESPECIFICACIONES SOBRE INVESTIGACIÓN Y DESARROLLO

Desde la Unión Europea se fomenta la cooperación entre los Estados Miembros, la industria, las partes interesadas, la sociedad civil y la Comisión para estimular y apoyar la introducción de la “seguridad y privacidad por diseño” desde una etapa temprana en el desarrollo de las aplicaciones involucradas en el funcionamiento de la tecnología RFID.

5.3.1. NORMATIVA ISO RELATIVA A RFID

En el capítulo 2.5.1 se habla sobre la Organización Internacional de Normalización de forma más general, en esta parte profundizaremos específicamente en las normas que afectan directamente a la tecnología RFID.

Para ello es importante conocer que los fabricantes de sistemas RFID se han basado en estándares que inicialmente fueron utilizados para la fabricación de antiguas tarjetas usadas en el sector bancario, la telefonía y la identificación.

No obstante generalmente los estándares suelen ser creados para unos fines específicos y siempre llevados a cabo por grupos de especialistas, expertos y técnicos en ese campo.

A continuación se citan los estándares referentes a las tarjetas IClass, aquellas que no necesitan contacto y que están directamente relacionadas con RFID y sus normas ISO.

NORMAS ISO DE LAS TARJETAS IClass (IC)

La ISO clasifica las tarjetas IC en tres grupos, llamados grupos de operación

TASK FORCE 1(TF1)

Se las denomina tarjetas de proximidad debido a su modo de funcionamiento. Necesitan estar en contacto o cerca del lector/escritor para poder llevar a cabo la operación para la que ha sido fabricada.

Su uso más frecuente se encuentra entre el transporte debido al tipo de comunicación de contacto o pequeña distancia para la comunicación con el lector/escritor.

Las normas relacionadas con estas tarjetas son las siguientes:

- IS 10536-1: trata sobre los aspectos físicos tales como el perfil de la superficie, métodos de prueba de fuerza mecánica, la temperatura a la que puede operar y la capacidad electromagnética.
- IS 10536-2: sobre las medidas, dimensiones y las áreas de acoplamiento definiendo el rango de dimensiones y los elementos de ensambladura que suministran energía, e importantes aspectos como la transmisión de datos entre lector/escritor y la tarjeta IC.
- DIS10536-3: sobre la señal electrónica y la forma en que intercambian señales, además del proceso de reseteo de la tarjeta.
- CD 10536-4: protocolos de comunicación.

TASK FORCE 2 (TF2)

Este grupo se caracteriza por ser tarjetas de acoplamiento remoto, suponen un avance en la detección de colisiones cuando en el área donde opera el lector se encuentran varias tarjetas.

Sus estándares:

- CD 14443-1 sobre los aspectos físicos
- CD 14443-2 sobre la interfaz de radiofrecuencia
- CD 14443-3 protocolos de transmisión.
- CD 14443-4 medios para la seguridad en la transmisión

TASK FORCE 3 (TF3)

Es el modelo más avanzado y todavía en desarrollo, una norma aplicable a estas tarjetas es la ISO 7816.

5.3.1.1 NORMA ISO 18000

Es importante conocer que no existen como tal las normas ISO 18000, las normas OHSAS 18000 están dirigidas a ser un sistema que dicta los requisitos a la hora de implantar un sistema con el fin de garantizar la salud y seguridad ocupacional.

Tiene como fin:

- Reducir al mínimo o evitar completamente los riesgos laborales.
- Conseguir eficiencia en cuanto a la utilización de personal, materiales y maquinaria utilizada.
- Seguridad ante accesos no deseados.
- La optimización del funcionamiento de la tecnología.
- Aumento del valor de los productos mediante la mejora de imagen consiguiendo confianza en el mercado.
- Mejora en la productividad y competitividad.

RFID Air Interface Standards

La ISO/IEC 18000 son los estándares relativos a la interfaz aérea de los sistemas de identificación por radiofrecuencia, y que tiene como finalidad la identificación a nivel de artículo. Las revisiones que se han hecho más recientemente tratan sobre:

- La revisión del estándar 18000-6 con el fin de incluir las nuevas especificaciones de EPC Global Generation 2 como Tipo C, así como mejoras a las ediciones Tipo A y Tipo B ya publicadas por la ISO.
- Actualización de todas las partes de la 18000 centrándose en las capacidades de las baterías y sensores de la tecnología actualmente.

APARTADOS DE LA ISO/IEC 18000

Cada una de las partes en que se divide corresponde a un rango de comunicación en la interfaz por aire:

- 18000-1: trata sobre los parámetros generales de la interfaz del aire (air interface) para las frecuencias que son usadas y aceptadas de forma global

- 18000-2: dedicada a las especificaciones y parametrización de la interfaz del aire con frecuencias por debajo de los 135 kHz.

- 18000-3: dedicada a las especificaciones y parametrización de la interfaz del aire para frecuencias que se encuentran en torno a los 13.56 MHz.

- 18000-4: parámetros de las comunicaciones por la interfaz del aire a 2.45 GHz.

- 18000-5: en un principio hacía referencia a las comunicaciones realizadas a 5.8 GHz, pero actualmente figura como proyecto abandonado o retirado.

- 18000-6: Parametrización de las comunicaciones realizadas por la interfaz del aire en el rango de frecuencias 860 MHz – 960 MHz.

- 18000-7: Parámetros de las comunicaciones por la interfaz del aire a 433MHz.

5.3.1.3. NORMA ISO 15693

Este estándar está dirigido sobre todo a sistemas que son utilizados en el mercado con fines tales como control de accesos, identificación y automatización de bibliotecas, control de fraudes y falsificaciones en artículos o productos de alto valor por ejemplo en el sector farmacéutico, como se ha referido en puntos anteriores en el caso de ciertos medicamentos.

También responde a la regulación de un campo magnético que utilizan ciertos dispositivos menor al utilizado por las ya mencionadas tarjetas de proximidad que necesitan campos en un rango de 1.5 a 7.5 A/m, en este caso estaríamos hablando de las llamadas tarjetas de vecindad que operan en torno a 0.15 A/m – 5 A/m.

Estas tarjetas de vecindad (vecinity cards), tienen las siguientes características:

- funcionan a distancias mayores que las de proximidad.
- La frecuencia en la que operan es de 13.56 MHz.
- La mayor distancia a la que se pueden leer está entre los 1 y 1.5 metros.
- Las memorias que llevan incorporadas son de 2048 bits y responde directamente a la necesidad de incluir mayor cantidad de memoria para las aplicaciones RFID, donde es imprescindible incluir datos y seguridad relacionada con éstos.

5.3.1.4. NORMA ISO 15961

Esta norma está dedicada sobre todo a la interfaz de aplicación de los sistemas RFID, incluyendo los protocolos de datos, y la gestión de artículos.

Esta norma junto a la ISO 15962 engloban en su totalidad los protocolos seguidos, ocupándose cada una de ellas de un tipo de interfaz.

CONTENIDO

De forma general esta Norma Internacional se centra en la interfaz entre la aplicación y el procesamiento del protocolo de datos, incluyendo la especificación de sintaxis de transferencia y definición de los comandos de aplicación y respuesta permitiendo una estandarización en datos y comandos independientemente de la interfaz de aire utilizada (ISO/IEC 18000) .

Estos son los aspectos que abarca la ISO 15961:

- Interfaz de la información con el sistema de aplicación.
- Tratamiento de datos y la presentación de los mismos en la etiqueta RFID.
- Tratamiento inicial de los datos capturados de una etiqueta RFID.
- Proporciona directrices sobre cómo presentar los datos como objetos.
- Definición de la estructura de la identificación de objetos.
- Especificación de comandos compatibles en la transferencia de datos entre la aplicación y la etiqueta RF.
- Especificación de las respuestas compatibles para la transferencia de datos entre la etiqueta RFID y la aplicación.
- Especificación de la sintaxis en la transferencia, basada en otros protocolos de codificación para datos que deben transferirse a la aplicación (ISO/IEC 8825-1)

- Es una referencia para el desarrollo de software adecuado para aplicaciones dirigidas a sistemas RFID.

5.4.CONTROL SOBRE USUARIOS

El uso de la tecnología RFID cuenta con múltiples aplicaciones que afectan a las actividades diarias de los ciudadanos, y progresivamente en los próximos años se verá incrementado debido a sus características y amplio campo de posibilidades para las que pueden ser aprovechados. Como hemos citado podemos encontrar sistemas RFID que estén presentes en tiendas de ropa, en la identificación de personas cuando se trata de acceder a instalaciones, empresas, o recintos privados, en la identificación de mascotas, mucho se ha escrito por ejemplo sobre su implantación directa en el cuerpo humano, y también nuestros pasaportes cuentan con identificación por radiofrecuencia.

Todo ello significa que muchos de nuestros datos personales ya se encuentran circulando en estos sistemas por lo que la privacidad puede verse amenazada por un intento de ataque, de forma más técnica se traduce en un intento no autorizado de acceso y lectura a los datos que están almacenados en los dispositivos RFID que nos rodean.

Como respuesta global a estas amenazas, surgen los distintos protocolos y estándares de seguridad que ya hemos mencionado, pero cuando se refieren a nivel de usuario se persigue evitar los accesos no deseados, y para ello se deben desarrollar distintas formas de llevarlo a cabo dependiendo de los distintos tipos de usuarios que existan. Principalmente la diferencia se encuentra en los datos que contengan las etiquetas y la criticidad de los mismos.

A continuación se exponen las medidas de seguridad para usuarios.

5.4.1 GUARDIANES Y FIREWALLS RFID

La necesidad de prevenir la aparición de lectores no deseados en nuestro entorno, hace llegar la aparición de los guardianes RFID. Es un dispositivo activo que protege activamente las etiquetas RFID que se encuentran en su radio de acción contra los lectores hostiles RFID. El procedimiento general que se lleva a cabo se basa en la autentificación de los lectores RFID como primer paso, y como segundo paso la utilización de listas de control de acceso para determinar finalmente si un lector está autorizado a leer una etiqueta determinada. En caso de no cumplirse esta condición la acción que toma el Guardián es emitir una señal de interferencia que evitará la lectura no deseada confundiendo al lector hostil.

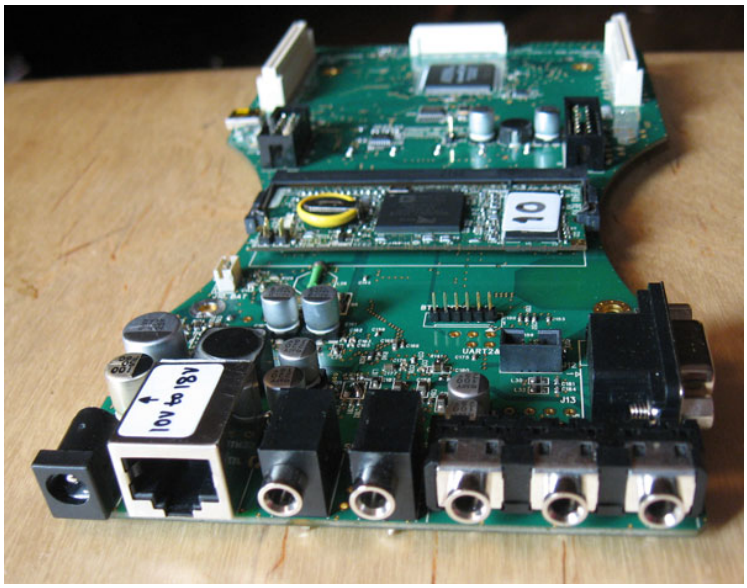


Ilustración 9: Guardián RFID

Imagen de la última versión (V4) de un Guardián RFID.

El desarrollo y fabricación de estos dispositivos en general siguen los estándares de la norma ISO-15693 operando en frecuencias de 13.56 MHz, aunque también existen aparatos que operan a más bajas frecuencias por ejemplo 125kHz – 135kHz, y otras que se contemplan en la norma ISO-18000.

Estos dispositivos están especialmente indicados y diseñados para entornos y usos como los siguientes:

TARJETAS DE CRÉDITO INTELIGENTES

Este tipo de tarjeta está comenzando a sustituir a la tarjeta de crédito habitual con banda magnética. Entre las notables mejoras se encuentra el tiempo de operación, que de media disminuye en 10 segundos con el modelo de banda magnética, además de la mejora que supone no necesitar un lector que se base en el contacto con la tarjeta.

La mayoría de los mecanismos de seguridad de la propia tarjeta no son publicados por medidas de seguridad, pero por ejemplo los datos ofrecen un cifrado triple DES de 128 bits, el resultado es la inutilidad de los datos robados para el potencial ladrón. Además cuenta con sensores que desactivan el chip en caso de intento de acceso de datos a una tarjeta robada.

Las tarjetas inteligentes resultan ser más seguras en algunos casos, partiendo de la base de que no tienen por qué abandonar las manos del poseedor de la misma.

COMPRAS EN PEQUEÑOS COMERCIOS

El uso de RFID en estos casos está dirigido al recuento, identificación y cobro de los artículos al cliente, habitualmente por medio de terminales que identifican todos los objetos del comprador, calculando el importe total y cobrando en el caso de uso de tarjetas inteligentes automáticamente el importe al cliente. Las etiquetas RFID funcionan como índices en los registros de pago de bases de datos y además podrían ayudar al vendedor en el rastreo de artículos defectuosos.

Este entorno podría ser vulnerable sobre todo en las operaciones de pago, por ello el uso de guardianes está indicado para este escenario, protegiendo los terminales de recuento y cobro, dando a conocer al guardián todos los artículos que pueden ser cobrados para evitar fraudes de cobros fraudulentos.

BIBLIOTECAS

El uso en bibliotecas asegura una mayor rapidez en los procesos de salida, inventario y devolución.

El proceso de prestación es relativamente sencillo una vez el usuario ha sido identificado con su tarjeta. Cuando la tarjeta de usuario se encuentra delante del lector de préstamo, el usuario es identificado y la cuenta abierta. El libro a prestar contiene una etiqueta RFID que es leída por el lector y el chip se resetea al estado de prestado, esto permite que los sensores de la salida de la biblioteca no activen la alarma. Uno de los mayores avances es que este proceso optimizado no necesita de un operador humano.

El proceso de inventario también puede ser automatizado, el usuario que lo realice, deberá conectar un lector a un portátil que contenga el software necesario, y desplazarlo por las distintas áreas de la biblioteca, esto hará que el lector detecte los libros, y el software haga las labores de recopilación de datos junto a bases de datos. Uno de los posibles inconvenientes es que algún libro o artículo quede fuera del alcance del lector.

La operación de devolución puede ser automatizada completamente, programando los lectores RFID para detectar el retorno de un libro, y pasándolo al estado devuelto, sin reparar en la identidad de la persona que lo devuelve ya que no es requisito imprescindible que sea la misma persona.

En este marco el Guardián podría evitar el posible robo de artículos mediante un lector no autorizado que cambiara el estado del chip ha prestado, e hiciera que no saltaran las alarmas en la salida del recinto.

Pasaporte con RFID (EPassport)

El Pasaporte actual en Europa como ya vimos utiliza RFID, en el chip se guardan datos biométricos así como una firma digital, y datos personales.

El sistema de comunicación entre lectores y etiquetas se denomina Basic Access Control (Control de Acceso Básico). Además utiliza otros tipos de estándares como MRZ (Machine Readable Zone) para el reconocimiento de caracteres y DES en la generación de claves de sesión aleatoria con el terminal.

El Guardián tendría la misión de evitar la aparición de cualquier lector hostil que aprovechara la comunicación terminal/ pasaporte para acceder a esos datos y clonar por ejemplo un pasaporte. Además debe tenerse en cuenta que algunas veces estos documentos como el pasaporte caen en manos de personas que no son directamente autorizadas a revisarlo, como personal de un hotel que nadie asegura que vayan a hacer un uso adecuado del documento.

AUTOMOVILES

En 1993 la cifra de automóviles robados alcanzó un valor demasiado elevado, y supuso un grave problema para las aseguradoras. Como respuesta se creó un sistema de inmovilización de automóviles que hoy en día incorporan gran parte de ellos en Europa. El número de robos de automóviles con inmovilizador supone una décima parte de los que no lo incorporan.

El resultado de una inmovilización es el bloqueo de puertas o la parada del motor si la identificación no ha sido la esperada. Algunos de estos mecanismos de seguridad utilizan un proceso de pregunta/respuesta. En la inicialización del proceso se lleva a cabo un intercambio de clave con cifrado secreto. Además el transponder responde a la cuestión enviada por el transceptor.

El protocolo seguido para esta respuesta es Frequency Shift Keying (FSK). El sistema de seguridad que lleva incorporado el coche calcula paralelamente o posteriormente la respuesta que le ha dado el transponder y la compara con la respuesta que el mismo ha elaborado y si coinciden o está dentro de los valores esperados, el sistema comunicará con el motor y permitirá actuar de forma normal.

IDENTIFICACIÓN DE ANIMALES

Hay una estimación aproximada de 50 millones de mascotas que portan un chip RFID para ser encontradas en caso de pérdida.

Los estándares en los que están basados los sistemas de identificación de animales son las normas ISO-11784, ISO-11785.

El microchip en estos casos está implantado bajo la piel de los animales, está fabricado de un material biocompatible y tiene un número de identificación único, su tamaño ronda los 12 mm.

Su utilidad consiste en que si el animal es perdido y recogido posteriormente por un refugio, el personal encargado, podrá utilizar un dispositivo lector para leer el número de identificación de la etiqueta, donde buscarán los datos relevantes (datos personales del dueño) en una gran base de datos, si los datos del dueño no aparecen, se recurre a los datos del veterinario que implantó el chip para que facilite los datos del dueño.

Algunas medidas de seguridad por parte de las empresas desarrolladoras de estos sistemas es crear sistemas de cifrado que solo podrán ser descifrados en caso de que el lector lleve incorporado los algoritmos necesarios, o que el usuario recurra a ponerse en contacto con la propia empresa desarrolladora del sistema.

El uso de guardianes está justificado ya que la etiqueta como hemos dicho puede contener los datos personales del dueño, y colocando estos dispositivos podemos evitar la lectura no deseada de datos.

CADENA DE SUMINISTRO

Uno de los principales y más importantes usos de los sistemas RFID se encuentra en la cadena de suministro. Continuamente se aprecia una mejora en la eficiencia de uso en este marco, pero a la vez se incrementan los riesgos asociados, como la filtración de información a lectores hostiles o desconocidos. Uno de los usos más recomendados para los Guardianes es instalarlos en los medios de transporte, como camiones, con el fin de evitar espionaje en tiendas o cadenas de suministro militares.

CASINOS

La industria del entretenimiento siempre busca e impulsa avances tecnológicos. En este caso los casinos estarían muy interesados en contar con la tecnología RFID, por ejemplo para incluir en sus fichas etiquetas RFID y así evitar y detectar posibles falsificaciones y robo de las mismas, o supervisar el comportamiento de los jugadores.

El primer uso que se hizo de RFID en la industria del juego fue en 1995 utilizando sistemas que operaban a frecuencias bajas de 125 kHz, y que suponían tiempos de operación demasiado largos, más tarde se cambió a sistemas más rápidos de 13.56 MHz resultando ser un éxito.

La capacidad de los sistemas RFID en este entorno puede leer 1000 chips por segundo y con una capacidad de memoria de más de 10000 bits, siendo cerca de cinco veces más que la capacidad que ofrecen los sistemas más cercanos con frecuencias más bajas.

El uso de Guardianes en un casino está totalmente justificado, para evitar lectores hostiles que puedan obtener datos económicos del propio casino, o de los usuarios así como sus datos.

GESTIÓN DE DESHECHOS

De forma general, los sistemas RFID se utilizan para dos tareas principales:

- Por un lado en la recogida de deshechos por parte de los camiones. El procedimiento que se sigue y el uso que se da a los sistemas, es para identificar los cubos de basura que va recogiendo el camión, registrando el lugar y la hora a la que se realiza. Todo este proceso supone mejorar y avanzar un grado en el nivel de seguimiento y control del proceso. El paso final sería mediante el middleware adecuado subir la información a un servidor informático y determinar la factura para el cliente.

- El segundo uso principal es la separación de residuos. Este caso está más en proceso de investigación que el anterior, la propuesta consiste en incluir un chip RFID en todos los artículos con el fin de mejorar notablemente la separación de deshechos a la hora de separarlos y tratarlos, por ejemplo distinguiendo los objetos que deben ser reciclados y los que deben ser incinerados.

La principal diferencia entre estos dos usos radica en cómo son leídas las etiquetas por los lectores RFID. En el primer caso se utiliza información de la basura mientras que en la separación de residuos, se utiliza la información de los propios objetos.

El uso de los Guardianes evitaría lecturas no deseadas, evitando el riesgo de acceso a datos posiblemente personales o privados del usuario que estén de alguna forma enlazados con el objeto del que se deshizo y que se encuentra en la basura.

CASOS DE USO DE LOS GUARDIANES RFID

A continuación se muestra un caso de uso relacionado con los marcos expuestos anteriormente. De forma general, funcionalmente, el Guardián siempre se sitúa entre la etiqueta o etiquetas a leer y el lector, verificando al lector, evitando así desconocidos y lecturas hostiles.

