INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Guía sobre seguridad y privacidad de la tecnología RFID

INSTITUTO NACIONAL DE **TECNOLOGÍAS** DE LA **COMUNICACIÓN**
AGENCIA ESPAÑOLA DE **PROTECCIÓN** DE **DATOS**

Edición: Mayo 2010

El **Instituto Nacional de Tecnologías de la Comunicación** (INTECO), sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional. Para ello, INTECO desarrollará actuaciones, al menos, en líneas estratégicas de Seguridad Tecnológica, Accesibilidad, Calidad TIC y Formación.

El Observatorio de la Seguridad de la Información (http://observatorio.inteco.es) se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica, siendo un referente nacional e internacional al servicio de los ciudadanos, empresas y administraciones españolas para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza de la Sociedad de la Información.

Más información: www.inteco.es

La **Agencia Española de Protección de Datos** es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, y que tiene por objeto la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y sus normas de desarrollo.

Sus funciones son, en general, velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación – en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos – atender las peticiones y reclamaciones que puedan ser formuladas por las personas afectadas por esta cuestión y la potestad sancionadora de las infracciones que puedan ser cometidas en la materia, así como la recogida de datos estadísticos e informar los proyectos de normas que incidan en materias de protección de datos, así como dictar instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD y seguridad y control de acceso a los ficheros.

Más información: http://www.agpd.es

Depósito Legal: LE-938-2010
Imprime: gráficas CELARAYN, s.a.

Índice

1. La tecnología RFID

1.1. ¿QUÉ ES LA TECNOLOGÍA RFID?

La **identificación por radio frecuencia** o **RFID** (*Radio Frequency IDentification*) es una tecnología que permite identificar automáticamente un objeto gracias a una onda emisora incorporada en el mismo que transmite por radiofrecuencia los datos identificativos del objeto, siendo esta identificación normalmente unívoca.

Probablemente su origen se remonta a los años 20 aunque parece que ya se empieza a utilizar durante la Segunda Guerra Mundial, donde comenzó su uso para que los aviones se identificasen como "amigos" ante sus propios efectivos. Con el tiempo, esta idea se traslada a sistemas más reducidos sirviendo para el seguimiento de personal y equipamiento militar hasta que dos empresas norteamericanas comienzan su comercialización civil a finales de los años 70.

En el momento actual, bajo las siglas RFID se agrupan tecnologías que sirven para identificar objetos mediante ondas de radio.

La tecnología RFID hace posible la auto-identificación de un objeto que contiene una emisora de radio. En el estado actual de desarrollo, el abaratamiento de los costes y la reducción en su tamaño permite que estas emisoras sean lo suficientemente pequeñas como para tener la forma de etiquetas adhesivas, pudiéndose incorporar casi a cualquier objeto.

Gracias a estas microemisoras o transpondedores (en adelante, *tags* o etiquetas) el producto puede ser localizado a una distancia variable, desde pocos centímetros, hasta varios kilómetros. La distancia de recepción, fiabilidad y velocidad de la transmisión y la capacidad de información emitida, depende de varias características de los *tags* como pueden ser la frecuencia de la emisión, la antena o el tipo de chip que se use para cada aplicación específica. Estas características se verán a lo largo de esta guía.

1.2. ¿CÓMO FUNCIONA?

El funcionamiento de esta tecnología se basa en la señal de radio que genera la etiqueta RFID, en la que previamente se han grabado los datos identificativos del objeto al que está adherida. Un lector físico se encarga de recibir esta señal, transformarla en datos y transmitir dicha información a la aplicación informática específica que gestiona RFID (denominada *middleware*).

Componentes de un sistema RFID

Los componentes que participan en la tecnología RFID son cuatro: las etiquetas, los lectores, el software que procesa la información y los programadores:

- **Etiqueta RFID:** permite almacenar y enviar información a un lector a través de ondas de radio. Coloquialmente suelen denominarse *tags* – que es el término en inglés – aunque también son conocidas como *transpondedores* (esta denominación proviene de la fusión de las palabras *transmitter* (transmisor) y *responder* (contestador).