En el caso de las compras en una tienda podríamos establecer un marco general como el siguiente:

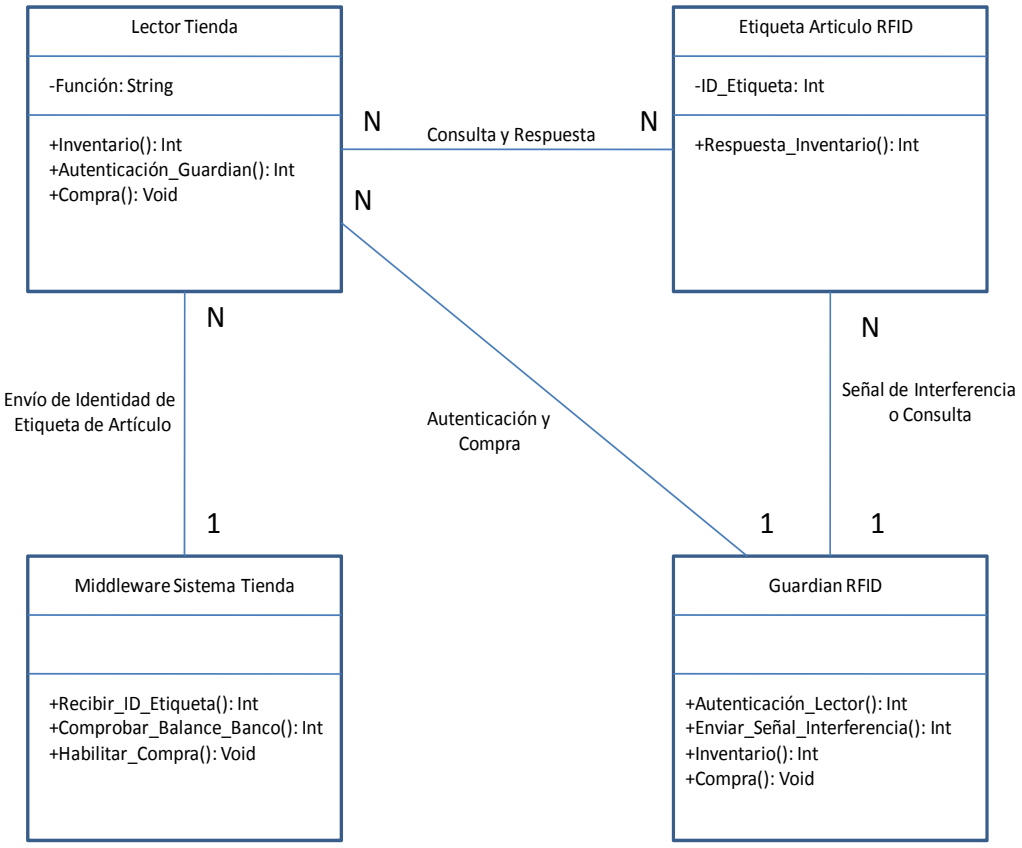


Ilustración 10: Diagrama de Clases

En un sistema simple podríamos contar con el lector RFID de la tienda, que identificaría, haría inventario y cobraría al cliente, el middleware de la tienda que gestionaría los datos recogidos por el lector de la tienda, las etiquetas pertenecientes a los objetos del comercio que van a ser cobrados o inventariados, y el guardián RFID, que como función principal tendría la de autentificar el lector de la tienda evitando la lectura de otros dispositivos ajenos. En caso de no verificar la

identidad del alguno de los lectores que están intentando acceder a la identidad de las etiquetas, el Guardián lanza una interferencia evitando el funcionamiento del supuesto lector ajeno al sistema.

El Caso de Uso es el siguiente:

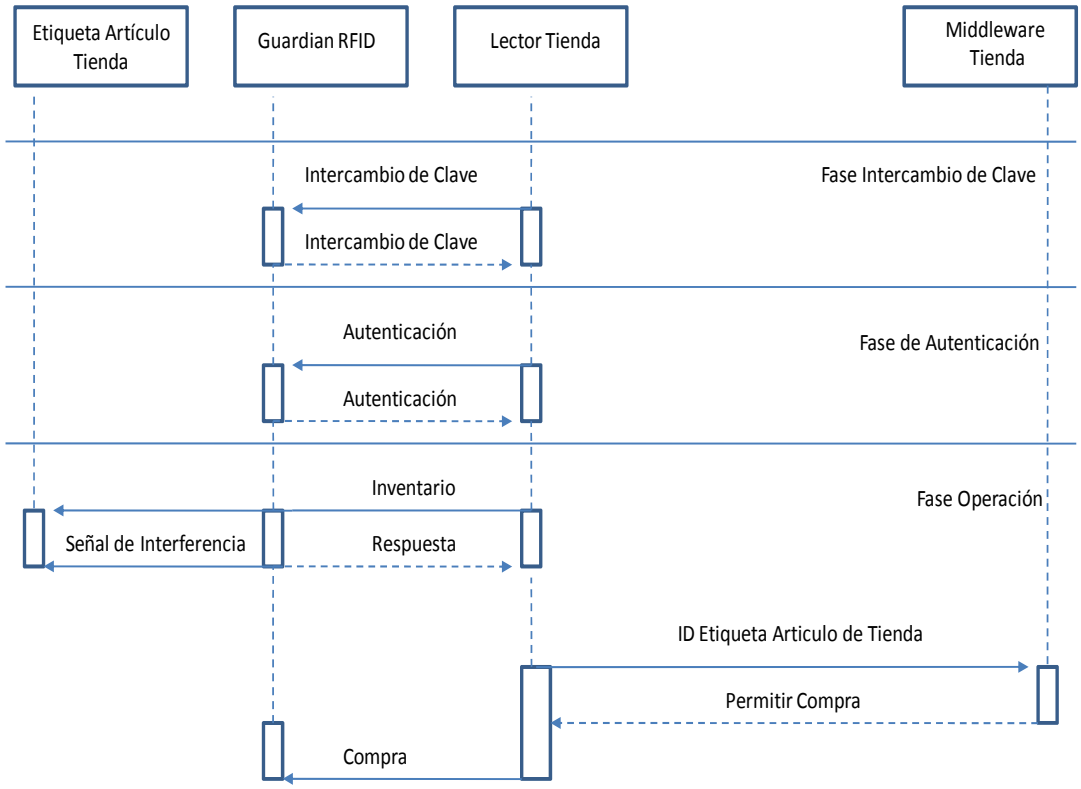


Ilustración 11: Caso Real

Puede apreciarse como funcionalmente el Guardián RFID se sitúa entre la etiqueta y el lector de la tienda. En primer lugar se lleva a cabo un intercambio de claves y si el resultado es el esperado, el Guardián autoriza a leer al dispositivo de la tienda, en caso negativo, emitiría interferencias confundiendo al lector hostil o sin identificar que intenta operar en el entorno. Si de otro modo, las autenticaciones se

llevan a cabo sin ningún problema ni anomalía se procede a realizar las operaciones normales del comercio, inventariado y compra.

ACCESO A LISTA DE CONTROL

El modo en que opera un Guardián suele ser con una ACL. Normalmente es controlada desde una interfaz de usuario.

La lista está compuesta por una serie de archivos agrupados en un directorio:

- Archivo de etiquetas o conjunto de etiquetas.
- Archivo de contexto (opcional), adjunto al archivo de etiquetas.
- Archivo de lectores, donde se definen los dispositivos y sus funciones.
- Archivo donde se definen las reglas que seguirá el guardián.
- Archivo opcional donde se encontrarán las consultas que lanzará el guardián a los lectores que intenten acceder a la lectura de etiquetas.

Pueden existir varias ACL, y habrá que elegir con cual se desea que opere el Guardián.

El funcionamiento general es así, una vez seleccionada la ACL con la que va a operar, cada vez que una consulta de RFID es recibida, se invoca a la ACL, creando una decisión basada en:

- Los roles que el lector actual puede adoptar
- El lector es identificado en el contexto en el que se encuentra el Guardián y es relacionado con él.
- Responde de forma esperada a las cuestiones lanzadas por el sistema.

5.4.2 OTRAS MEDIDAS DE SEGURIDAD

WATCHDOG

Existen un tipo de etiquetas denominadas perros guardianes (watchdog en inglés), y suponen otro sistema para brindar un entorno seguro al usuario.

Antes hablábamos de los Guardianes que interceptaban los intentos de lectura, los verificaban, y aceptaban o interferían según la identidad del lector. En cambio las etiquetas watchdog lo que hacen es informar de todos los intentos de lectura y escritura que reciben en su área de operación.

CARCASAS METÁLICAS, FUNDAS

Es un sistema de protección directamente físico, y su fin es evitar cualquier tipo de lectura, por lo que el chip que contenga el objeto a proteger, quedará inactivo mientras tenga la funda o carcasa puesta.

El efecto deseado es la llamada "jaula de Faraday" que se consigue con aislamientos metálicos o plásticos de la etiqueta u objeto que la porte.

En algunos documentos incluso animan a los portadores de tarjetas de crédito con chips RFID, a fabricarse sus propias carcasas con aluminio casero evitando así lecturas espía.

ELIMINACIÓN DE LA ETIQUETA

En las recomendaciones de la Comisión Europea podemos encontrar medidas de seguridad recomendadas como la eliminación de la etiqueta adherida a los objetos una vez sean adquiridos por el cliente, si estos contienen información y datos sobre la privacidad del mismo. Además en caso de no contener datos que en principio sean privados o susceptibles de amenazar la privacidad del cliente, se ha de ofrecer una forma sencilla de eliminación sin coste adicional para el cliente.

Las formas en que se puede destruir de forma general una etiqueta son las siguientes:

- Físicamente: se destruye la etiqueta directamente.
- Lanzar el comando KILL desde el lector autorizado, inhabilitando la actividad de la etiqueta.

5.6.CONTROL SOBRE PROVEEDORES

Gracias a las características que ofrece este tipo de identificación, y por la variedad de aplicaciones, RFID se está convirtiendo cada vez más en una opción elegida por múltiples organizaciones de todo el mundo para realizar sus procesos, se prevé que en los próximos años serán muchas más las que lo harán.

Para poder ofrecer un entorno lo más estable posible para el usuario, hay que tener en cuenta factores tan importantes como la privacidad y seguridad, evitando así daños a éstos que repercuten además directamente en la compañía con problemas como pérdida de imagen pública y por tanto daño directo a los ingresos de la organización.

Además una de las premisas que se pretenden con las decisiones tomadas desde Europa y desde los organismos oficiales reguladores, es evitar fijar como centro de las aplicaciones y operaciones al usuario, lo que se pretende es fijar la información en los objetos que portan las etiquetas evitando dañar al cliente, y reducir al máximo los datos innecesarios referentes a la figura del usuario.

5.6.1 PRIVACY IMPACT ASSESMENT (PIA)

A partir del comunicado emitido por la Comisión Europea en el 2009 se establece la obligación de implantar un marco de datos de carácter personal y evaluaciones sobre el impacto en la intimidad y privacidad de los usuarios (PIA). Este marco debe ser desarrollado por la industria en colaboración con las autoridades civiles.

El objetivo de esta evaluación es "ayudar a los operadores de aplicaciones RFID a descubrir los posibles riesgos asociados a una aplicación RFID, evaluar la probabilidad de que ocurran, y documentar las medidas que se adoptarán para hacer frente a dichos riesgos".

En primer lugar, al realizar una evaluación de este tipo se deben considerar principalmente tres cuestiones:

- Quien se considera realmente el operador de las aplicaciones RFID (quién)
- El alcance de las aplicaciones RFID (qué)
- El momento en que es realizado el PIA (cuando)

Independientemente en principio de las especificaciones, la Comisión Europea recomienda realizar un PIA a todos los operadores RFID (toda persona física, o jurídica, autoridad pública, servicio o cualquier organismo que solo o conjuntamente, determina los fines y medios de la operación de una aplicación mediante RFID). Ahora bien, no es lo mismo una operación que afecta a miles de usuarios que una pequeña tienda que incorpora RFID para cobrar a sus clientes.

En los casos de menor envergadura se recomienda realizar un PIA cuando se incorporen nuevos sistemas o modificaciones que afecten al proyecto inicial, con el fin de detectar el grado de efecto sobre la privacidad y seguridad de los usuarios.

Hay casos en los que la tecnología RFID no opera directamente en ningún caso con datos privados, o no se utilizan datos que afecten directa o indirectamente a la privacidad y seguridad del usuario, en tales casos no es necesario realizar un PIA.

La necesidad de llevar a cabo un PIA se puede ver de forma gráfica con el siguiente árbol de decisión:

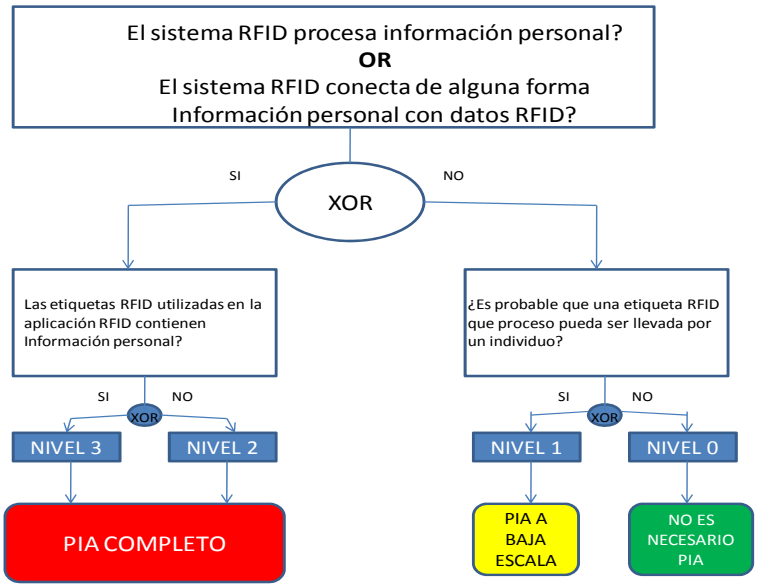


Ilustración 12: Niveles aplicables

Los niveles que aparecen reflejados en el árbol, se refieren a la profundidad con que se estudiarán los posibles riesgos asociados al tipo de procesamiento de datos privados que haya en nuestro sistema RFID. Cuanto mayor nivel, mayor complejidad y especificación en el estudio de riesgos.

Sin embargo hay aplicaciones en las que a priori directamente con el uso de lectores y etiquetas no se tratan datos personales, ni privados, pero mediante una asociación de datos, en la parte de la aplicación software y en la red en general se vinculan datos personales y privados a datos que no lo son, lo que obliga a la realización de un PIA, siempre entendiendo datos personales según la definición de la Unión Europea (cualquier información relativa a una persona identificada o identificable , a su vez una persona identificable es aquella que puede determinarse, directa o indirectamente, mediante un número de identificación específico o uno o varios elementos específicos de su identidad física, fisiológica, psíquica, económica, cultural o social).

METODOLOGÍA SOBRE EVALUACIÓN DE RIESGOS EN LA PRIVACIDAD

Al igual que en muchas gestiones o procesos de negocio, la aplicación de una metodología para llevar a cabo un proceso asegura identificar los puntos clave, en el caso que concierne a la evaluación de riesgos de privacidad asegura la identificación de los mismos y las estrategias correctas para mitigarlos.

El modelo genérico de referencia del proceso descrito por el PIA se muestra a continuación:

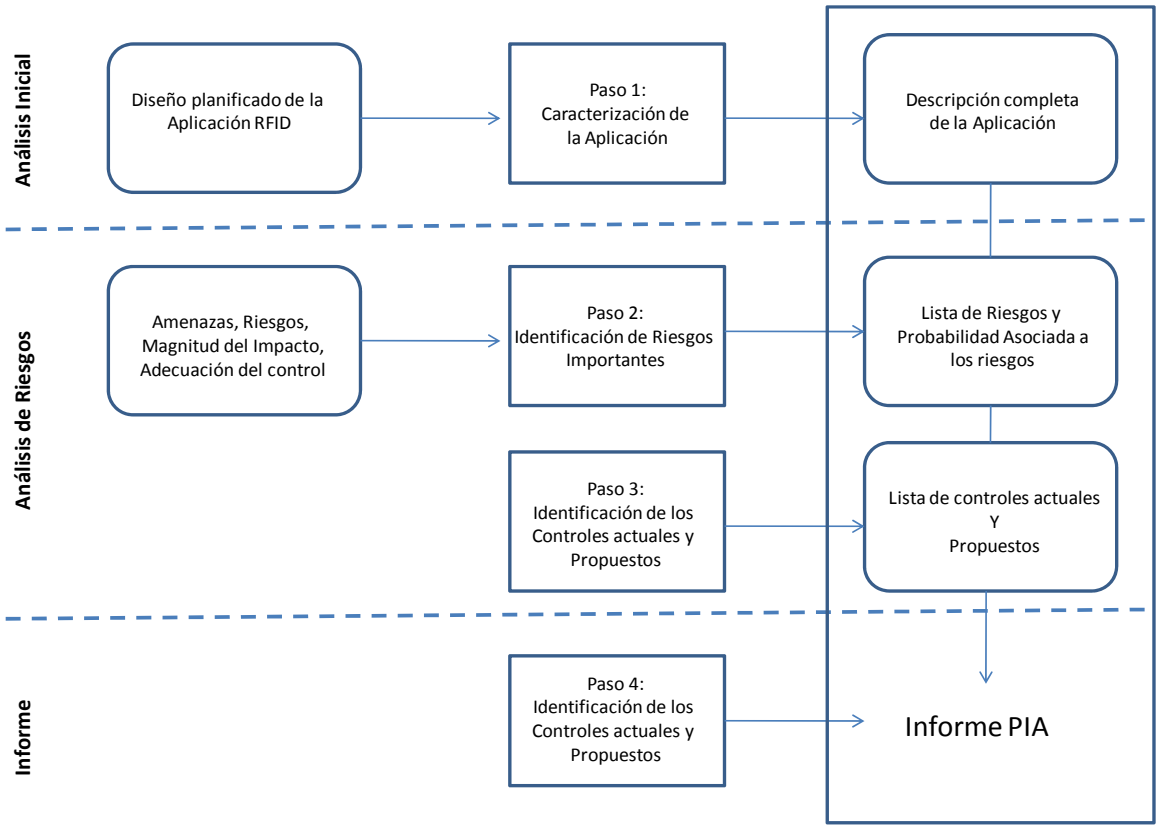


Ilustración 13: Pasos Evaluación

Si este proceso inicial determina que es necesario realizar un PIA, se deben seguir los siguientes pasos, de los cuales los dos primeros se consideran el foco principal para detectar los riesgos más importantes en privacidad.

Los pasos se muestran de forma general en el gráfico siguiente:

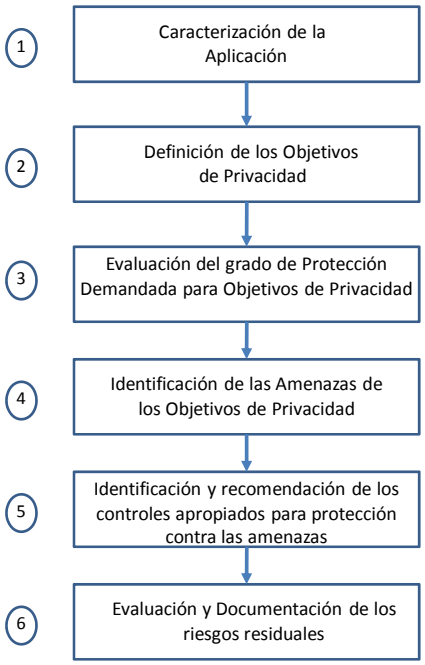


Ilustración 14: Pasos Evaluación

PASOS EN LA ELABORACIÓN DE UNA EVALUACIÓN DE RIESGOS (PIA)

Los pasos según la metodología propuesta son los siguientes:

1. **Caracterización de la aplicación**: en esta fase el objetivo principal es completar una caracterización de la aplicación, eso se traduce, en hacer una detallada descripción de escenarios, casos de usos, sistemas, componentes, interfaces, flujos de datos y partes involucradas. Identificar claramente el alcance, los límites los recursos e información utilizada.
2. **Definición de objetivos de privacidad:** El objetivo principal es comprender que es lo que está realmente en riesgo, el punto de partida como referencia para dicho análisis es la legislación europea, asegurando así el cumplimiento legal, y si hablamos de un proyecto dentro del territorio español, debe estar en concordancia también con la LOPD.
3. **Evaluación del grado de protección demandada para cada objetivo de privacidad:** desde el punto de vista de la privacidad, todos los objetivos son igual de importantes pero pueden tener más urgencia algunos de ellos para la

empresa. A veces es difícil calcular los posibles daños que puede causar una posible amenaza en privacidad, en ese caso deben ser considerados los factores como daños potenciales a la reputación de la compañía o a sus implicaciones sociales, para ello es necesario una evaluación cualitativa realizada por expertos. Puede que una amenaza no llegue a dañar directamente a los usuarios pero si existe puede causar mala prensa, o reputación dañando la imagen y la actividad de la empresa. Por ello es importante fijar muy bien los objetivos de privacidad.

4. **Identificación de las amenazas para cada objetivo de Privacidad:** tras identificar los objetivos de privacidad, se trata de identificar de que forma se puede ver amenazado dicho punto. La propia organización PIA suministra una lista sobre posibles amenazas asociadas a partes de la privacidad.
5. **Identificación y recomendación de los controles apropiados para protección contra las amenazas:** otro paso esencial en la evaluación de los riesgos para la privacidad es identificar los controles que pueden ayudar a minimizar, mitigar o eliminar los riesgos asociados a la privacidad que han sido ya identificados. Los tipos de controles pueden ser técnicos o no técnicos. Entre los controles técnicos encontramos controles de acceso a mecanismos, sistemas de autenticación, o métodos de cifrado. Los controles no técnicos son los relacionados con el control de gestión, medidas y controles de políticas, procedimientos operacionales y medidas sobre los datos recogidos de los usuarios.
6. **Evaluación y Documentación de los riesgos residuales:** en este paso se evalúa la lista de controles recomendados que resultan del paso anterior. La evaluación puede ser en función de varios parámetros por ejemplo en función de la viabilidad y la eficacia o fijándose en un análisis de coste-beneficio. A continuación se evalúan los controles, que pueden ser ordenados en una lista de prioridades. Como resultado se obtiene un plan de aplicación para el control, del que se derivan los riesgos residuales, esto se refiere por ejemplo a si un control implementado reduce la magnitud de impacto de una amenaza pero no elimina la amenaza completamente por razones técnicas o de negocio.