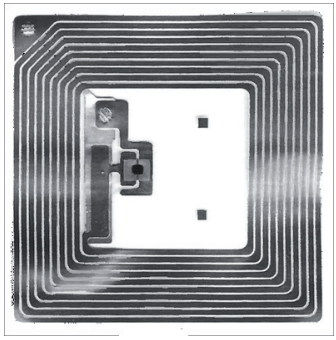


Ilustración 1: Etiqueta RFID

La etiqueta RFID está compuesta por una antena, un transductor radio y un microchip (no presente en las versiones de menor tamaño). La antena es la encargada de transmitir la información que identifica a la etiqueta. El transductor es el que convierte la información que transmite la antena y el chip posee una memoria interna para almacenar el número de identificación y en algunos casos datos adicionales. La capacidad de esta memoria depende del modelo. En el caso de *tags* sin chip, la información que se puede almacenar es bastante limitada (hasta 24 bits).

Las etiquetas actualmente tienen precios muy bajos (apenas unos céntimos de euro) y dimensiones de hasta 0,4 mm^2, por lo que están preparadas para su integración en todo tipo de objetos.

- **Lector de RFID:** se encarga de recibir la información emitida por las etiquetas y transferirla al *middleware* o subsistema de procesamiento de datos. Las partes del lector son: antena, transceptor y decodificador. Algunos lectores incorporan un módulo programador que les permite escribir información en las etiquetas, si éstas permiten la escritura.

- **Subsistema de procesamiento de datos o *middleware*:** es un software que reside en un servidor y que sirve de intermediario entre el lector y las aplicaciones empresariales. Se encarga de filtrar los datos que recibe del lector o red de lectores, de forma que a las aplicaciones software sólo les llega información útil. Algunos programas se encargan de la gestión de la red de lectores.

- **Programadores RFID:** Los programadores RFID son los dispositivos que realizan la escritura de información sobre la etiqueta RFID, es decir, codifican la información en un microchip situado dentro de una etiqueta RFID. La programación de las etiquetas se realiza una única vez si las etiquetas son de sólo lectura, o varias veces si son de lectura/escritura.

La potencia que necesita el programador para escribir la información en las etiquetas es mayor que la que necesita el lector, es decir, el radio de acción de un equipo grabador es menor que el radio de acción del lector. Por esta razón en la mayoría de las ocasiones, el programador necesita contacto directo con las etiquetas.

En la Ilustración 2 se puede observar de manera sencilla de qué manera se estructura el esquema general de funcionamiento de un sistema RFID: las etiquetas o *tags* envían información al lector mediante una antena y éste la transmite al subsistema de procesamiento de datos o middleware para que se encargue de filtrar los datos. De este modo, a las aplicaciones software sólo les llega información válida.

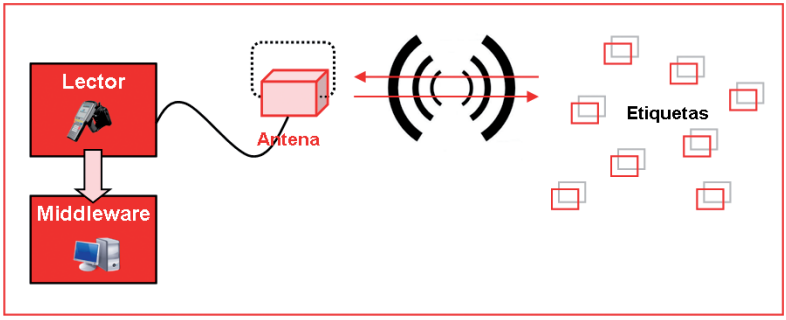


Ilustración 2: Esquema general de funcionamiento de la tecnología RFID

Tipos de etiquetas

Hay una enorme variedad de etiquetas RFID, existen diferentes tipos dependiendo de la fuente de energía que utilicen, la forma física que posean, el mecanismo que utilicen para almacenar datos, la cantidad de datos que pueden almacenar, la frecuencia de funcionamiento o de la comunicación que utilizan para transmitir la información al lector. Gracias a esto, es posible elegir la etiqueta más adecuada para cada aplicación específica.