5.7.GARANTIZAR USO ADECUADO

BUENAS PRÁCTICAS

Con el fin de evitar ciertos riesgos es aconsejable además de todas las medidas obligatorias que han de tomar los comercios y la industria, llevar una serie de acciones minimizando lo posible cualquier amenaza a la privacidad o seguridad del entorno y usuarios de los dispositivos. Es importante recalcar que además de las medidas técnicas asociadas a cada riesgo, hay que tener en cuenta que en general es fundamental una vigilancia y cuidado por medio del personal responsable de la seguridad, evitando la inclusión de dispositivos externos, supervisando el correcto funcionamiento, reforzando la vigilancia, dando al cliente consejos sobre seguridad, evitando directamente el fraude, y animando al cliente a usar sistemas de seguridad básicos como las carcasas aislantes.

Las siguientes medidas están clasificadas según las amenazas que se desean evitar.

SUPLANTACIÓN DE ETIQUETA

Existe la posibilidad de que un lector intente simular la identidad de una etiqueta, esto es posible adaptando su pseudónimo y respondiendo de forma que parezca la etiqueta.

La solución más sencilla es que a la etiqueta se la identifique con varios pseudónimos, ya que es difícil que un lector malintencionado conozca la totalidad de ellos y el orden en que van a usarse, evitando así el intento de réplica. Contrarrestando este tipo de defensa existen lectores que efectivamente intentan detectar la secuencia que utiliza la etiqueta y copiar así sus identidades y el orden seguido. La solución final sería alargar el tiempo de respuesta de la etiqueta al máximo evitando la secuenciación por parte del lector espía.

Otra solución a este tipo de amenaza es autenticar la comunicación entre lector y etiqueta añadiendo una clave secreta con la que poder verificar el intercambio de datos, y evitando la participación de dispositivos externos al sistema creado.

INTERCEPCIÓN DE COMUNICACIÓN LECTOR/ETIQUETA

Normalmente la capacidad de las etiquetas en cuanto a memoria no es demasiado extensa, por lo que se tiende a optimizar al máximo el espacio. Esto traducido a seguridad y cifrado significa que algunos algoritmos usados comúnmente para otro tipo de comunicaciones no es válido para etiquetas RFID. Algunos de los cifrados utilizados es el DES como está explicado en puntos anteriores.

En este caso también es aplicable otros sistemas de seguridad como la autenticación de la comunicación para evitar dispositivos externos.

MANIPULACIÓN DE LA INFORMACIÓN EN ETIQUETAS

Además de aplicar la autenticación, la medida más adecuada sería la de incluir solamente en la memoria del lector el identificador, y asociado a este código identificador en el software del sistema en una base de datos o en un servidor, almacenar todos los datos asociados a este producto, en caso de ser un objeto a la venta, precio, lote, fabricante, y demás datos.

5.7.1 SEGURIDAD

A continuación un análisis de los posibles riesgos físicos que pueden afectar a los usuarios. Hay que tener en cuenta que RFID usa ondas de radio, de distinta frecuencia, dependiendo del tipo de sistema, y por tanto hay que incluir el estudio de los posibles impactos que tienen además de éstas, las microondas y las radiaciones generadas sobre el hombre.

Cuando se estudia llevar a cabo el uso de transmisores en el que intervienen ondas de radio, hay varios factores principales a tener en cuenta. Un importante factor es la frecuencia con que opera el transmisor.

Es importante exponer los distintos tipos de magnitud utilizados para el estudio del impacto de dispositivos con radiofrecuencia en el hombre:

- **SAR (Specific Absorption Rate):** suele ser la más común y la más útil para los sistemas que van a ser utilizados cerca del cuerpo, se traduce como la tasa de absorción específica. Es una medida de potencia que se introduce en el cuerpo, pudiéndose diferenciar por zonas o áreas específicas o un promedio. Su unidad de medida es el Watt por Kilogramo de tejido (W/kg)

- **BQ (Bequeler):** velocidad a la que una muestra se desintegra, se mide en Bq y se expresa como número de desintegraciones por unidad de tiempo.

- **Sv (Sievert):** es la unidad que mide la dosis de radiación , y el daño producido por todo tipo de radiación al cuerpo humano, la magnitud es dosis de radiación.

De entre las expuestas, la que tiene mayor uso, y se tiene más en cuenta es la tasa de absorción específica (SAR). Para hacernos una idea, la tasa de exposición estándar para dispositivos móviles en Europa tiene como límite 2 W/kg de tejido humano, medidos sobre 10 gramos de tejidos, a diferencia de Estados Unidos que para el mismo tipo de dispositivos establece una tasa de 1,6 W/Kg. Dependiendo del modelo de dispositivo móvil, esta tasa puede variar entre los 0,4 y los 1,4 W/Kg, la media está por debajo de 1 W/Kg. Como dato importante cabe destacar que los dispositivos WIFI no están obligados a comunicar su tasa SAR.

Otros factores interesantes e importantes que afectan a RFID, es la potencia transmitida y la distancia del cuerpo al dispositivo. Hay una diferencia de potencia

utilizada de los dispositivos utilizados cerca del cuerpo como los teléfonos móviles e inalámbricos (potencias bajas), a los usados en vehículos (potencias más altas), la razón de esto, es que la distancia de la antena de los dispositivos con baja potencia se colocan a muy poca distancia del cuerpo, como es el caso de los teléfonos móviles.

ESPECIFICACIONES RFID

Además de las regulaciones que afectan a los dispositivos móviles, existen otras normativas seguidas por los organismos oficiales y gubernamentales que afectan directamente al uso de radiofrecuencia. La mayoría de estas normativas y guías más tenidas en cuenta por los organismos gubernamentales, son las desarrolladas por:

- **IEEE** (Institute of electrical and electronics engineers), la organización técnica científica más importante del mundo, formada por expertos de los distintos estándares que se desarrollan para industrias del campo científico.
- **NCRP** (National Council on Radiation Protection and Measurements), consejo establecido en los años 60 para la regular y proporcionar todo tipo de información para asegurar la protección de la salud frente a la radiación.
- **ICNIRP** (International Commissionfor non-ionizong Radiation Protection), organización independiente responsable de proporcionar guías e información sobre los posibles riesgos para el hombre de la exposición a radiación no ionizante.
- **FCC** (Federal Communications and Commission), organización estatal e independiente de Estados Unidos, que tiene entre otras competencias la de dar licencias a las estaciones encargadas de transmitir señal de radio y televisión, también la de asignar frecuencias de radio, y lo que más nos interesa para este punto es que desde los años setenta, también elaboran

Las guías y normativas proporcionadas por las organizaciones anteriores difieren en algunos puntos y matices, pero en general son bastante similares en cuanto a las líneas principales sobre las frecuencias que se deben utilizar en dispositivos con radiofrecuencia.

Es importante conocer los dos tipos de exposiciones principales que son considerados a la hora de elaborar normativas:

- Exposición ocupacional o de “entornos controlados”: lugar donde las personas son conscientes de estar sometidas a radiaciones de radiofrecuencia.
- Exposición del público o de “entornos incontrolados”: lugar donde las personas no son conscientes de estar sometidas a radiaciones de radiofrecuencia.

Las especificaciones pueden también verse en la Norma IEEE-C95. 1-1991

En general coinciden en permitir un nivel de exposición mucho más bajo (hasta cinco veces) en entornos de exposición del público a los entornos controlados, enmarcado en el margen de frecuencias de hasta 3000MHz.

Además existen otros tipos de clasificaciones a la hora de analizarlas, estudiarlas, y más tarde elaborar normativas y guías:

- Exposición corporal completa: son recibidas por todo el cuerpo.
- Exposición corporal parcial: son recibidas solo en una parte del cuerpo
- Exposición por promedios de tiempo: son medidas por intervalos, generalmente establecidos éstos entre los 6 y 30 minutos.
- Exposiciones de baja potencia: a este grupo le aplican los intervalos de tiempo, ya que se considera que una exposición baja no es dañina cómo para tener que controlar el tiempo de exposición, aunque algunas organizaciones como ICNIRP y FCC (Federal Communications and Commission) también lo tienen en cuenta.

Es importante saber cómo se han creado estas guías, generalmente el proceso que se sigue es mediante un consejo de científicos e ingenieros, basándose en la información dejada por los expertos hasta el momento en radiofrecuencia y sus efectos cuando los seres vivos son expuestos a ella. En este proceso se revisan un enorme número de documentos, de distinto tipo, y además de todo tipo de expertos relacionados con el tema, se incluyen a veces al mismo público al que va destinado a proteger.

Una de las importantes conclusiones a las que se han llegado sobre la exposición en seres vivos, es que los campos electromagnéticos bajos, no tienen efecto clínico aparente sobre seres humanos y animales. Sin embargo también se llegó a la conclusión firme tras numerosos experimentos que sobre animales de laboratorio una exposición a cuerpo completo (SAR de exposición completa) a partir de un rango de 4 W/Kg producía un efecto común en los sujetos expuestos. Los animales afectados por una subida de temperatura, abandonaban las rutinas que estaban realizando y para las que habían estado entrenados. Sobre seres humanos no se ha

probado esto, pero con una alta probabilidad se asegura que ocurriría lo mismo, el cuerpo ascendería a una temperatura parecida a la que alcanza en un entorno con un clima extremadamente caluroso, o mediante un ejercicio con resultados extenuantes, lo que produciría probablemente el estímulo necesario para abandonar toda actividad compleja. Es importante destacar que los efectos son reversibles en los experimentos observados.

Los datos reales de los que se dispone en cuanto a efectos de exposición de energía producida por radiación no son muy amplios, ya que no se ha sometido a humanos a exposiciones altas con el fin de obtener datos por los posibles riesgos. Si existen experimentos con radiaciones parecidas a las producidas por los teléfonos móviles sin efectos perjudiciales observables.

Respecto a los teléfonos móviles se han mostrado algunas investigaciones en las que se comparaban el número de víctimas producidas por cáncer cerebral entre usuarios de teléfono móvil y usuarios de teléfono adaptado al coche con la antena acoplada al techo (la diferencia se encuentra en que una antena está pegada al cerebro, y otra se encuentra en el techo del coche). Los resultados no indican que alguno de los dos tipos de aparatos esté relacionado de una forma más directa con este tipo de patologías.

Las personas con marcapasos, y otro tipo de aparatos implantados en sus cuerpos deben consultar a su médico, y en ocasiones al fabricante del dispositivo con radiofrecuencia que desean utilizar para ver la viabilidad en caso de hacerlo, y si existen riesgos asociados.

Definitivamente todos los organismos responsables de suministrar guías de seguridad, y estudiar los posibles riesgos coinciden en que las evidencias observadas hasta el momento indican que aparentemente no hay riesgo en la utilización de aparatos con radiofrecuencia, con niveles y frecuencias regulados. Por lo que dispositivos de Wifi y sistemas RFID no suponen una amenaza para nuestra salud.

5.7.2 MEDIDAS PARA LA MEJORA DE LA PRIVACIDAD

Antes de hablar de las medidas adecuadas para asegurar la privacidad en sistemas RFID, repasaremos las amenazas específicas para las que se sugieren las medidas. Los puntos especialmente susceptibles relacionados con la tecnología RFID:

- Capacidad de una etiqueta para ser leída a distancia sin la participación del individuo.
- Posibilidad de revelar información sensible acerca de las personas a través de interferencias o lectura no autorizada.
- Hacer seguimiento no autorizado de un sistema RFID.

Además hay algunas propiedades asociadas a RFID que o bien suponen posibles amenazas o son vistas con escepticismo por un sector de la población, y que en un momento dado puede suponer un freno para el desarrollo y expansión de la tecnología. Son las siguientes propiedades:

INVISIBILIDAD EN LA TRANSMISIÓN DE DATOS

Como ya sabemos la comunicación entre los dispositivos de un sistema RFID se lleva a cabo mediante señales electromagnéticas, lo que quiere decir que la comunicación es capaz de llegar desde las etiquetas hasta los lectores a través de los materiales que conforman, ropa, la mayoría de envoltorios no aislantes, recipientes y casi toda clase de objetos, lo que hace tener una idea de "comunicación invisible", no perceptible a los sentidos. Además esta propiedad hace susceptible a la tecnología de ciertos ataques como interferencias, escuchas no autorizadas y acceso a datos de forma remota.

Todo ello puede crear la idea en el cliente de cierta inseguridad y de no saber que puede estar ocurriendo con sus datos, lo que supone un aspecto negativo en su progresión en el mercado.

Obviamente, hemos analizado los posibles aspectos negativos, pero esta propiedad es también una de las mayores cualidades para hacerlo atractivo para su uso comercial e industrial.

PERFILES

El acceso a los objetos que pertenecen a una persona y que incluyen una etiqueta RFID, puede suponer una amenaza en cuanto a su privacidad, debido a la creación de perfiles.

Esto se refiere a la posibilidad del seguimiento de una persona a partir de sus objetos y compras, extrayendo así aspectos y datos de su vida personal. Por ejemplo si alguien accede de forma no autorizada a la lectura de las etiquetas RFID de los medicamentos que porta un individuo, y ese medicamento está indicado para enfermedades como la depresión, podría crearse un perfil en el que se relacionara a esta persona con dicha enfermedad, algo que viola completamente la privacidad de los ciudadanos.

Los fines pueden ser de todo tipo, por ejemplo con intereses comerciales, con el fin de conocer cuáles son las preferencias de ciertos ciudadanos, o revelar los datos de una persona en concreto.

RASTREO

Una de las funciones clave de RFID, y uno de sus mayores usos en la industria en general, es el de rastreo, por ejemplo de mercancías, animales o productos. Ciertos parques temáticos incluyen dispositivos RFID para que los padres puedan asegurarse de no perder a sus hijos en las instalaciones.

El procesamiento de los datos puede hacerse en tiempo real, o una vez recopilados los datos con apoyo de bases de datos, dependiendo del sistema que haya implementado.

La amenaza para la privacidad aparece de nuevo en las lecturas y rastreos no autorizados que ponen en peligro la privacidad y datos personales de los usuarios, existiendo la posibilidad incluso de detectar un individuo específico y realizar así su seguimiento. O en caso de realizarse el seguimiento a una empresa por parte de otra rival, podría suponer una filtración de información que afectaría de forma negativa a la compañía espiada.

Para ello la Comisión Europea indica que debe hacerse una evaluación de riesgos durante su diseño y así poder limitar el campo de acción y la cantidad de datos a manejar en el sistema como ya hemos visto.

INTEROPERABILIDAD

De forma general se pueden establecer dos tipos de entornos en donde los sistemas RFID operan:

- **Entornos cerrados**: los datos simplemente llevan un seguimiento, por una misma compañía, y los dispositivos que intervienen son siempre los mismos, o están claramente identificados, así como la naturaleza de las operaciones y datos.
- **Entornos abiertos**: los dispositivos, las operaciones, y los datos están sujetas a cambios continuamente, y son múltiples los actores que entran en juego en el proceso. Los datos pueden sufrir modificaciones, y los dispositivos pueden variar continuamente.

El primer tipo de entorno supone un marco más seguro para la protección de los datos y la privacidad, es más sencillo el control directo sobre cada una de las partes que intervienen en el proceso. Por otra parte, utilizar dispositivos RFID en este tipo de entorno tan estático no supone un gran avance respecto a otros sistemas de identificación como los códigos de barras, el único campo donde supondría a priori una gran ventaja sería en la velocidad de recopilación de datos.

El segundo tipo de entornos donde por ejemplo el número de lectores es variable, y en las operaciones se pueden modificar datos continuamente, supone un potencial muy grande para las posibles aplicaciones a llevar a cabo con identificación con radiofrecuencia. A cambio el riesgo de sufrir ataques a dispositivos y prácticas no autorizadas crece considerablemente, al ser un marco más dinámico donde es más complicado llevar un control sobre los accesos a esos datos.

MEDIDAS

Toda medida de seguridad afecta directamente a la privacidad, haciendo un sistema más estable y restringido, ayudando a mantener el anonimato y privacidad de los usuarios.

Además existen una serie de acciones que previene la estabilidad de los sistemas y las características que acabamos de repasar. Las medidas son las siguientes:

1. **Notificación del uso de tecnología RFID a los usuarios**:
   En las medidas elaboradas por la Comisión Europea se incluye la necesidad de avisar a los usuarios de forma directa y sin lugar a equívocos del uso de etiquetas y lectores RFID, para llevarlo a cabo los objetos deben incluir un símbolo que esté patentado y la hagan fácilmente identificable.

Ilustración 15: Símbolo Advertencia

2. **Notificación al usuario del acceso a datos:**
   Es necesario también informar de forma clara al usuario de las zonas y momentos en los que se proceda al acceso de datos en las etiquetas que estén relacionadas con el usuario.

3. **Política de privacidad:**

   Es necesario tener una regulación sobre el tipo de operaciones que se van a realizar con los datos del usuario y además facilitar el acceso de esta política a los propios usuarios.

4. **Modificación y eliminación de datos:**

   El usuario tiene derecho a modificar y eliminar si es preciso los datos que constan en los sistemas. En el caso de operaciones en las que directamente se considere crítica la información utilizada, deberá ser eliminada de la etiqueta una vez salga del control de la empresa, si la información no es considerada de riesgo, se deberá facilitar de forma gratuita la posibilidad de eliminar la información al usuario.

5. **Personal:**

   El personal que esté a cargo de las operaciones con RFID debe estar correctamente formado en estas cuestiones ofreciendo un entorno y un uso más seguro por medio de su supervisión.

6. **Eliminación de las etiquetas:**

   Una vez acabado el uso para el que estaban diseñadas las etiquetas se debe proceder a su eliminación para acabar con cualquier tipo de vínculo que pueda existir entre la etiqueta y el usuario, con el fin de evitar posibles creaciones de perfiles de usuario, o manejo de datos no autorizado como el rastreo. Al igual que ocurría con la modificación y eliminación de datos, la empresa deber facilitar sin coste adicional la forma de eliminar la etiqueta aun cuando se considere después de la evaluación de riesgos que no supone una amenaza para el cliente.

7. **Filtración de datos:**

   Evitar el traspaso de datos o información relevante relacionada con los sistemas RFID que en un futuro puedan suponer un riesgo para la creación de perfiles o seguimiento no autorizado de los clientes.

8. **Mejora continua:**

   Es una forma de estar actualizando los sistemas de cara a nuevas amenazas y ofrecer la mejor calidad de servicio.

9. **Realización de auditorías periódicas:**

   La forma más directa de evaluar y garantizar un servicio seguro.

6. TEST EVALUACIÓN RIESGOS SOBRE SEGURIDAD Y PRIVACIDAD

Se han expuesto las diferentes legislaciones, normativas, metodologías y marcos para lograr un entorno seguro en la utilización de sistemas RFID. Desde el punto de vista de un operador se ha considerado la idea de aportar una forma sencilla, rápida y directa de realizar un diagnóstico sobre seguridad y privacidad del sistema actual, futuro sistema, o actualización parcial de una infraestructura RFID.

Hemos visto como mediante un PIA podemos hacer un estudio en profundidad del estado del sistema en cuanto a seguridad, datos personales, privacidad, todo ello siguiendo varias fases de análisis dependiendo del nivel de complejidad. El método aquí propuesto sería una forma más directa de evaluar los distintos focos donde se localizan las posibles amenazas, y elaborar un informe del estado en que se encuentra si el sistema está ya implementado, tanto si es un diseño o una ampliación.

La forma en que se elabora el informe es mediante el diagnóstico de veinte preguntas divididas en cinco apartados, a las que se podrá contestar de forma sencilla en la mayoría de los casos SI/NO, y en otros casos dando una valoración numérica, o descriptiva sobre la forma en que se realiza alguna función. Según las respuestas dadas, se elaboran una serie de recomendaciones, un diagnóstico del nivel de seguridad en cada área, y en caso de considerarse necesario una serie de recomendaciones y buenas prácticas.

6.1 AREAS DE DIAGNÓSTICO

Como se ha comentado, el estudio se dirige a cinco puntos, considerados los focos de posibles carencias en la seguridad y privacidad, cada área constará de cuatro preguntas que servirán para dar un diagnóstico global.

RECOPILACIÓN

En este apartado se formulan cuatro preguntas que intentan englobar la forma y aspectos generales sobre la forma de recoger los datos, las políticas seguidas para ello, y posibles prácticas inadecuadas que pueden llevarse a cabo incluso de forma involuntaria pero pueden ser ilegales, como leer etiquetas de otra compañía sin autorización de la misma.

Recopilación	1	1.¿El tratamiento de datos se realiza de acuerdo a una política definida basada en el tratamiento legal y lícito de los datos, reflejado en los requisitos legales?	Si
		2.¿Hay definidas medidas para promover la calidad de los datos?/¿Evitar la evasión de datos?	Si
		3.¿Los lectores de su empresa/entidad leen etiquetas emitidas por otras organizaciones con las que no se tiene un acuerdo para tal fin?	Si
		4.¿Está claramente indicada la presencia de lectores RFID?	Si

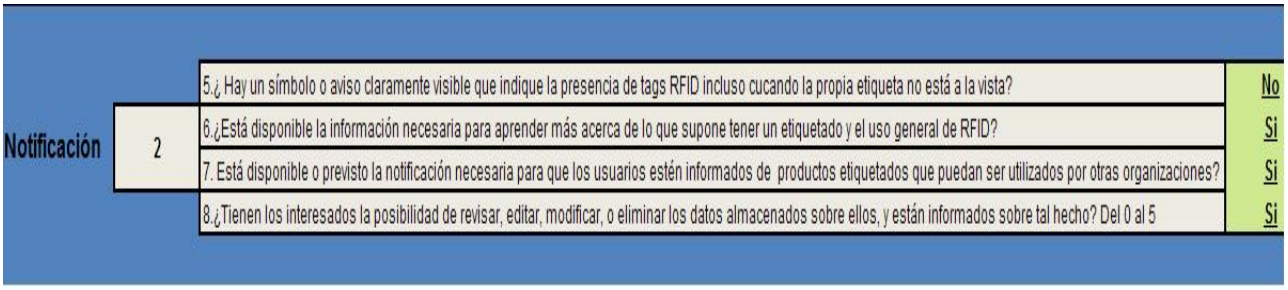
Ilustración 16: Recopilación

NOTIFICACIÓN

Este apartado se refiere al nivel de comunicación que hay entre la empresa y el cliente, sobre la existencia y funcionamiento de RFID. Como hemos visto el cliente debe ser avisado en todo momento si hay alguna operación que va a afectar a sus datos, o la zona donde se van a leer las etiquetas , o su tarjeta de crédito. Además se evalúa el nivel de disposición que tienen los datos para los clientes, en aspectos como la eliminación o modificación de aquellos que considerara críticos y estuvieran relacionados con su privacidad.

Además de requisitos que son considerados imprescindibles, se incorporan algunas preguntas que ayudan al operador a detectar posibles mejoras en su sistema o marco general. Por ejemplo en este punto se pregunta sobre la existencia

de una posible documentación o información para el usuario en cuanto a la tecnología y proceso seguido en el uso de RFID, lo que se supone creará una idea más clara en el cliente reforzando la imagen percibida de la empresa, y una difusión del uso de RFID.

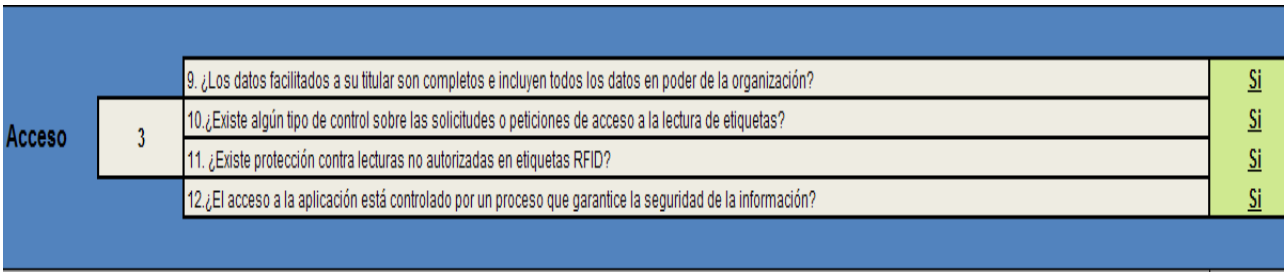


Notificación	2	5.¿ Hay un símbolo o aviso claramente visible que indique la presencia de tags RFID incluso cucando la propia etiqueta no está a la vista?	No
		6.¿Está disponible la información necesaria para aprender más acerca de lo que supone tener un etiquetado y el uso general de RFID?	Si
		7. Está disponible o previsto la notificación necesaria para que los usuarios estén informados de productos etiquetados que puedan ser utilizados por otras organizaciones?	Si
		8.¿Tienen los interesados la posibilidad de revisar, editar, modificar, o eliminar los datos almacenados sobre ellos, y están informados sobre tal hecho? Del 0 al 5	Si

Ilustración 17: Notificación

ACCESO

En este punto se pretende tener en cuenta la seguridad en torno a los datos que están contenidos en las etiquetas, la forma en que es accesible la aplicación y la forma en que son protegidas las etiquetas ante lecturas no autorizadas. Se considera que con las siguientes preguntas se puede dar un diagnóstico general, y detectar si hay alguna deficiencia grave en el sistema.



Acceso	3	9. ¿Los datos facilitados a su titular son completos e incluyen todos los datos en poder de la organización?	Si
		10.¿Existe algún tipo de control sobre las solicitudes o peticiones de acceso a la lectura de etiquetas?	Si
		11. ¿Existe protección contra lecturas no autorizadas en etiquetas RFID?	Si
		12.¿El acceso a la aplicación está controlado por un proceso que garantice la seguridad de la información?	Si

Ilustración 18: Acceso

SEGURIDAD

El concepto de seguridad asociado directamente con la aplicación RFID y el sistema en general está muy ligado a las etiquetas. La razón es que es el contenedor portátil de datos del producto, y si de alguna manera pueden ser extraídos y poner en riesgo datos confidenciales se ha de tener unas medidas de seguridad adecuadas.

En una de las cuestiones se pregunta sobre la distancia a la que es posible leer las etiquetas, no es un factor determinante en la seguridad, pero si se deben tener en cuenta varias medidas dependiendo si la distancia es fácilmente alcanzable por lectores ajenos, en tal caso es altamente recomendable utilizar dispositivos como un firewall RFID, o guardianes que interfieran en posibles lecturas externas. También es importante saber si las etiquetas están integradas en el artículo vendido y si se sigue algún tipo de procedimiento general para separar o evitar que el cliente porte innecesariamente con etiquetas tras la compra.

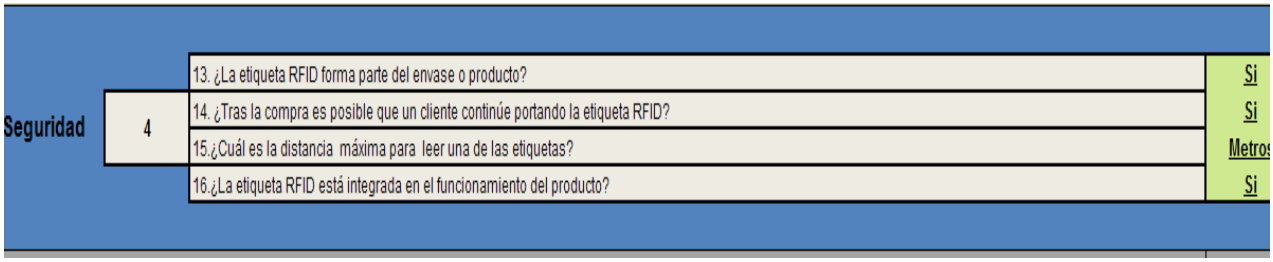


Ilustración 19: Seguridad

PRIVACIDAD

En estas preguntas se recoge el grado de criticidad de los datos que están almacenados en las etiquetas. Trabajar en una aplicación RFID con datos privados situados en las etiquetas no supone directamente un problema, pero si aumenta considerablemente el riesgo de ser víctima de un intento de ataque, por lo que se asignará un riesgo mayor a aquellos sistemas que trabajen con datos privados en las etiquetas. La propia Unión Europea recomienda no hacer esto de forma directa, sino enlazando un identificador almacenado en la etiqueta, con los datos privados almacenados dentro de la aplicación.

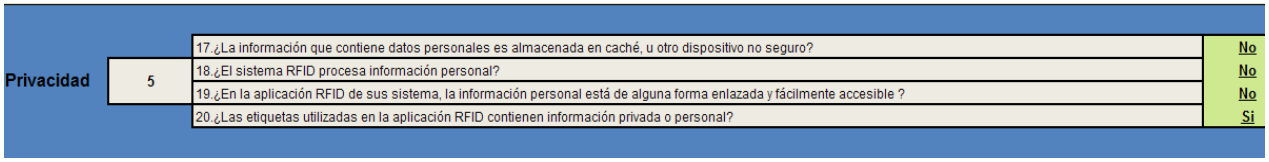


Ilustración 20: Privacidad

6.2 FUNCIONAMIENTO GENERAL DE LA EVALUACIÓN

El proceso que sigue la evaluación, consta de las siguientes partes:

1. Realización del test de 20 preguntas, dividido en 5 áreas.
2. Evaluación de las respuestas.
3. Generación automática de un informe exponiendo los porcentajes de riesgo por área y dando un breve diagnóstico subdividido por cada categoría de seguridad.

Uno de los objetivos del sistema de evaluación es proporcionar una sencilla y rápida herramienta al operador RFID, que será el usuario de la misma, por ello solo tendrá que abrir el archivo donde se encuentra el test de 20 preguntas, separadas en los distintos apartados de estudio (Recopilación, Acceso, Notificación, Seguridad, Privacidad), en las que se podrá contestar con unos valores dados.

Area de Riesgo	#	Cuestiones	Respuestas
Recopilación	1	1.¿El tratamiento de datos se realiza de acuerdo a una política definida basada en el tratamiento legal y lícito de los datos, reflejado en los requisitos legales?	Si
		2.¿Hay definidas medidas para promover la calidad de los datos?/¿Evitar la evasión de datos?	Si
		3.¿Los lectores de su empresa/entidad leen etiquetas emitidas por otras organizaciones con las que no se tiene un acuerdo para tal fin?	Si
		4.¿Está claramente indicada la presencia de lectores RFID?	Si
Notificación	2	5.¿ Hay un símbolo o aviso claramente visible que indique la presencia de tags RFID incluso cucando la propia etiqueta no está a la vista?	No
		6.¿Está disponible la información necesaria para aprender más acerca de lo que supone tener un etiquetado y el uso general de RFID?	Si
		7. Está disponible o previsto la notificación necesaria para que los usuarios estén informados de productos etiquetados que puedan ser utilizados por otras organizaciones?	Si
		8.¿Tienen los interesados la posibilidad de revisar, editar, modificar, o eliminar los datos almacenados sobre ellos, y están informados sobre tal hecho? Del 0 al 5	Si
Acceso	3	9. ¿Los datos facilitados a su titular son completos e incluyen todos los datos en poder de la organización?	Si
		10.¿Existe algún tipo de control sobre las solicitudes o peticiones de acceso a la lectura de etiquetas?	Si
		11. ¿Existe protección contra lecturas no autorizadas en etiquetas RFID?	Si
		12.¿El acceso a la aplicación está controlado por un proceso que garantice la seguridad de la información?	Si
Seguridad	4	13. ¿La etiqueta RFID forma parte del envase o producto?	Si
		14. ¿Tras la compra es posible que un cliente continúe portando la etiqueta RFID?	Si
		15.¿Cuál es la distancia máxima para leer una de las etiquetas?	Metros
		16.¿La etiqueta RFID está integrada en el funcionamiento del producto?	Si
Privacidad	5	17.¿La información que contiene datos personales es almacenada en caché, u otro dispositivo no seguro?	No
		18.¿El sistema RFID procesa información personal?	No
		19.¿En la aplicación RFID de sus sistema, la información personal está de alguna forma enlazada y fácilmente accesible ?	No
		20.¿Las etiquetas utilizadas en la aplicación RFID contienen información privada o personal?	Si

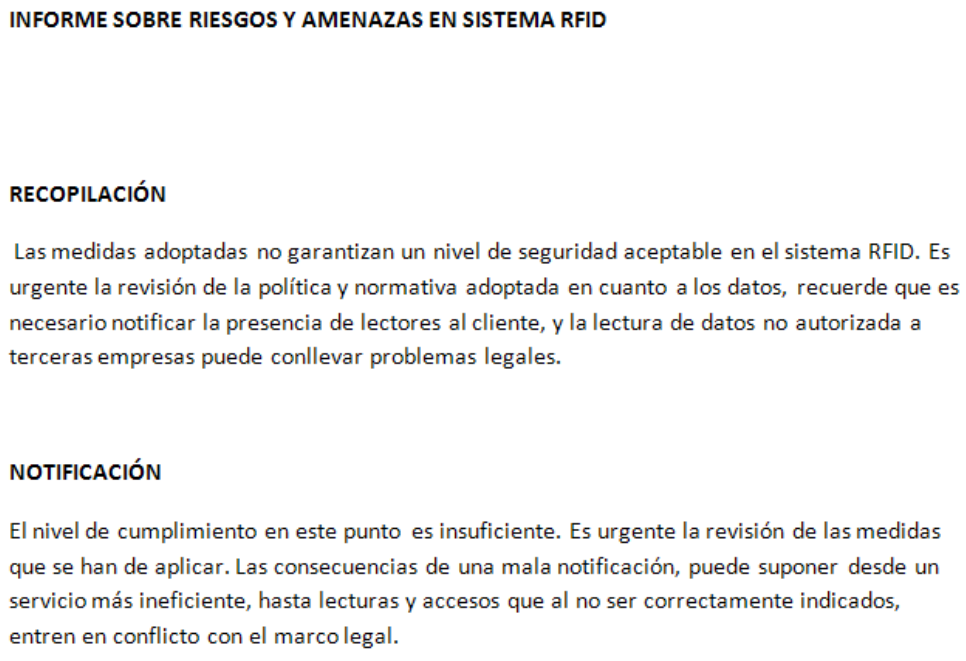
Ilustración 21: Test

A continuación el usuario tendrá pulsar con el ratón sobre el botón Evaluar que se encuentra bajo el Test.

Ilustración 22: Botón Evaluar

Automáticamente a partir de ahí el programa analiza las respuestas y genera un Informe en el que se muestra un breve diagnóstico por áreas con las sugerencias sobre seguridad y privacidad en los sistemas RFID. Además se adjunta una gráfica con el porcentaje de riesgo en cada área según las respuestas dadas.

La siguiente imagen es un fragmento de un posible Informe generado:



INFORME SOBRE RIESGOS Y AMENAZAS EN SISTEMA RFID

RECOPILACIÓN

Las medidas adoptadas no garantizan un nivel de seguridad aceptable en el sistema RFID. Es urgente la revisión de la política y normativa adoptada en cuanto a los datos, recuerde que es necesario notificar la presencia de lectores al cliente, y la lectura de datos no autorizada a terceras empresas puede conllevar problemas legales.

NOTIFICACIÓN

El nivel de cumplimiento en este punto es insuficiente. Es urgente la revisión de las medidas que se han de aplicar. Las consecuencias de una mala notificación, puede suponer desde un servicio más ineficiente, hasta lecturas y accesos que al no ser correctamente indicados, entren en conflicto con el marco legal.

Ilustración 23: Fragmento Informe

La gráfica que muestra los riesgos asociados a cada área de seguridad será similar a la siguiente:

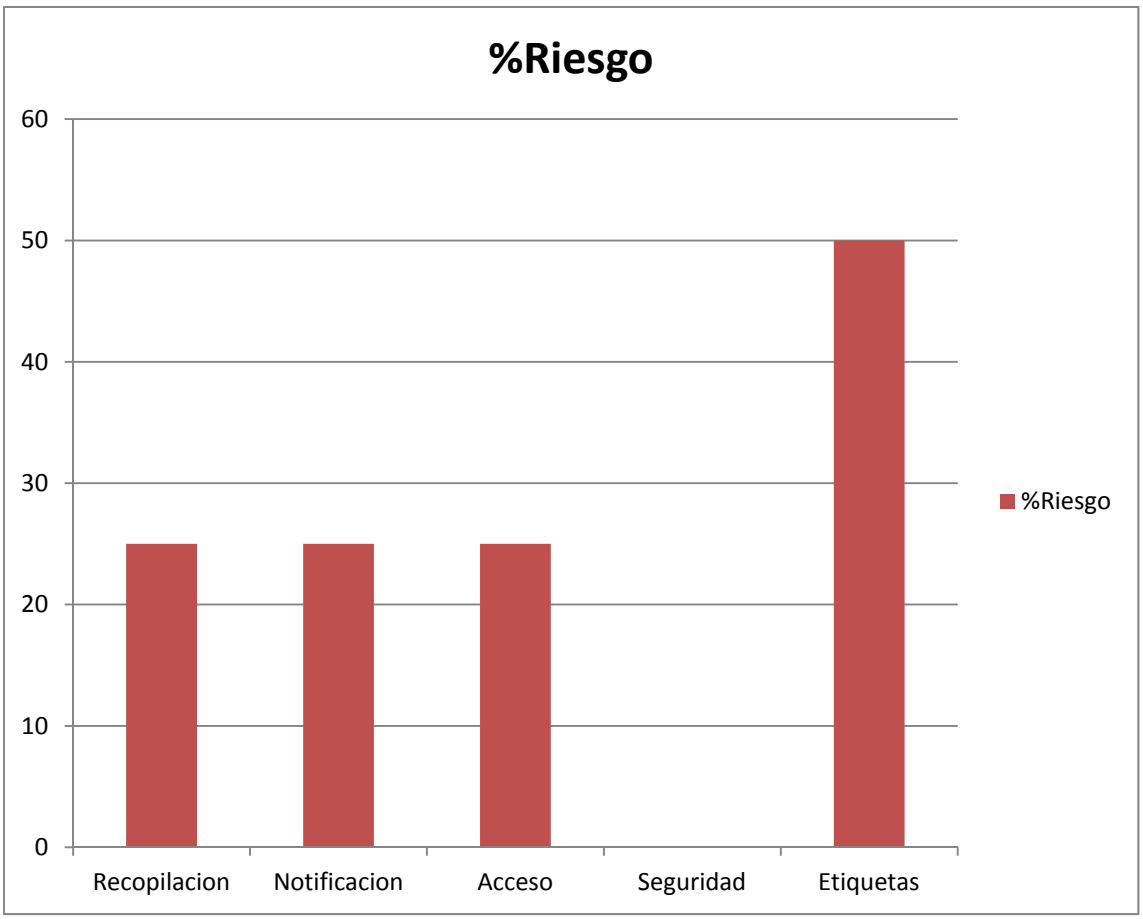


Ilustración 24: Gráfico % Asociado

Como se puede ver el tiempo y esfuerzo por parte del usuario, como la eficiencia y la sencillez en la exposición de los datos, supone una rápida herramienta para el usuario que le permite en muy pocos minutos detectar posibles carencias muy importantes en su sistema RFID.

6.3 ESPECIFICACIONES

El sistema de evaluación ha sido diseñado e implementado con herramientas de Microsoft Office. El test se encuentra en un archivo Microsoft Office Excel, versión 2007, compatible con las versiones más recientes, y la versión 2003. El programa creado analiza las respuestas y crea automáticamente un archivo Microsoft Office Word 2007.

El paso intermedio entre el test, y la evaluación junto con la creación del informe está implementado con un sistema de macros programado en Visual Basic. Es un lenguaje de programación dirigido por eventos, lo que significa que la estructura y la ejecución de las subrutinas y funciones están determinados por los sucesos que ocurren en el sistema y que van a estar dirigidos o provocados por el mismo usuario. Una de las características de Visual Basic es el acceso a casi la totalidad de librerías con las que se puede operar con el propio sistema operativo, o enlazar operaciones con otros programas, estas librerías son denominadas DLL (Dynamic Link Library).

6.3.1 ESPECIFICACIONES PARA EL CORRECTO FUNCIONAMIENTO

Para que el sistema de evaluación funcione correctamente es necesario tener habilitados algunos parámetros en los programas utilizados.