A grandes rasgos se pueden clasificar las etiquetas RFID siguiendo dos criterios:

- **Según la fuente de energía que utilicen**

  - **Etiquetas RFID pasivas:** No necesitan una fuente de alimentación interna, son circuitos resonantes, ya que toda la energía que requieren se la suministra el campo electromagnético creado por el lector, que se encarga de activar el circuito integrado y alimentar el chip para que éste transmita una respuesta. En este tipo de etiquetas, la antena debe estar diseñada para que pueda obtener la energía necesaria para funcionar.

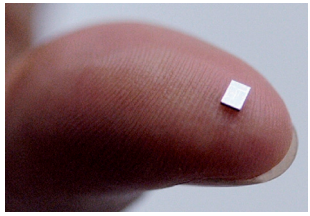


Ilustración 3: Etiqueta pasiva 1

El alcance de estas etiquetas varía dependiendo de muchos factores, como la frecuencia de funcionamiento, o la antena que posean. Alcanzan distancias entre unos pocos milímetros y 6-7 metros.

Al no tener una batería interna, son las etiquetas de menor tamaño (ver Ilustración 3), y a menudo se insertan en pegatinas.

Las etiquetas RFID pasivas son las etiquetas más económicas del mercado.

Ilustración 4: Etiqueta pasiva 2

b **Etiquetas RFID activas:** Poseen una batería interna, con la que alimentan sus circuitos y transmiten la respuesta al lector. Su cobertura de difusión es mayor gracias a que poseen una batería propia, y su capacidad de almacenamiento también es superior.

Al transmitir señales más potentes, su alcance es mejor y puede llegar a ser válido para su uso en entornos hostiles como puede ser sumergido en agua o en zonas con mucha presencia de metales. Estas etiquetas son mucho más fiables y seguras.

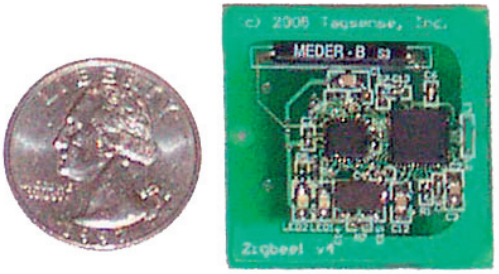


Ilustración 5: Etiqueta activa

Estas etiquetas también son las más caras del mercado y las de mayor tamaño. El posible rango de cobertura efectivo de éstas puede llegar a ser varios cientos de metros (dependiendo de sus características), y la vida útil de sus baterías puede ser de hasta 10 años.

c **Etiquetas RFID semi-pasivas:** Este tipo de etiquetas posee una mezcla de características de los dos tipos anteriores. Por una lado, activa el chip utilizando una batería (como las etiquetas RFID activas) pero por otro, la energía que necesita para comunicarse con el lector, se la envía el propio lector en sus ondas de radio que al ser captadas por la antena de la etiqueta, aportan suficiente energía para la emisión de la información (como las etiquetas RFID pasivas).

Son más grandes y más caras que las etiquetas pasivas (ya que disponen de una batería) y más baratas y pequeñas que las activas. Sus capacidades de comunicación son mejores que las pasivas aunque no alcanzan a las activas en estas características.

- **Según la frecuencia a la que trabajen**

Dependiendo de la frecuencia de operación, las etiquetas se pueden clasificar en baja, alta, ultra alta frecuencia y microondas. La frecuencia de operación determina aspectos de la etiqueta como la capacidad de transmisión de datos, la velocidad y tiempo de lectura de éstos, el radio de cobertura y el coste de la etiqueta.

Tabla 1: Bandas de frecuencia utilizadas en la tecnología RFID

Frecuencia	Denominación	Rango
125 kHz – 134 kHz	LF (Baja Frecuencia)	Hasta 45 cm.
13,553 MHz – 13,567 MHz	HF (Alta Frecuencia)	De 1 a 3 m.
400 MHz – 1000 MHz	UHF (Ultra Alta Frecuencia)	De 3 a 10 m.
2,45 GHz – 5,4 GHz	Microondas	Más de 10 m.