HABILITAR MACROS EXCEL

En primer lugar es necesario tener habilitada en el menú Excel la ejecución de macros. Para ello seguiremos los siguientes pasos en Microsoft Office Excel 2007:

1. Abrir Microsoft Office Excel.
2. Acceder al menú Botón de Office en la esquina superior izquierda:

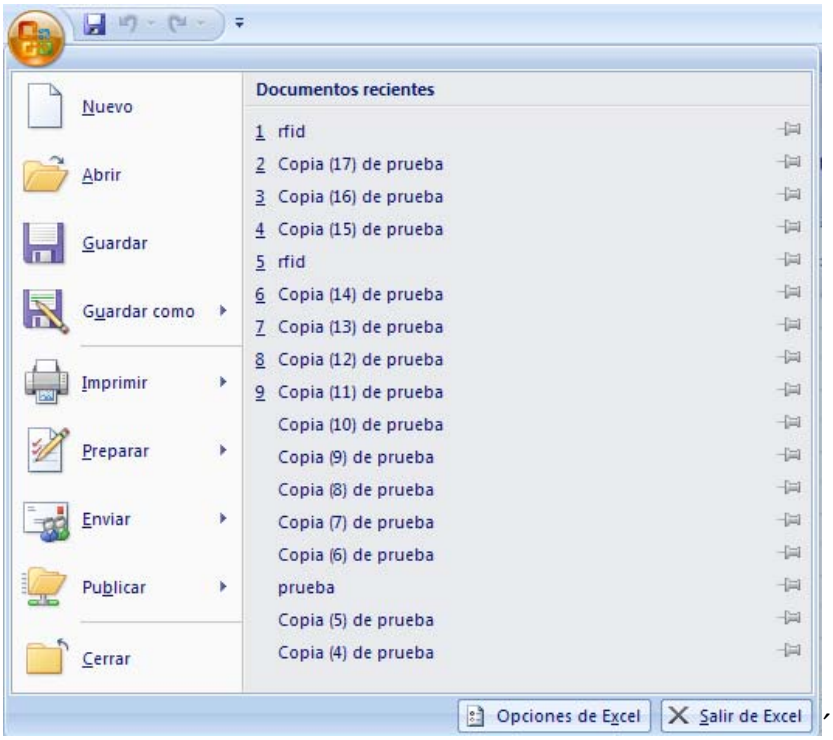


Ilustración 25: Configuración Macro

3. En el menú desplegado se pulsa sobre “Opciones de Excel”

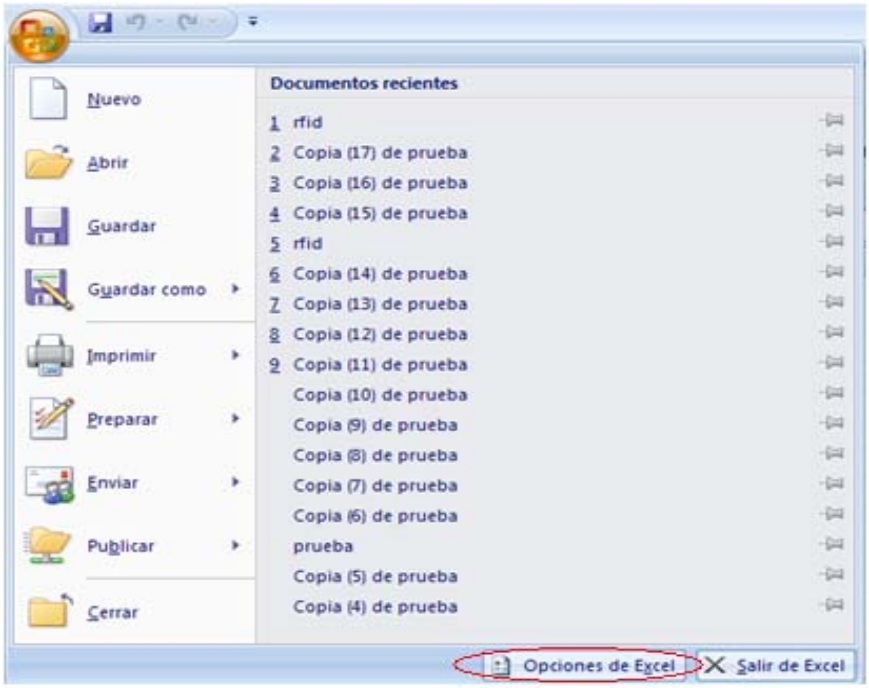


Ilustración 26: Configuración Macro

4. Una vez situados en el siguiente menú pulsamos “Centro de Confianza”

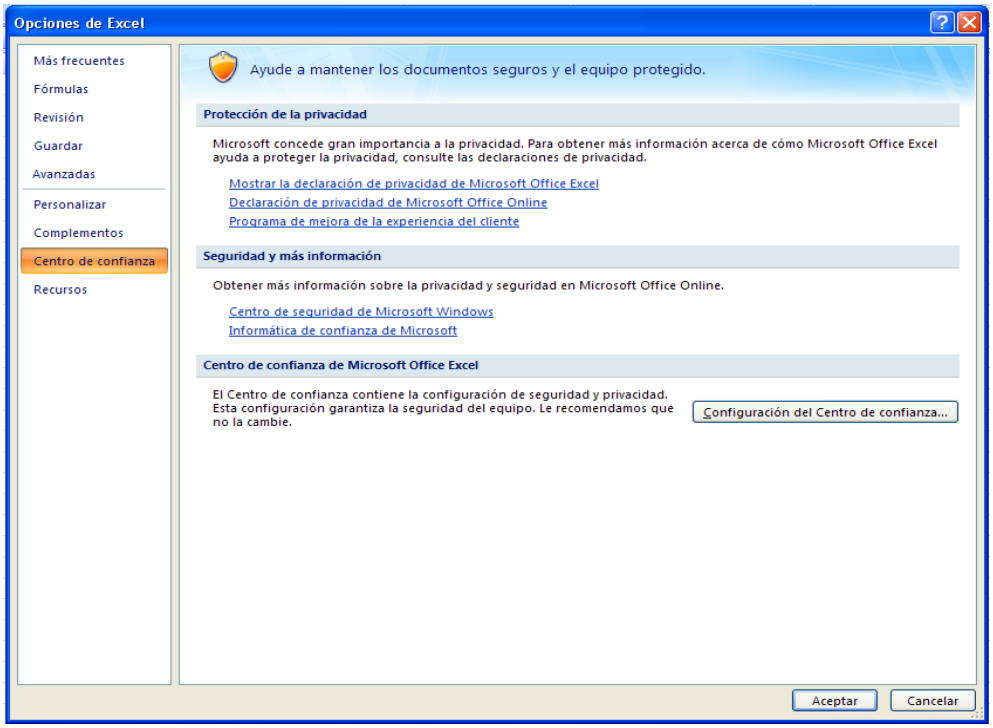


Ilustración 27: Configuración Macro

5. Accedemos a la opción “Configuración del Centro de confianza…”

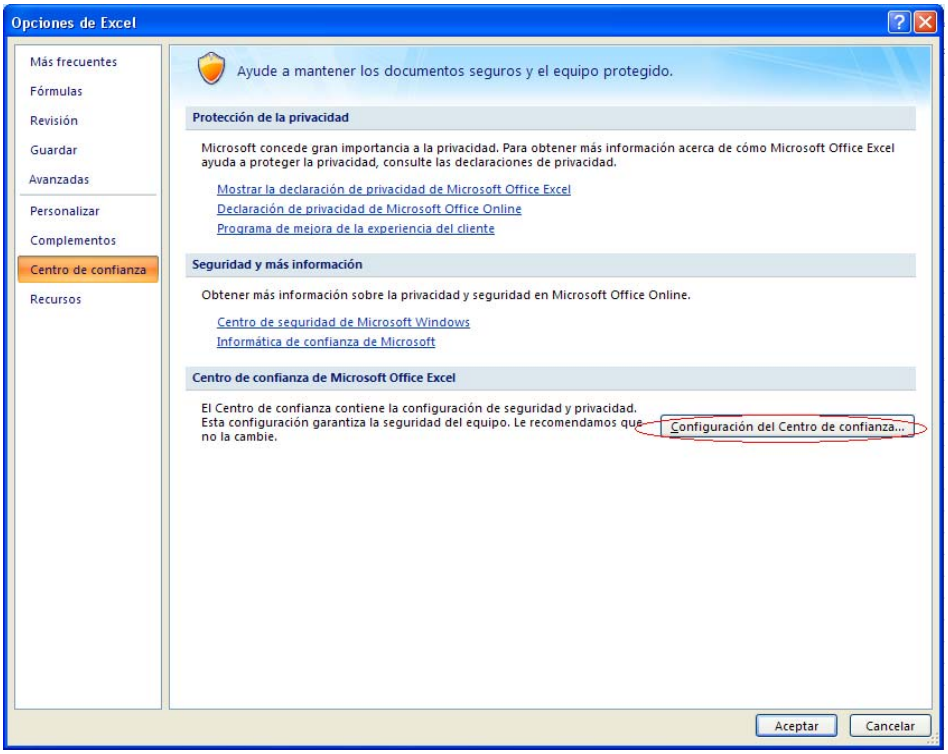


Ilustración 28: Configuración Macro

6. Cuando accedemos a la siguiente pantalla pulsar sobre la opción "Configuración de macros" y a continuación "Habilitar todas las macros" que aparece en la lista de opciones de la derecha, finalmente "Aceptar".

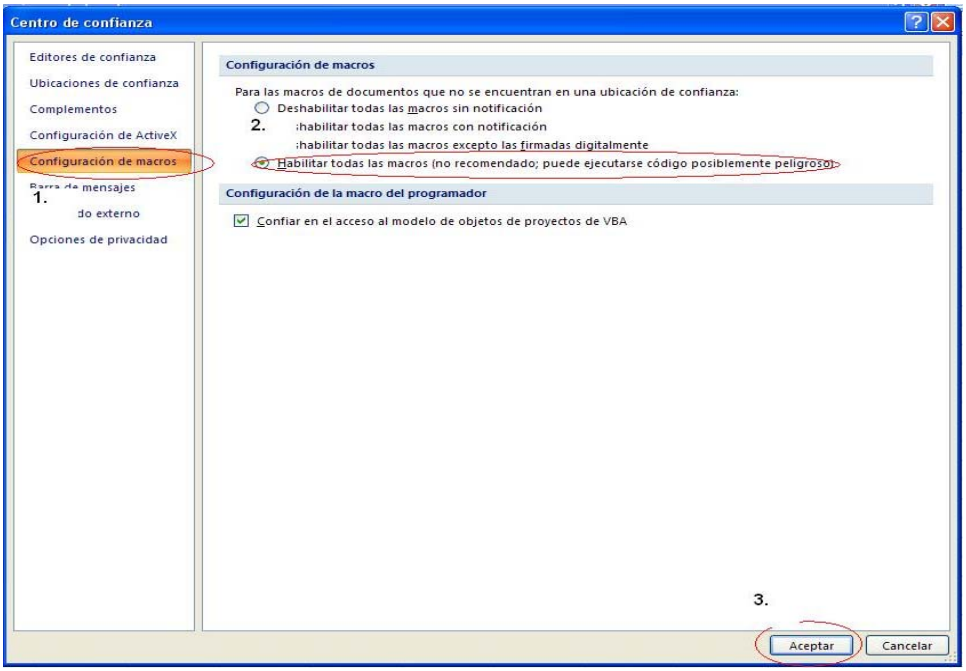


Ilustración 29: Configuración Macro

HABILITAR LIBRERÍA WORD EN MENÚ DE MACROS

Además de trabajar con las librerías Excel que están incluidas de forma predeterminada en el programa, es necesario incluir la librería Word de la forma que explicamos a continuación. La razón es que creamos el informe con un documento Word desde Excel.

Pasos:

1. Desde el editor de Macros de Microsoft Office Excel, pulsar la pestaña "Herramientas" y a continuación la opción "Referencias" del menú desplegable:

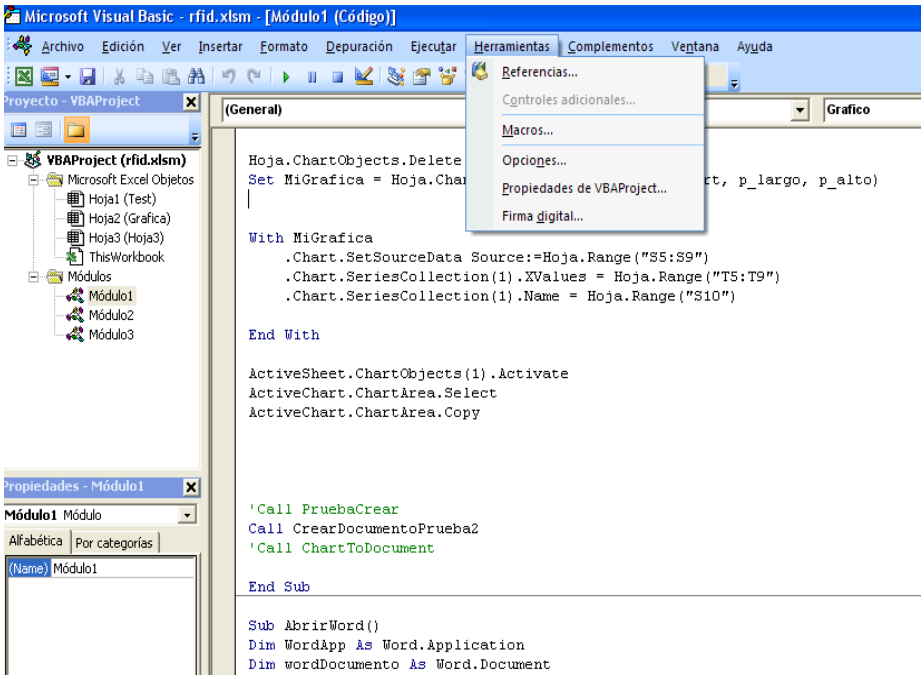


Ilustración 30: Configuración Librerías

2. A continuación aparecerán las librerías que tenemos activadas , y todas las que están disponibles, en esa lista debemos tener marcadas las que

aparecen a continuación, siendo imprescindible además de las que aparecerán por defecto seleccionadas, tener incluida la librería "Microsoft Word 12.0 Object Library (el número de versión no debería suponer un problema si es anterior o más avanzado).

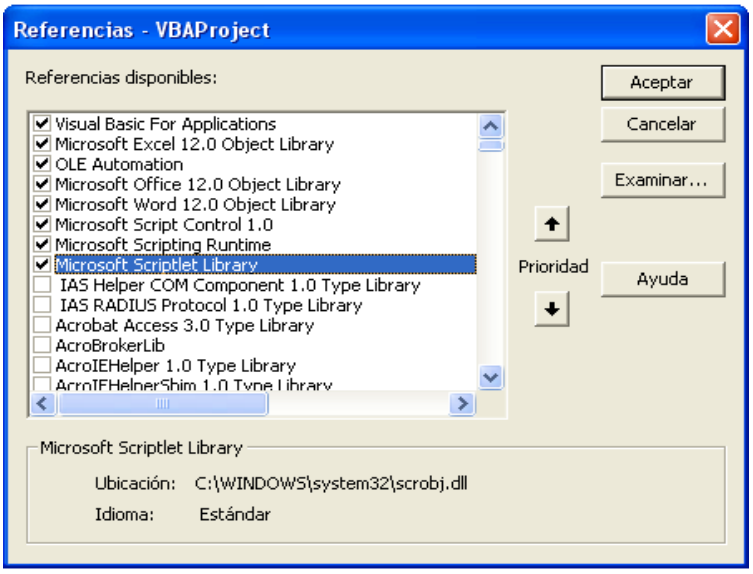


Ilustración 31: Configuración Librerías

CAPÍTULO 7. GESTIÓN DEL PROYECTO

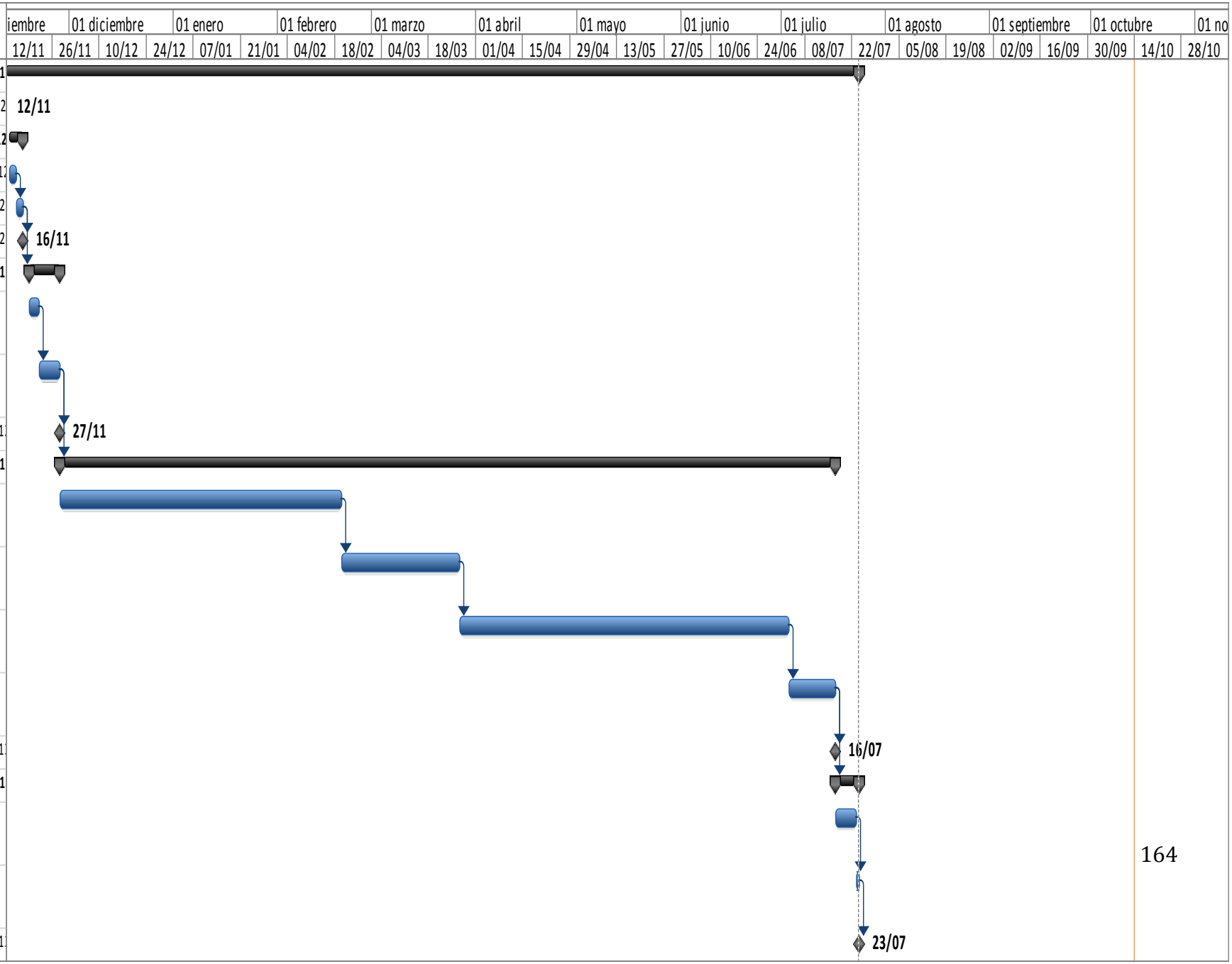
7.1.1 PLANIFICACIÓN INICIAL DEL PROYECTO

La duración estimada inicialmente del proyecto estaba fijada en 182 días. En un principio la fecha estimada para la entrega del proyecto se situaba a finales de Julio.

El Gantt con la planificación inicial se encuentra en la siguiente página.

Diagrama Gantt:

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Proyecto RFID**	**182 días**	**lun 12/11/12**	**mar 23/07/13**
2	ANALISIS DEL PROYECTO	0 días	**lun 12/11/12**	lun 12/11/12
3	**Análisis del Proyecto**	**4 días**	mar 13/11/12	**vie 16/11/12**
4	Definir Objetivos	2 días	mar 13/11/12	mié 14/11/12
5	Definir Alcance	2 días	jue 15/11/12	vie 16/11/12
6	INICIO PLANIFICACIÓN	0 días	vie 16/11/12	vie 16/11/12
7	**Planificación**	**7 días**	**lun 19/11/12**	**mar 27/11/12**
8	Selección puntos del índice	3 días	lun 19/11/12	mié 21/11/12
9	Recopilación de material sobre RFID	4 días	jue 22/11/12	mar 27/11/12
10	INICIO DESARROLLO	0 días	mar 27/11/12	mar 27/11/12
11	**Desarrollo**	**165 días**	**mié 28/11/12**	**mar 16/07/13**
12	Obtención de información	60 días	mié 28/11/12	mar 19/02/13
13	Clasificación de la información	25 días	mié 20/02/13	mar 26/03/13
14	Construcción del documento	70 días	mié 27/03/13	mar 02/07/13
15	Verificación de la información	10 días	mié 03/07/13	mar 16/07/13
16	INICIO PRESENTACIÓN	0 días	mar 16/07/13	mar 16/07/13
17	**Presentación**	**5 días**	**mié 17/07/13**	**mar 23/07/13**
18	Elaboración de la presentación	4 días	mié 17/07/13	lun 22/07/13
19	Entrega del documento y presentación	1 día	mar 23/07/13	mar 23/07/13
20	FIN DE PROYECTO	0 días	mar 23/07/13	mar 23/07/13



7.1.2 PLANIFICACIÓN REAL

En el diagrama anterior se muestra la planificación inicial, la fecha de finalización que en principio estaba marcada se situaba en los últimos días de Julio.

Finalmente las fechas reales coinciden con las estimadas en el comienzo del proyecto, pero sufre un retraso de algo más de dos meses y medio respecto a la fecha estimada como fecha final.

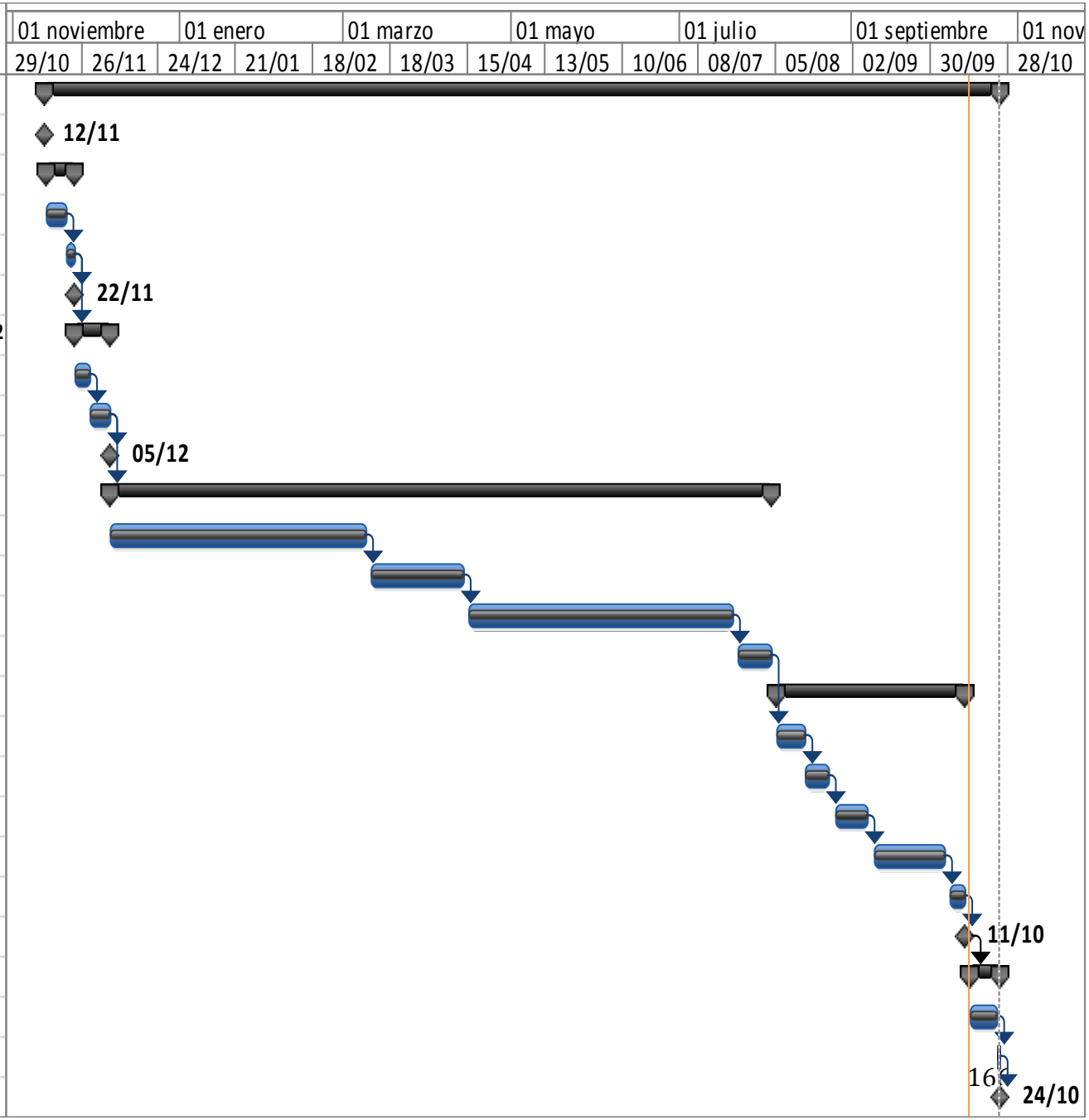
La razón más importante por la que el proyecto sufre un retraso, es la identificación a lo largo del desarrollo del estudio, de la posibilidad de aportar una aplicación que aporte una forma práctica y rápida de detectar posibles carencias en un sistema RFID. En el diagrama se pueden ver las fases totales de las que consta su desarrollo.

Además el tiempo dedicado en la mayor parte del proyecto no ha podido ser total por mi parte, debido a la realización de una beca a tiempo parcial.

A continuación se muestra el diagrama de Gantt.

Diagrama de Gantt:

Id	Nombre de tarea	Duraci	Comienzo	Fin
1	**Proyecto RFID**	**249 días**	**lun 12/11/12**	**jue 24/10/13**
2	ANALISIS DEL PROYECTO	0 días	**lun 12/11/12**	lun 12/11/12
3	**Análisis del Proyecto**	**8 días**	mar 13/11/12	**jue 22/11/12**
4	Definir Objetivos	5 días	mar 13/11/12	lun 19/11/12
5	Definir Alcance	3 días	mar 20/11/12	jue 22/11/12
6	INICIO PLANIFICACIÓN	0 días	jue 22/11/12	jue 22/11/12
7	**Planificación**	**9 días**	**vie 23/11/12**	**mié 05/12/12**
8	Selección puntos del índice	4 días	vie 23/11/12	mié 28/11/12
9	Recopilación de material sobre RFID	5 días	jue 29/11/12	mié 05/12/12
10	INICIO DESARROLLO	0 días	mié 05/12/12	mié 05/12/12
11	**Desarrollo**	**172 días**	**jue 06/12/12**	**vie 02/08/13**
12	Obtención de información	67 días	jue 06/12/12	vie 08/03/13
13	Clasificación de la información	25 días	lun 11/03/13	vie 12/04/13
14	Construcción del documento	70 días	lun 15/04/13	vie 19/07/13
15	Verificación de la información	10 días	lun 22/07/13	vie 02/08/13
16	**MACRO**	**50 días**	**lun 05/08/13**	**vie 11/10/13**
17	Análisis Requisitos y Objetivos Macro	8 días	lun 05/08/13	mié 14/08/13
18	Diseño Test	7 días	jue 15/08/13	vie 23/08/13
19	Diseño del Programa	10 días	lun 26/08/13	vie 06/09/13
20	Implementación	20 días	lun 09/09/13	vie 04/10/13
21	Pruebas	5 días	lun 07/10/13	vie 11/10/13
22	INICIO PRESENTACIÓN	0 días	vie 11/10/13	vie 11/10/13
23	**Presentación**	**9 días**	**lun 14/10/13**	**jue 24/10/13**
24	Elaboración de la presentación	8 días	lun 14/10/13	mié 23/10/13
25	Entrega del documento y presentació	1 día	jue 24/10/13	jue 24/10/13
26	FIN DE PROYECTO	0 días	jue 24/10/13	jue 24/10/13



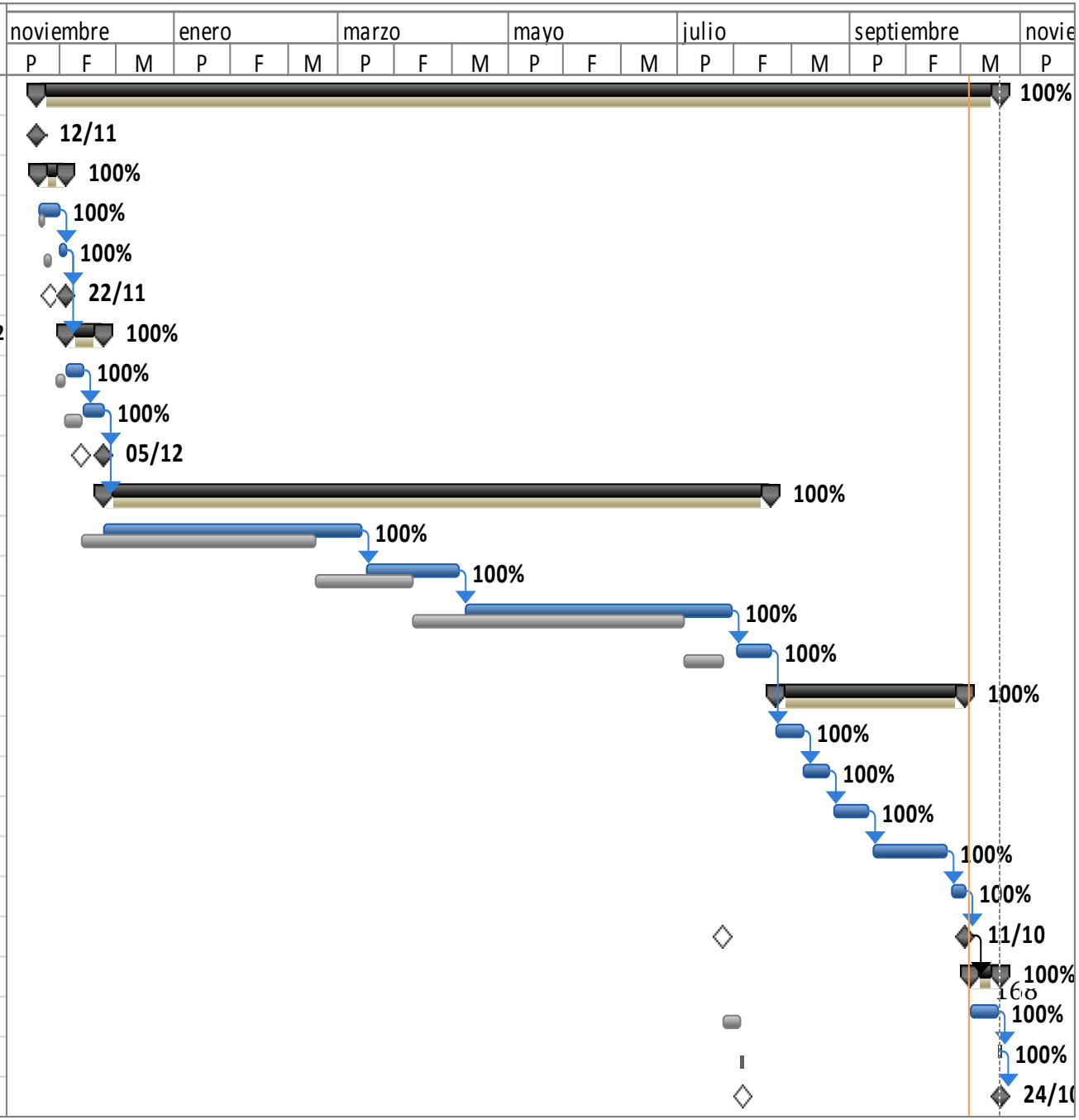
7.1.3 ANÁLISIS DE LA PLANIFICACIÓN DEL PROYECTO

A continuación se muestra una comparación mediante un diagrama Gantt entre la planificación estimada inicialmente y la que ha resultado finalmente.

Las tareas que aparecen en gris son las estimadas, y en color azul las tareas con la planificación real.

Diagrama de Gantt:

Id	Nombre de tarea	Duraci	Comienzo	Fin
1	**Proyecto RFID**	**249 días**	**lun 12/11/12**	**jue 24/10/13**
2	ANALISIS DEL PROYECTO	0 días	lun 12/11/12	lun 12/11/12
3	**Análisis del Proyecto**	**8 días**	**mar 13/11/12**	**jue 22/11/12**
4	Definir Objetivos	5 días	mar 13/11/12	lun 19/11/12
5	Definir Alcance	3 días	mar 20/11/12	jue 22/11/12
6	INICIO PLANIFICACIÓN	0 días	jue 22/11/12	jue 22/11/12
7	**Planificación**	**9 días**	**vie 23/11/12**	**mié 05/12/12**
8	Selección puntos del índice	4 días	vie 23/11/12	mié 28/11/12
9	Recopilación de material sobre RFID	5 días	jue 29/11/12	mié 05/12/12
10	INICIO DESARROLLO	0 días	mié 05/12/12	mié 05/12/12
11	**Desarrollo**	**172 días**	**jue 06/12/12**	**vie 02/08/13**
12	Obtención de información	67 días	jue 06/12/12	vie 08/03/13
13	Clasificación de la información	25 días	lun 11/03/13	vie 12/04/13
14	Construcción del documento	70 días	lun 15/04/13	vie 19/07/13
15	Verificación de la información	10 días	lun 22/07/13	vie 02/08/13
16	**MACRO**	**50 días**	**lun 05/08/13**	**vie 11/10/13**
17	Análisis Requisitos y Objetivos Macro	8 días	lun 05/08/13	mié 14/08/13
18	Diseño Test	7 días	jue 15/08/13	vie 23/08/13
19	Diseño del Programa	10 días	lun 26/08/13	vie 06/09/13
20	Implementación	20 días	lun 09/09/13	vie 04/10/13
21	Pruebas	5 días	lun 07/10/13	vie 11/10/13
22	INICIO PRESENTACIÓN	0 días	vie 11/10/13	vie 11/10/13
23	**Presentación**	**9 días**	**lun 14/10/13**	**jue 24/10/13**
24	Elaboración de la presentación	8 días	lun 14/10/13	mié 23/10/13
25	Entrega del documento y presentació	1 día	jue 24/10/13	jue 24/10/13
26	FIN DE PROYECTO	0 días	jue 24/10/13	jue 24/10/13



7.2 PRESUPUESTO

1.- Autor:

Carlos Cobos Moreno

2.- Departamento:

3.- Descripción del Proyecto:

- Titulo	**Control de los entornos de los sistemas RFID**
- Duración (meses)	**10**
Tasa de costes Indirectos:	**20%**

4.- Presupuesto total del Proyecto (valores en Euros):

Euros

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F. (no rellenar - solo a titulo informativo)	Categoría	Dedicación (hombres mes) [a)]	Coste hombre mes	Coste (Euro)
Cobos Moreno, Carlos		Ingeniero Técnico	9	800,00	7.200,00
		Hombres mes	**9**	**Total**	7.200,00

[a)] 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1575 horas)

Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (1.155 horas)

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [d)]
Ordenador HP	700,00	100	10	60	116,67
Licencia Microsoft Office	269,00	100	10	60	44,83
		100		60	0,00
		100		60	0,00
		100		60	0,00
					0,00
				Total	161,50

OTROS COSTES DIRECTOS DEL PROYECTO[e)]

Descripción	Empresa	Costes imputable
Material de oficina		150,00
	Total	150,00

6.- Resumen de costes

Presupuesto Costes Totales	**Presupuesto Costes Totales**
Personal	7.200
Amortización	162
Subcontratación de tareas	0
Costes de funcionamiento	150
Costes Indirectos	1.502
Total más IVA	9.014

CAPITULO 8 CONCLUSIONESY LINEAS FUTURAS DE TRABAJO

CAPÍTULO 8.1 CONCLUSIONES

Con la realización de este proyecto se han obtenido diversas conclusiones que se pueden agrupar en:

Conocimientos adquiridos:

- Con el desarrollo de este proyecto se han estudiado en profundidad los sistemas RFID, dando una visión general de su actual situación desde un punto de vista técnico.
- Se han analizado los sistemas RFID, los dispositivos de que consta, su modo de funcionamiento, operaciones, sus aplicaciones más importantes, y su enorme potencial de cara al futuro.
- Se han estudiado los riesgos referentes a la seguridad, que existen actualmente en torno a la tecnología RFID, de forma directa e indirecta.
- Se ha profundizado en el análisis de posibles riesgos relacionados con la privacidad de los usuarios de sistemas RFID.
- Se han estudiado las distintas normativas y se ha profundizado sobre las elaboradas y las vigentes en Europa.
- Se han analizado los puntos clave del marco legislativo que afecta y respalda la privacidad y seguridad del usuario, los

derechos en torno a los datos de los usuarios y su aplicación real para el caso específico de los sistemas RFID.

Objetivos alcanzados:

- Con la realización de este proyecto se ha desarrollado un estudio en profundidad de las características y funcionamiento de la tecnología RFID.
- Detección de las principales amenazas para la seguridad y privacidad de los sistemas de identificación por radiofrecuencia.
- La presentación de un marco con las principales metodologías y normas que permiten el desarrollo seguro desde las fases iniciales de la tecnología RFID.
- Elaboración de un plan de evaluación de seguridad y privacidad previo, durante las etapas de diseño, o aplicable a fases de remodelación o ampliación de un sistema completo, con el fin de detectar potenciales amenazas.
- Aplicación de soluciones técnicas y estructurales a los sistemas una vez evaluados.

8.2 LINEAS DE TRABAJO FUTURAS

Tras la finalización de un estudio profundo de los sistemas RFID, se procede a abrir algunas de las líneas de posibles trabajos de ahora en adelante:

- Metodologías activas en la prevención de amenazas en la seguridad RFID
- Profundización en las metodologías propuestas de prevención.
- Evolución del modelo propuesto de detección de posibles amenazas a la seguridad y privacidad de un sistema RFID.

Los puntos propuestos están referidos a posibles trabajos relacionados con el tratamiento únicamente activo de las amenazas, en el presente proyecto se habla sobre las metodologías, y normativas existentes, y sobre todo a la prevención en las fases preferiblemente iniciales de implantación de sistemas RFID.

Además se considera que se podría añadir o profundizar en alguno de los puntos presentados del proyecto y especialmente serían interesantes posibles ampliaciones en el programa implementado para informar sobre posibles amenazas, la posibilidad de desarrollarlo con más profundidad permitiendo realizar un diagnóstico en otros campos de un sistema RFID.

CAPÍTULO 9. BIBLIOGRAFÍA

- Agencia Española de Protección de Datos: Nota Informativa – "En un informe elaborado por ambas instituciones sobre seguridad y privacidad de la tecnología RFID (etiquetas de identificación por radiofrecuencia)" (INTECO, 2010)

- Agencia Española de Protección de Datos: Nota informativa - "La Comisión Europea abre una consulta pública por Internet sobre los dispositivos de identificación por radiofrecuencia (RFID)" (2006).

- Ari Juels, RSA Laboratories : "RFID Security and Privacy: A Research Survey" (2006)

- Comisión de las Comunidades Europeas: "La identificación por radiofrecuencia (RFID) en Europa: pasos hacia un marco político" (Julio 2011)

- Cristina Hernández: "Seguridad proactiva RFID"(RFID Magazine,2008)

- ETSI "Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436" (2013)

- INTECO, "Guía sobre seguridad y privacidad de la tecnología RFID" (Mayo 2010)

- Katherine Albretch: 'Spy Chips' (Plume, 2007)

- Luis Miguel Godenez González: "RFID, Oportunidades y riesgos, su aplicación práctica" (Alfaomega, 2008)

- Marc Witteman: "Attacks on Digital Passports" (SecurityLab, 2005)

- ONTSI: "La tecnología RFID: Usos y oportunidades" (2009)

- ONTSI-"Tecnologías de la Información y las Comunicaciones en la microempresa española " (2012)

- S. Srinivasan : "Security and Privacy Trade-offs in RFID Use" (2009)

- Simson L. Garfinkel: “RFID Security and Privacy” (2006)

REFERENCIAS

http://www.grupotec.com/index.php?page=activos&hl=esp

Último acceso: Septiembre 2013

http://www.dipolerfid.com/products/RFID_tags/Default.aspx

Último acceso: Septiembre 2013

http://www.oecd.org/sti/ieconomy/40892347.pdf

Último acceso: Septiembre 2013

http://www.dipolerfid.es/Productos/Lectores-RFID/Factores-Clave.aspx

Último acceso: Septiembre 2013

http://www.rfidpoint.com/fundamentos/middleware/

Último acceso: Septiembre 2013

www.alientechonology.com**Último acceso: Septiembre 2013**

http://www.identityweek.com/the-evolution-of-smartcard-and-certificate-support/**Último acceso: Septiembre 2013**

http://www.kriptopolis.org/clonar-tarjetas**Último acceso: Septiembre 2013**

http://www.forbes.com/sites/andygreenberg/2012/01/30/hackers-demo-shows-how-easily-credit-cards-can-be-read-through-clothes-and-wallets/

Último acceso: Septiembre 2013

http://wifitech.wordpress.com/rfid/**Último acceso: Septiembre 2013**

http://news.cnet.com/2010-1069-980325.html**Último acceso: Septiembre 2013**

http://www.businesswire.com/news/home/20110824006557/es/

Último acceso: Septiembre 2013

http://www.mrc.org/**Último acceso: Septiembre 2013**

http://www.morerfid.com/details.php?subdetail=Report&action=details&report_id=1328&display=RFID) **Último acceso: Septiembre 2013**

http://www.e-channelnews.com/ec_storydetail.php?ref=410057

Último acceso: Septiembre 2013

http://endthelie.com/2012/04/03/branded-how-rfid-spychips-are-being-used-by-government-and-major-corporations/#axzz2ScduruGq

Último acceso: Septiembre 2013

https://www.youtube.com/watch?v=0u4pg_XwNk8

Último acceso: Septiembre 2013

http://www.fidis.net/interactive/**Último acceso: Septiembre 2013**

http://www.commercialsecuritydevices.com/es/pasaporte_biom%C3%A9trico.html**Último acceso: Septiembre 2013**

http://www.dhs.gov/enhanced-drivers-licenses-what-are-they

Último acceso: Septiembre 2013

http://www.spychips.com/press.html**Último acceso: Septiembre 2013**

http://www.satellite-links.co.uk/directory/ero.html

Último acceso: Septiembre 2013

http://www.cept.org/ecc/tools-and-services**Último acceso: Septiembre 2013**

http://www.etsi.org/**Último acceso: Septiembre 2013**

http://europa.eu/legislation_summaries/information_society/radiofrequencies/l24120a_en.htm**Último acceso: Septiembre 2013**

http://europa.eu/legislation_summaries/information_society/strategies/n26104_en.htm**Último acceso: Septiembre 2013**

http://www.rfidineurope.eu/SR**Último acceso: Septiembre 2013**

http://www.ti.com/lit/an/sloa141/sloa141.pdf

Último acceso: Septiembre 2013

http://webstore.iec.ch/preview/info_isoiec15961%7Bed1.0%7Den.pdf

Último acceso: Septiembre 2013

http://www.rfidguardian.org/index.php/Reference_Manual:_ACL#Grammar

Último acceso: Septiembre 2013

http://www.ehowenespanol.com/proteger-tarjetas-credito-rfid-como_11860/

Último acceso: Septiembre 2013

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile

Último acceso: Septiembre 2013

http://transition.fcc.gov/cgb/spanish/**Último acceso: Septiembre 2013**

http://cafelectromagnetico.blogspot.com.es/2012/10/magnitudes-y-limites-de-radiacion.html**Último acceso: Septiembre 2013**

http://www.rfidpoint.com/fundamentos/middleware/

Último acceso: Junio 2013

www.rfidvirus.org**Último acceso: Mayo 2013**

http://www.e-channelnews.com/ec_storydetail.php?ref=410057

Último acceso: Mayo 2013

http://www.fidis.net/interactive/**Último acceso: Abril 2013**

http://www.datenschutz-bayern.de/technik/orient/oh_rfid_eu2009recommendation.pdf

Último acceso: Septiembre 2013

http://europa.eu/legislation_summaries/information_society/radiofrequencies/l24120a_en.htm**Últimoacceso: Septiembre 2013**

http://europa.eu/legislation_summaries/information_society/strategies/n26104_en.htm**Último acceso: Septiembre 2013**

http://www.rfidineurope.eu/SR**Último acceso: Septiembre 2013**

http://www.ti.com/lit/an/sloa141/sloa141.pdf

Último acceso: Septiembre 2013

http://webstore.iec.ch/preview/info_isoiec15961%7Bed1.0%7Den.pdf

Último acceso: Septiembre 2013

http://www.cs.vu.nl/~melanie/rfid_guardian/papers/lisa.06.pdf

Último acceso: Septiembre 2013

http://www.rfidguardian.org/index.php/Reference_Manual:_ACL#Grammar

Último acceso: Septiembre 2013

ANEXO I HISTORIA, ANTECEDENTES Y FUNDAMENTOS DE LA RADIO FRECUENCIA

En este punto se hará un repaso de los antecedentes e historia de la radiofrecuencia.

Para entender la radiofrecuencia, antes tenemos que hablar sobre la energía electromagnética. Los científicos resumen la creación con una gran explosión llamada Big Bang.

Como breve explicación científica podemos decir que el electromagnetismo sobrevive hasta nuestros días como resultado del Big Bang en forma de microondas debido a que en los primeros segundos del origen del universo, los protones, neutrones y electrones comenzaron la formación del universo chocando con los fotones (elementos de los cuantos de la energía electromagnética) convirtiendo así la energía en masa.

Un descubrimiento fundamental fue el del electrón, en 1897, por Sir Joseph John Thomson (1856-1940), sus investigaciones cobraron interés cuando se centró en el estudio de la medida de la carga eléctrica generada por un gas sometido a un haz de rayos X, publicado junto al físico matemático Ernest Rutherford (1871-1937).

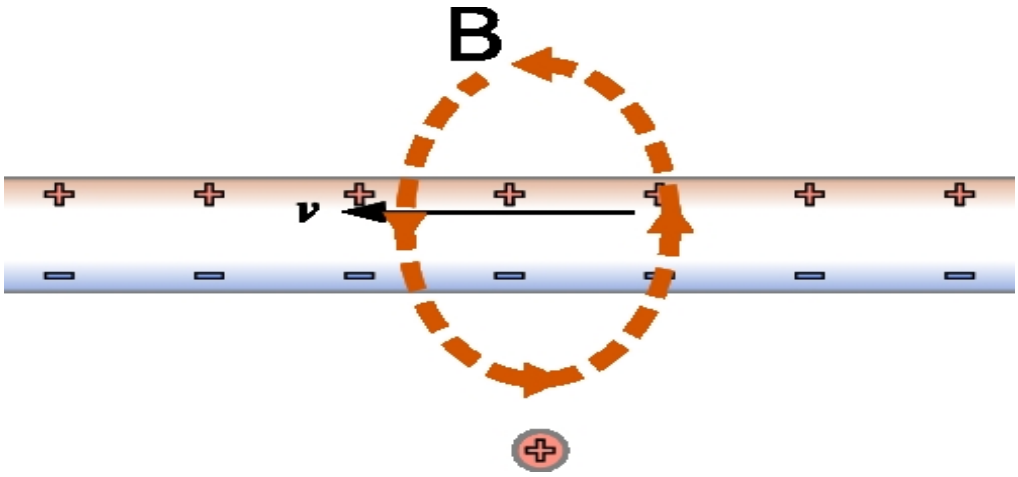
Uno de los descubrimientos más importantes de Thomson tras mejorar la técnica de realizar el vacío, fue su conclusión sobre los rayos catódicos. Descubrió que los rayos eran independientes de la naturaleza del gas de llenado de la ampolla y de la

naturaleza de los electrodos que se colocaran en ella, así como el modelo del átomo que posee un número de electrones de los que puede desprenderse con relativa facilidad, acabó con la teoría del átomo indivisible. Estos descubrimientos y el concepto "planetario" del átomo permiten a Rutherford penetrar en la naturaleza de las transformaciones radiactivas.

ONDAS ELECTROMAGNÉTICAS

La radio fue en un principio ideada por el físico y matemático James Maxwell (1831-1879) que en el año 1864 predijo la posibilidad de la radio si se empleaban frecuencias suficientemente elevadas. Está considerado el gran precursor pero desgraciadamente no pudo llegar a ver plasmadas sus teorías en la práctica, adelantándose 24 años a este hecho.

Los fenómenos eléctricos y magnéticos se unen en una misma teoría por Michael Faraday (1791-1867), y que tiene como resultado las cuatro ecuaciones que relacionan los campos eléctricos y magnéticos, son las conocidas ecuaciones de Maxwell.



El resultado es la unión de los fenómenos eléctricos y magnéticos, el electromagnetismo, que es la parte de la Física que estudia los campos eléctricos y campos magnéticos, sus interacciones sobre las sustancias sólidas, líquidas y gaseosas, y en general, la electricidad, el magnetismo y las partículas subatómicas que generan el flujo de carga eléctrica. Por tanto también estudia los fenómenos en los cuales intervienen cargas eléctricas en reposo y en movimiento, así como los relativos a los campos magnéticos y a sus efectos sobre diversas sustancias en los distintos estados.

Uno de los conceptos más importantes que podemos extraer del electromagnetismo es que no podemos estudiar los campos eléctricos y magnéticos por separado. Tal como ocurre en el fenómeno de inducción electromagnética, base para el funcionamiento de generadores eléctricos, motores de inducción eléctrica y transformadores en que un campo magnético variable produce un campo eléctrico. De una forma parecida los campos eléctricos variables generan un campo magnético.

Como vemos hay una dependencia mutua entre los dos campos, por tanto se les considera como uno solo: campo electromagnético. Esta unificación de conceptos es resultado de los descubrimientos de los científicos en el siglo XIX, y sus consecuencias fueron sumamente importantes, como la explicación de la naturaleza del fenómeno de la luz.

La naturaleza de lo que nosotros percibimos como “luz visible” es en realidad una propagación oscilatoria en el campo electromagnético, llamada onda electromagnética. Las diferentes oscilaciones tienen como resultado las diferentes formas de radiación electromagnética, desde ondas de radio (frecuencias bajas), luz visible (frecuencias intermedias), hasta rayos gamma (frecuencias altas).

A continuación un cuadro resumen con los distintos tipos de ondas, su longitud de onda comparada con objetos y cuerpos reales, así como su frecuencia y temperatura en objetos en los que es ms intensa la radiación:

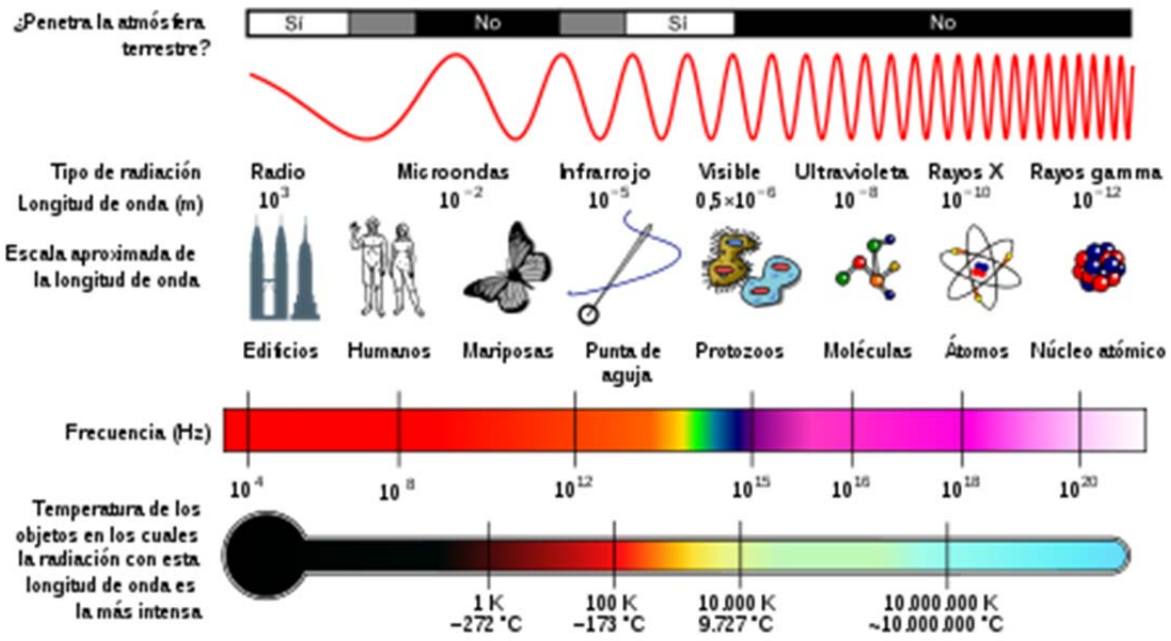


ILUSTRACIÓN 1- MODELO 2

Podemos destacar los avances del profesor de la Universidad de Bonn, Heinrich Rudolf Hertz (1857-1894) que consiguió la realización de la "teoría electromagnética de la luz" de James Clero Maxwell que trata del estudio del espacio en las proximidades de los cuerpos eléctricos y magnéticos. Esta teoría supone que en dicho espacio hay una materia en movimiento que produce los efectos electromagnéticos observados.

Uno de los hallazgos más importantes y que más nos interesan en el caso de RFID relativo a Hertz es la invención del **transmisor** y **receptor**.

El emisor:

Estaba construido con un carrete de Ruhmkorff de grandes dimensiones, al que adaptó algo parecido a una antena dipolo.

El receptor:

Poco sensible, estaba formado por un anillo abierto, entre cuyas puntas solían saltar chispas.

En 1883 se realizó una convocatoria para que se presentaran estudios sobre el campo magnético, es entonces cuando Hertz comienza a hacer experimentos al respecto. Aplicando las ecuaciones de Maxwell construyó un circuito eléctrico que podía producir ondas magnéticas, una onda era producida por cada oscilación, la radiación generada tenía una longitud de onda grande.

Construyó un receptor para constatar la presencia de la radiación. El dispositivo constaba de dos espiras entre las que existía un pequeño espacio de aire. Descubrió que al pasar corriente por la primera espira se generaba corriente en la segunda, lo que hoy llamaríamos una **antena**.

La conclusión a la que llegó fue que la transmisión de ondas electromagnéticas se generaba a través del espacio existente entre las dos espiras.

Por medio de un detector determinó la longitud de onda (66 cm), al igual que la velocidad de la luz (299.792.458 m/s).

En su época como profesor de física en Bonn logró determinar el carácter ondulatorio de los rayos catódicos así como la demostración sobre la naturaleza radiactiva electromagnética del calor.

Es así como se crearon las primeras ondas radioeléctricas (hercianas) producidas por el hombre. Todo esto contribuyó a reforzar la teoría de Maxwell que aseguraba la existencia de un espectro total de radiaciones en el que la luz visible solo

constituía una pequeña parte. Como decimos esta teoría se vio apoyada con descubrimientos como el de los Rayos X años más tarde.

Más adelante, a principios de la década 1900 fue descubierta la emisión de rayos gamma por parte de los materiales radiactivos. Fue la evidencia definitiva de la existencia del espectro electromagnético antes de ser explotado.

CLASIFICACIÓN ONDAS ELECTROMAGNÉTICAS

Las ondas electromagnéticas pueden ser descritas en términos de longitud de onda y frecuencia.

Longitud de onda: distancia entre las crestas de ondas sucesivas.

Frecuencia: cantidad de ciclos del movimiento de la onda en cualquier tiempo dado.

Existen grandísimas diferencias en estos dos aspectos entre distintos tipos de onda.

ESPECTRO ELECTROMAGNÉTICO

En un extremo del espectro están los rayos gamma, con longitud de onda 10^-12 a 10^-10 con una frecuencia de 10^22 a 10^20 por segundo, y en el extremo contrario se encuentran las ondas radioeléctricas con 10^6 longitud de onda y con frecuencia 10^4 por segundo.

Como vemos hay gran diferencia de un tipo de ondas a otras, en el caso de los rayos gamma con millonésimas de pulgada de longitud hasta las ondas radioeléctricas con longitud de onda de hasta miles de metros. En medio del espectro podemos encontrar los Rayos X, ondas ultravioleta, la luz visible, los

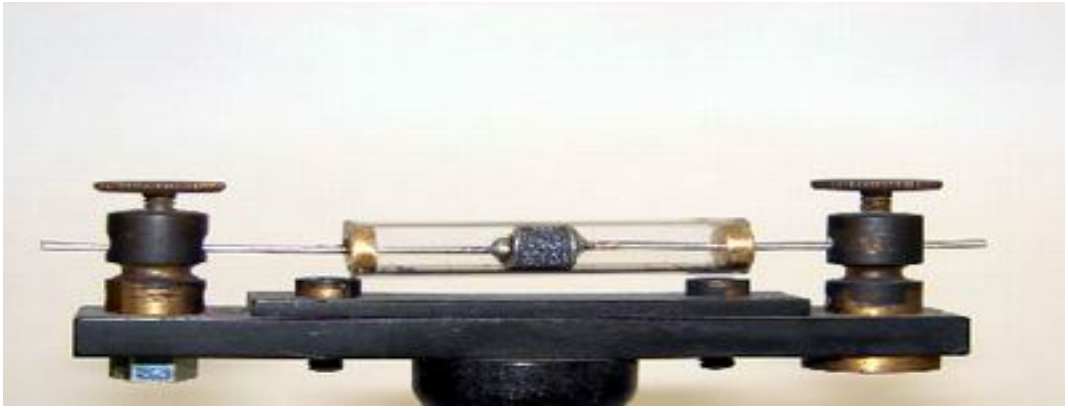
infrarrojos y por último las mencionadas ondas radioeléctricas, las cuales llenan una gran parte del espectro yendo desde las radiaciones de extremada alta frecuencia o EHF a las más largas pero de frecuencia muy baja, VLF.

Fue así como surgió el descubrimiento de las que hoy llamamos "ondas de radio". Anteriormente llamadas "ondas hercianas", es por eso que todavía hoy recordamos a su creador, llamando a la forma de medir su frecuencia en hercios (Hz), que son las oscilaciones por segundo y las frecuencias de radio en megahercios (MHz).

Más tarde se fueron sucediendo avances y mejoras de los descubrimientos ya hechos, este es el ejemplo de **Edouard Brenly (1846- 1940).** A él le debemos el invento del cohesor.

El cohesor es un objeto que consta de un tubo de cristal, dentro del cual se encuentran unas limaduras metálicas que pueden ser de hierro, y que quedan aprisionadas entre dos émbolos metálicos. Pasan de ofrecer una resistencia de pocos Ohms si son sometidos a la acción de ondas a estar muy apretadas y ofrecer altas resistencias de MOhm.

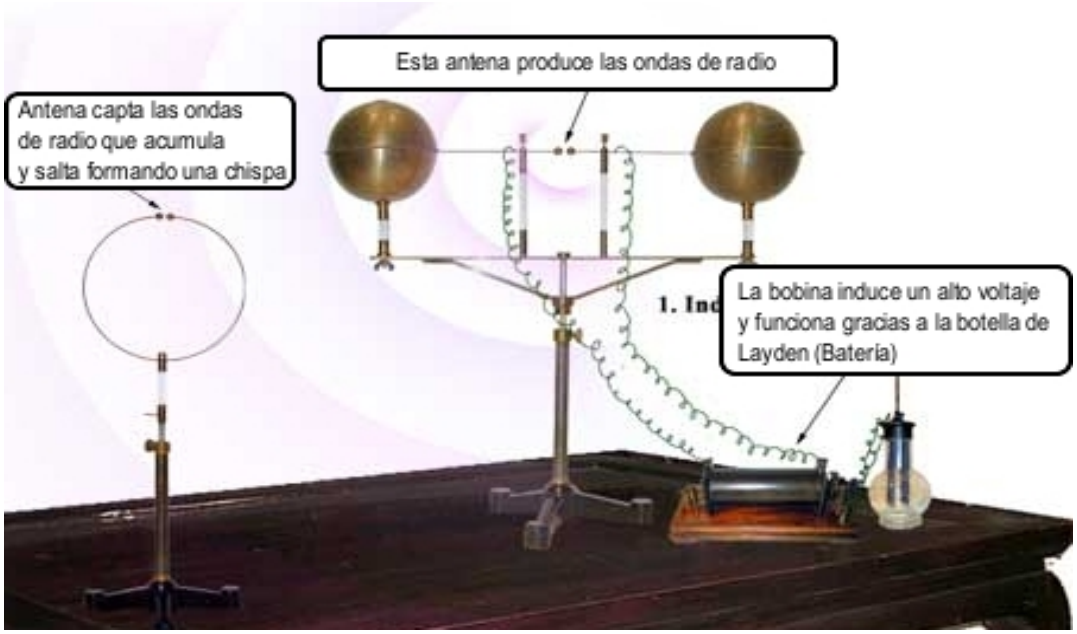
Cohesor:



Gracias a este invento de Branley se pudo realizar el primer experimento de una transmisión a distancia en el Colegio Lassalle de Paris, de una ventana a otra con un patio en medio de 20 metros de longitud.

La posibilidad de captar ondas hercianas a distancia era mayor al resonador de Hertz.

Resonador de Hertz:



Aleksandr Stepanovich Popov (1859-1905) además de utilizar el tubo de Branly como detector de tempestades, (basándose en la creación de ondas capaz de ser detectadas por el cohesor en las nubes tempestuosas), halló el mejor sistema para radiar y captar ondas: la antena originalmente constituida por hilo metálico.

Con el tiempo lo fue mejorando, por ejemplo añadiendo al sistema receptor un hilo metálico extendido en sentido vertical, así podía captar mejor las oscilaciones eléctricas al elevarse en la atmósfera. El hilo estaba unido de los polos del cohesor

en uno de sus extremos, el otro comunicaba con tierra. Con esto lo que se pretendía era captar las diferencias de potencial entre los dos extremos causadas por el paso de ondas electromagnéticas procedentes de las nubes tormentosas, cada vez que esto ocurría sonaba un timbre, si el sonido era muy continuado daba una idea del paso de la tempestad. Es así como surgió la primera antena, llamada así por su semejanza a las antenas de los buques.

En 1986 realizó la primera comunicación de señales sin hilos. Estaban constituidas por simples impulsos obtenidos mediante grandes descargas eléctricas de corriente almacenadas en condensadores.

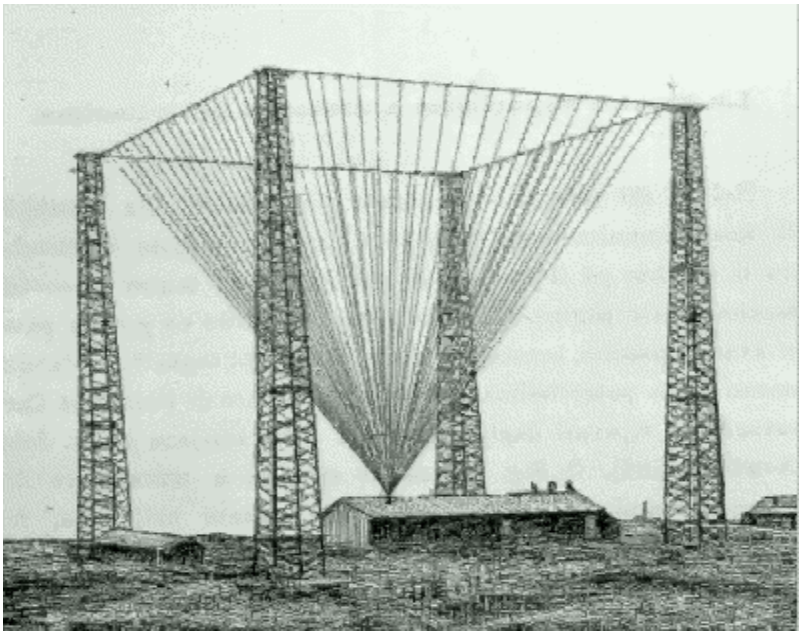
Tenemos entonces tres elementos necesarios para establecer un sistema de radiocomunicación, pero todavía era necesario encontrar un conjunto lo suficientemente seguro y fiable para poder tener aplicaciones comerciales.

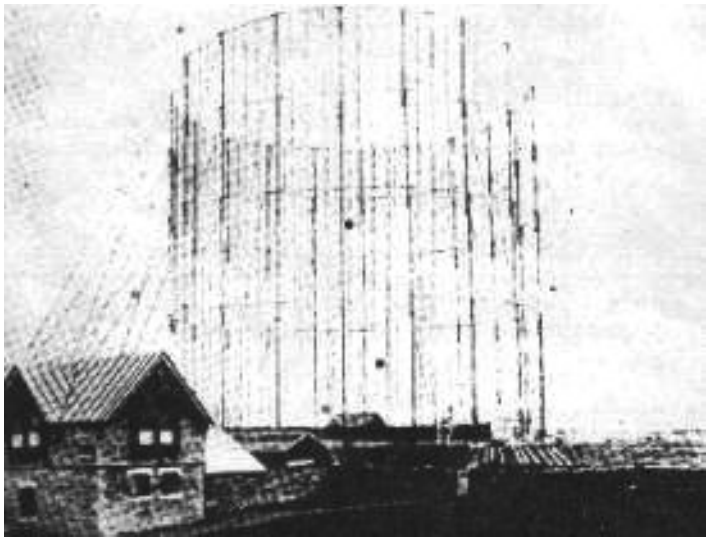
Guglielmo Marconi (1874- 1937), realizó avanzados experimentos que le llevaron a ser conocido como el inventor de la radiocomunicación.

Comenzó a la temprana edad de 20 años estudiando el fenómeno de resonancia eléctrica y logró comunicaciones a distancias de hasta 2400 metros utilizando un alambre vertical como antena en vez de anillos cortados y un detector (descubría señales muy débiles).

Fue aumentando la distancia de sus transmisiones hasta que en 1896 obtuvo la primera patente de **telegrafía inalámbrica.**

Llama la atención el tamaño de las primeras antenas instaladas por Marconi:





La razón de este tamaño, es que al principio utilizaba longitudes de onda superiores a 200 metros. El receptor basaba su funcionamiento en el cohesor del que antes hablamos. Este aparato fue perfeccionándose progresivamente, constando de un tubo de vidrio lleno de limaduras de hierro, que en presencia de una señal de alta frecuencia que procede de la antena, se vuelve conductor y da acceso a una corriente que hace sonar un timbre. Este modelo seguía teniendo un

problema, cuando la corriente desaparecía el cohesor seguía conduciendo y la única forma de evitarlo era dándole un golpe. En resumen, los sistemas de transmisión tenían un largo camino por delante hasta poder tener aplicaciones comerciales.

Se sucedieron continuos avances como la invención de un sistema de sintonía, es decir un sistema capaz de utilizar el mismo receptor para recibir distintas emisiones. El autor fue **Sir Oliver Joseph Lodge (1851 - 1940).**

Las comunicaciones se fueron haciendo a mayores distancias, llegando en 1897 a realizar la primera transmisión sobre mar entre dos buques de guerra a una distancia de 19 km.

Como curiosidad podemos citar que el primer contacto por radio en Francia fue en 1898 entre la Torre Eiffel y el Pantheon a una distancia de 4 km.

Marconi continuó con sus investigaciones y experimentos, tras algunas comunicaciones que llegaron a lograr el auxilio de la tripulación de un barco gracias a una llamada de auxilio captada por el investigador, comenzó la era de la telegrafía sin hilos. Fue en 1901, cuando el ingeniero italiano elevó una antena receptora con globos a 120 metros de altura y captó la letra S del código Morse. La emisión había recorrido alrededor de 3.600 kilómetros.

A partir de entonces comienza la experimentación a mayor escala de la telegrafía sin hilos.

Como sabemos **Thomas Alva Edison (1847 – 1931)** experimentó con varias formas de lámparas incandescentes, y llegó a la conclusión que más tarde se llamaría como “efecto Edison”.

El efecto Edison se basó en sus observaciones relacionadas con el ennegrecimiento del vidrio progresivo respecto al tiempo de funcionamiento. Pensó que podía estar

producido por la proyección de partículas por parte del filamento. En primer lugar intentó captar las partículas con resultados nulos, hasta que decidió utilizar un galvanómetro, con el que descubrió que cuando la placa era de polaridad positiva respecto al filamento había conducción de corriente, en cambio cuando era negativa no ocurría.

El descubridor del electrón **J.J Edison** continuó con las investigaciones del efecto Edison y llegó a demostrar que los filamentos de las lámparas emitían electrones.

Más tarde **Sir Owen Williams** consiguió demostrar que la emisión de electrones no se debía a una causa química sino a una aportación energética.

En 1881 **John Ambrose Fleming (1849 – 1945)** trabajador de la empresa *Edison Electric Light Company of London* investigó sobre múltiples problemas relacionados con las lámparas incandescentes. Tras estudiar lo experimentado por Edison pensó que podía aplicar el Efecto Edison como método para rectificar corrientes alternas de baja frecuencia. Años más tarde en 1886 se almacenaron todas las lámparas del laboratorio al considerar que las investigaciones no tenían aplicación práctica.

En los siguientes años, el principal problema en la radiocomunicación fue encontrar receptores más sensibles y seguros. El circuito que utilizaban no empleaba batería auxiliar y el diodo Fleming rectificaba la corriente que pasaba por los auriculares.

En 1912 la British Marcony Company sacó a la luz un receptor con detector duplicado, al que Fleming llamó erróneamente de "válvulas oscilantes" ya que estas válvulas dieron origen al diodo que se siguió utilizando hasta cincuenta años más tarde en pequeños receptores.

A la vez que ocurría todo esto, en 1900 un profesor de filosofía llamado Lee de Forest, tenía instaladas en su hogar lámparas de gas, en su dormitorio que también era usado como laboratorio, había una lámpara modelo Welsbach. El profesor

tomó nota de un suceso que no pasó por alto, había variaciones de luz en la lámpara de gas cuando transmitía su transmisor de chispa, desde entonces empezó a creer en la posibilidad de utilizar los gases incandescentes como detectores de señales inalámbricas.

Influenciado por esta idea, tres años más tarde en 1903, experimentó construyendo un circuito en base a un mechero Bunsen, y el resultado fue satisfactorio recibiendo la señal procedente de buques del puerto (T.S.H).

Por tanto fue consolidada la hipótesis planteada acerca de las propiedades eléctricas de gases calientes.

Lee fue mejorando las investigaciones, eliminando el mechero Bunchen y utilizando recipientes de vidrio que contenían gas calentado por un filamento incandescente. Como curiosidad, saber que se llamó al receptor audión, debido al "ruido" generado por las estaciones TX.

En 1906 se instaló un receptor en la base naval Key West. En el año siguiente, hizo una mejora, recubriendo el receptor con una hoja de papel de estaño y conectar la antena también a un electrodo exterior, que como resultado tuvo un efecto amplificador. Realizó similares mejoras conectando los extremos a una antena y a tierra.

Sucesivas mejoras como la implantación de una placa que conectaba a la antena y la otra a los cascos-batería-tierra, o incluirle al tubo una rejilla en zig-zag situada entre placa y filamento. Nuevos filamentos de tántalo y tungsteno en vez de filamentos de carbón, que dio como resultado el nacimiento de la lámpara tríodo, base de las posteriores lámparas tetrodo, pentodo, etc…

Desde entonces la lámpara tríodo fue utilizada con el fin de amplificar, detectar frecuencia y osciladora. A partir de este invento se pudo generar corriente de alta frecuencia con posibilidad de modularla fácilmente y dio lugar a la **radiotelefonía**.

Todo este proceso que ha sido explicado anteriormente, aunque aparentemente simple fueron los responsables de dar lugar a la radio y la electrónica revolucionando la ciencia y tecnología, y a su vez influyendo en el modo de vida del ser humano.

La tecnología que en este proyecto es objeto de estudio, RFID (Radio Frequency Identificación) es la combinación entre la radiodifusión y radar.

CAPITULO 10. GLOSARIO

A

AA: Autenticación Activa

Accenture: es una multinacional con sede en Dublín que se dedica a la consultoría, servicios de tecnología y outsourcing.

ACL: Acceso Lista de Control.

Alien Technology: proveedor de la industria RFID, con productos basados en los estándares internacionales EPCglobal y Gen2.

Application of microwave homodyne: Aplicación de microondas homodino.

AT&T: compañía Americana del sector de las telecomunicaciones.

Auto-ID Center: Antiguo organismo de investigación que designó los laboratorios Auto-ID para diseñar la arquitectura de Internet de Objetos junto a la organización EPCglobal. Se centra en el desarrollo y especialización de software y hardware para la tecnología RFID.

B

BAC: Control de Acceso Básico.

BBC (British Broadcasting Corporation): Corporación Británica de Radiodifusión, servicio público de comunicación del Reino Unido.

Bell South: compañía estadounidense del sector de las telecomunicaciones.

Big Bang: teoría inicial que trata de explica el inicio del universo como una gran explosión.

Biocompatible: se dice de la materia que no tiene efectos tóxicos y perjudiciales sobre la función biológica.

Biometría: estudio de métodos para automatizar procesos de reconocimiento único de humanos mediante rasgos de conducta o físicos.

BQ (Bequeler): unidad derivada del Sistema Internacional que mide la actividad radiactiva.

Buffer: ubicación o espacio reservado en memoria o en un dispositivo electrónico para almacenar temporalmente información digital.

C

Caso de Uso: es un diagrama que trata de representar la forma en que un cliente (actor) opera con el sistema en desarrollo, intentando mostrar, la forma, el tipo y orden en que los elementos interactúan.

CASPIAN (Consumers Against Supermarket PrivacyInvasion and Numbering): Consumidores Contra la Invasión de la Privacidad y Numeración en los Comercios, como su nombre indica es una asociación de consumidores en contra de las tecnologías relacionadas con la identificación que según su criterio suponen una amenaza para la privacidad.

CIP (Competitiveness and Innovation framework Programe): Marco para el Programa de Innovación y Competitividad de la Comisión Europea, tiene como objetivos mejorar la competitividad de las empresas europeas frente a los desafíos de la globalización.

Color Moist Hazelnut: nombre comercial de una barra de labios.

Comisión Europea (CE): órgano ejecutivo de la Unión Europea, tiene la función de proponer la legislación y aplicación de las decisiones, defender los tratados de la Unión y del transcurso general de la Unión Europea.

Criptosistema: conjunto de transformaciones de texto claro en texto cifrado y viceversa, en la que la transformación o transformaciones que se han de utilizar son seleccionadas por claves. Las transformaciones son definidas normalmente por un algoritmo matemático.

CVV (Card Verification Value): valor de verificación de la tarjeta, sistema de seguridad contra el fraude en tarjetas de crédito.

D

DBm: unidad de medida de nivel de potencia, decibelios.

Department of Homeland Security: Departamento de Seguridad Nacional, referido a los Estados Unidos, es un ministerio del Gobierno de este país con responsabilidades sobre el protectorado del territorio de ataques exteriores y desastres naturales.

DES (Data Encryption Standard): esquema de encriptación simétrico, creado con el objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de ordenadores, sometido a las leyes de USA y basado en la aplicación de todas las teorías criptográficas que existen hasta el momento.

DoS Ataque de Denegación de Servicio: en el contexto de seguridad informática se entiende como un ataque a un sistema o red que consigue que un servicio o recurso sea inaccesible a los usuarios legítimos. Las consecuencias suelen ser la pérdida de conectividad a la red por consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos del sistema del a víctima.

E

EAC: Control de Acceso Extendido.

EAN (European Article Number): traducido como Numero de Artículo Europeo, y ahora renombrado para su uso en todo el mundo como International ArticleNumber, se refiere al estándar para la identificación de productos conocido como código de barras.

ECC (Electronic Communication Committee): Comité de Comunicación Electrónica, organismo relacionado con ERO. Comité.

Electromagnetismo: de la física donde se estudia de manera conjunta la parte eléctrica y magnética, se considera fundadores de esta teoría a Michael Faraday y James Clerk Maxwell.

Electrón: partícula elemental estable cargada negativamente que constituye una de las partes fundamentales del átomo.

End to end: se puede traducir como principio de extremo a extreme aplicado a las redes de computadores. El principio afirma que las funciones específicas de la aplicación deben residir en los hosts finales de una red y no en los nodos intermedios.

EPC (Electronic Product Coda): Código electrónico de producto.

ERO (European Radiocommunications Office): Oficina Europea de Radiocomunicaciones, fundada en 1991, con base en Dinamarca y es uno de los organismos oficiales de la Unión Europea para la regulación de los aspectos sobre radio y telecomunicaciones.

ETSI (European Telecommunications Standard Institute): Instituto Europeo de Normas de Telecomunicaciones, organización dedicada el desarrollo de estándares para el campo de las telecomunicaciones.

European Parlament: Parlamento Europeo.

Estados Miembros (Unión Europea): Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia ,Dinamarca , Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia,

Grecia, Hungría ,Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumania, Suecia.

F

FCC (Federal Communications and Commissions): Comisión Federal de Comunicaciones, es una agencia estatal independiente de Estados Unidos bajo la responsabilidad del Congreso, encargada de la regulación de telecomunicaciones interestelares e internacionales por radio, televisión , redes inalámbricas, teléfonos, satélite y cable.

Firma digital: mecanismo criptográfico que permite en la transmisión de un mensaje cifrado, que el receptor determine la identidad mediante una autenticación de origen confirmando que no ha sido modificado ni alterado.

Frequency Shift Keying (Frequency Shift Keying): Modulación por desplazamiento de frecuencia, técnica de transmisión digital de información binaria utilizando dos frecuencias distintas.

Friendo or Foe (IFF): sistema de comunicación por radio entre lector y transpondedor de uso militar y para diferenciar aviones enemigos de aviones amigos.

FSA (Freedman, Sharp, Associates): corporación que se dedica al desarrollo de software de seguridad.

FIDIS (Future of Identify in the Information Society): traducido como Futuro de la Identificación en la Sociedad de la Información, se encuentra dentro del marco de Investigación y Desarrollo Tecnológico en las Tecnologías de la Sociedad de la Información (IST), se centra sobre todo en temas de seguridad.

G

Gillette: marca que se dedica actualmente a la comercialización de productos de higiene masculina, fundada en 1901.

H

Hardware: todas las partes físicas que componente un sistema informático (eléctricos, electrónicos, electromecánicos y mecánicos).

Header (cabecera): en un contexto tecnológico, se refiere a datos complementarios situados al principio de un bloque de datos que son almacenados o transmitidos, normalmente después de esta cabecera vienen los llamados datos útiles.

Hercio (Hz): es la unidad de frecuencia en el Sistema de Unidades Internacional, es el número de ciclos por segundo de un fenómeno periódico.

High Frequency (HF): traducido Altas Frecuencias, es el intervalo de frecuencias referido al espectro electromagnético que se encuentra entre los 3MHz a 30MHz.

I

IBM: multinacional Americana dedicada a la tecnología y consultoría, fabrica y comercializa hardware y software, ofrece infraestructuras, hosting y servicios de consultoría en una gran variedad de áreas.

ICAO (Organización de la Aviación Civil Internacional): se ocupa de estudiar problemas relacionados con la aviación civil internacional y promover reglamentos y normas relacionados con el área aeronáutica.

IClass (IC): tipo de tarjetas inteligentes que incluyen tecnología que hace capaz de múltiples aplicaciones como autenticación biométrica o ventas sin efectivo.

ICNIRP (Commissionfor non-ionizozing Radiation Protection): Comisión Internacional de Radiación No Ionizante, su función es la de controlar y regular normas sobre temas relacionados con la radiación y la población.

Identificación unívoca: método que asigna una identidad única a cada sujeto.

IEC (International Electrotechnical Comission): Comisión Electrotécnica Internacional, organización dedicada al desarrollo de normas en áreas relacionadas con distintos campos (tecnologías, electricidad, todo lo relacionado con lo electrónico).

IPhone: marca comercial del teléfono móvil producto de la empresa Apple.

ISM (Industrial – Scientific – Medical): Bandas reservadas de radiofrecuencia electromagnética exclusivamente para uso industrial, científico y médico.

ISO: Organización Internacional de Normalización fundada en el año 1947 y su función principal desde entonces es la de promover el desarrollo de normas de fabricación para todo el mundo.

ISOGON CORPORATION: empresa del sector de las Tecnologías de la Información que ofrece soluciones de administración y gestión.

J

Jaula de Faraday: caja metálica que tiene como fin proteger campos eléctricos estáticos.

JPEG/JPEG2000 (Joint Photographic Experts Group): las siglas se traducen como Grupo Conjunto de Expertos en Fotografía, y se refiere a un estándar de compresión y codificación de imágenes digitales.

K

Kg: Kilogramo unidad de masa del Sistema Internacional

KILL: matar, es un comando utilizado en sistemas RFID para desactivar una etiqueta.

L

Longitud de Onda: distancia entre un pulso y otro de una onda.

LOPD: Ley Orgánica de Protección de Datos, ley española.

Los Alamos Scientific Laboratory: Laboratorio Científico Los Álamos fundado en 1943 situado en Estados Unidos fundado en 1943 y actualmente perteneciente al Departamento de Energía de su país.

Low Frequency (LF): traducido Bajas Frecuencias, es el intervalo de frecuencias referido al espectro electromagnético que se encuentra entre los 30 kHz y 300kHz.

M

Memoria EEPROM: las siglas se corresponden con Electrically Erasable Programmable Read-Only Memory (Memoria de solo lectura, programable y borrada eléctricamente). Memoria no volátil.

Memoria RAM: Memoria de acceso aleatorio (Random Access Memory)

Memoria ROM: Memoria de solo lectura (Read Only Memory)

Mensajes encriptados: se suele utilizar también cifrado, mensaje cifrado.

MHz: símbolo en el Estándar Internacional para el megahercio.

Microwave :microonda, ondas electromagnéticas definidas en un rango de frecuencia determinado dependiendo de los estándares y de longitud de onda entre 1m y 1mm.

Microwave Institute Foundation: Fundación Instituto de Microondas en Suecia, y que colaboró en el desarrollo de teorías sobre RFID.

Middleware: es el software que sirve como medio de interactuación o comunicación entre otras aplicaciones.

Mm: unidad de longitud que representa la milésima parte del metro, llamada milímetro.

MOhm: símbolo en el Estándar Internacional para el megohmio.

Monitorización: supervisión necesaria para ejecutar un plan de acción establecido, asegurando los objetivos marcados, evitando errores, o detectando posibles correcciones.

MRC (Media Research Center): organización de análisis de contenidos de forma científica con sede en Estados Unidos.

Mw: megavatio unidad de potencia en el Sistema Internacional equivale a 10^6 vatios.

N

NCR: compañía del sector de la tecnología especializada en soluciones para empresas, conocida anteriormente como National Cash Register.

NCRP (National Council on Radiation Protection and Measurements): Consejo Nacional de Mediciones y Protección Radiológica en Estados Unidos creado en 1964.

NFC (Near Field Communication): grupo de estándares para teléfonos móviles y dispositivos similares para el establecimiento de una comunicación por radio con otro dispositivo por medio de contacto de los dispositivos o en distancias muy reducidas (pocos centímetros).

O

Ohm: es la unidad de resistencia eléctrica en el Sistema Internacional.

Oil: aceite (nombre) y pintar (verbo).

Olay: marca de productos cosméticos nacida en los en la década de 1950.

Object Class: clase de objeto referido a los códigos EPC.

ONTSI (Observatorio Nacional de las Telecomunicaciones y de la SI): órgano adscrito a la entidad pública empresarial Red.es, cuyo principal objetivo es el seguimiento y análisis del sector de las Telecomunicaciones y de la Sociedad de la Información.

OCR: Reconocimiento Óptico de Caracteres.

OCDE (Organization for Economic Cooperation and Developtment): Organización para la Cooperación Económica y Desarrollo, tiene como objetivo promover políticas que mejoren el bienestar económico y social de las personas de todo el mundo.

P

PA: Autenticación Pasiva.

Pepsico: multinacional americana que se dedica a la fabricación, comercialización y distribución de alimentos.

PETs (Promoting Data Protection by Privacy Enhancing Technologies): Fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad, tiene como función definir los objetivos para lograr una mejor protección de la intimidad, gracias al uso de las tecnologías de la información y la comunicación, y establecer medidas claras para conseguir los objetivos.

Pfizer: empresa farmacéutica estadounidense fundada en 1849.

Philips: empresa dedicada a la electrónica y fundada en los Países Bajos.

PIA (Privacy Impact Assesment): Evaluación sobre Impacto en la Privacidad.

Plug-and-play: traducido como "enchufar y usar" se refiere a la posibilidad de conectar un dispositivo informático a un ordenador o computador sin necesidad de configuraciones previas gracias a ciertos tipos de software evitando el uso de controladores.

Procter & Gamble: compañía propietaria de más de 50 marcas entre las que se encuentran productos para la higiene personal.

Pseudónimos: nombre que oculta el real con fines estéticos, o en este caso por razones de seguridad.

PYME(Pequeña Y Mediana Empresa): es el acrónimo para y su definición es la de una empresa que cumple unas determinadas características en cuanto a número de empleados e ingresos.

R

Radio Transmission systems with modulatable passive responder: Sistemas de Transmisión por Radio con un contestador/respondedor modulable.

Radiofrecuencia (RF): se refiere al rango menos energético del espectro electromagnético que se sitúa entre los valores 3 kHz y 300 GHz aproximadamente.

Rayos Catódicos: corrientes de electrones que se pueden apreciar en tubos al vacío de cristal con electrodos aplicando un voltaje.

Rayos X: se denomina así a la radiación electromagnética, invisible, capaz de atravesar cuerpos opacos y de imprimir películas fotográficas.

REPLAY: Repetición.

S

SAR (Specific Absorption Rate): Tasa de Absorción Específica, medida de la potencia máxima con que un campo electromagnético de radiofrecuencia es absorbido por el tejido vivo.

SEC: es un tipo de documentos clasificados así por la Comisión Europea.

Security and privacy by design: es un término que significa que la privacidad y la protección de datos deben estar integrados a lo largo de todo el ciclo de vida de las tecnologías, desde la fase inicial de diseño, hasta su uso y eliminación.

Segunda Guerra Mundial: conflicto militar a nivel global entre los años 1939 y 1945, en el que se vieron implicadas la mayor parte de naciones del mundo.

Serial Number: referido al código EPC, clase de objeto que va a tener la etiqueta.

ShmooCon Congreso Seguridad: es una convención de hackers realizada en América sobre seguridad informática.

Software: soporte lógico de un sistema informático que tiene la función de hacer posible la realización de tareas específicas.

Steps towards a policy framework: traducido, Pasos hacia un marco político.

Systemedia Corporation: grupo asociado a la empresa mencionada NCR.

Systemedia Division: una parte de la corporación NCR dedicada a la fabricación de impresoras a nivel internacional.

T

Texas Instruments (TI): empresa norteamericana del sector electrónico dedicada al desarrollo y comercio de semiconductores y tecnología para ordenadores.

Transponder/transpondedor: dispositivo electrónico que es al a vez transmisor y respondedor.

Tag: se refiere al dispositivo RFID también llamado etiqueta.

TCP/IP: es un protocolo de red en los que está basado Internet, que tiene como finalidad la transmisión de datos entre dispositivos. Formada por el Protocolo de Control de Transmisión(TCP) y Protocolo de Internet(IP).

TIC (Tecnologías Información y Comunicación): concepto entendido como el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información.

Tarjetas Gen: estándar internacional en el que trabajan EPCglobal para el uso de RFID en la cadena de suministro.

Teradata: referido a la corporación, es una empresa estadounidense especializada en data warehousing y herramientas de análisis empresarial.

U

UCC (Uniform Code Council): Consejo de Código Uniforme, es el nombre de la familia de estándares de la cadena de suministro, formalmente el sistema EAN.UCC.

Ultra High Frequency (UHF): es un intervalo en el espectro electromagnético que se encuentra entre los 300 MHz a los 3GHz, se traduce como Ultra Alta Frecuencia.

Uniform Code Council: Organización de Numeración de los Estados Unidos para administrar y gestionar los estándares sobre la cadena de suministro incluyendo algunos como el uso de códigos de barras en la mayoría de productos actualmente se llama GS1 US.

V

Valores hash: se refiere a los valores de la función hash, también llamada función resumen. La función tiene como entrada un conjunto de elementos generalmente cadenas, y los convierte en un rango de salida finito, normalmente cadenas de una longitud fija.

Vecinity Cards: son tarjetas que pueden ser leídas a corta distancia, llamadas tarjetas de vecindad.

W

Wal-Mart: corporación multinacional de minoristas de origen estadounidense que opera cadenas de grandes almacenes de descuento y clubes de almacenes. Tercera mayor corporación pública del mundo fundada en 1962 por Sam Walton. (Wikipedia)

Watchdog: perro guardián, en contexto tecnológico, es un dispositivo o mecanismo de seguridad que realiza la acción de reseteado en caso de bloqueo, en

el caso RFID, se trata de unas etiquetas que controlan si hay acceso indebido por parte de lectores no autorizados.

Watt (W): vatio.

Wireless: término referido a la comunicación inalámbrica entre un emisor y un receptor que no se sirve de un medio de propagación físico sino de ondas electromagnéticas como medio de transmisión a través del espacio.