Fuente: red.es

Las etiquetas pasivas habitualmente utilizan la banda de baja frecuencia. Tanto las etiquetas de baja como de alta frecuencia funcionan mediante acoplamiento inductivo, es decir, utilizan el campo magnético generado por la antena del lector como principio de propagación. La banda UHF como la de microondas se utilizan tanto en las etiquetas activas como pasivas.

1.3. BENEFICIOS DE LA TECNOLOGÍA RFID

La tecnología RFID se ha dirigido principalmente al sector logístico (almacenamiento, distribución, etc.) y al sector de la defensa y seguridad, no obstan-

te los beneficios que proporciona se extienden a otros campos relacionados con la identificación de procesos:

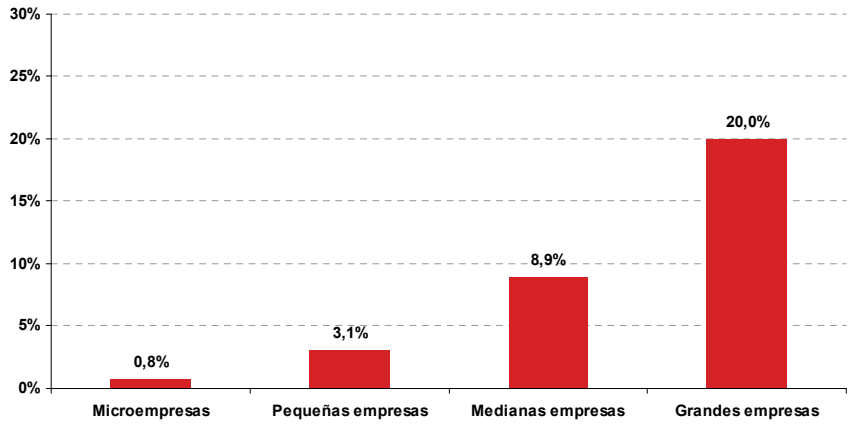
- Permite un gran volumen de almacenamiento de datos mediante un mecanismo de reducidas proporciones.
- Automatiza los procesos para mantener la trazabilidad y permite incluir una mayor cantidad de información a la etiqueta, reduciendo así los errores humanos.
- Facilita la ocultación y colocación de las etiquetas en los productos (en el caso de las etiquetas pasivas) para evitar su visibilidad en caso de intento de robo.
- Permite almacenar datos sin tener contacto directo con las etiquetas.
- Asegura el funcionamiento en el caso de sufrir condiciones adversas (suciedad, humedad, temperaturas elevadas, etc.).
- Reduce los costes operativos ya que las operaciones de escaneo no son necesarias para identificar los productos que dispongan de esta tecnología.
- Identifica unívocamente los productos.
- Posibilita la actualización sencilla de la información almacenada en la etiqueta en el caso de que ésta sea de lectura/escritura.
- Mayor facilidad de retirada de un determinado producto del mercado en caso de que se manifieste un peligro para la seguridad.
- Posibilita la reescritura para así añadir y eliminar información las veces deseadas en el caso de que la etiqueta sea de lectura/escritura (a diferencia del código de barras que sólo se puede escribir una vez).

2. Usos y aplicaciones de RFID

Entre las empresas españolas el **uso de la tecnología RFID** es aún incipiente. Así, el nivel de adopción de esta tecnología por parte de las microempresas es del 0,8%, entre las pymes el porcentaje se eleva a 3,1%, en el caso de las entidades de 10 a 49 empleados, y a 8,9% si el rango va de 50 a 249 trabajadores. Si se habla de grandes compañías (más de 249) el porcentaje es del 20%[1].

Por tanto, puede verse claramente cómo un mayor tamaño de empresa está relacionado con un mayor uso de la tecnología RFID.

Gráfico 1: Uso de la tecnología RFID por tamaño de empresa (%)



Fuente: ONTSI a partir de los datos del INE 2009

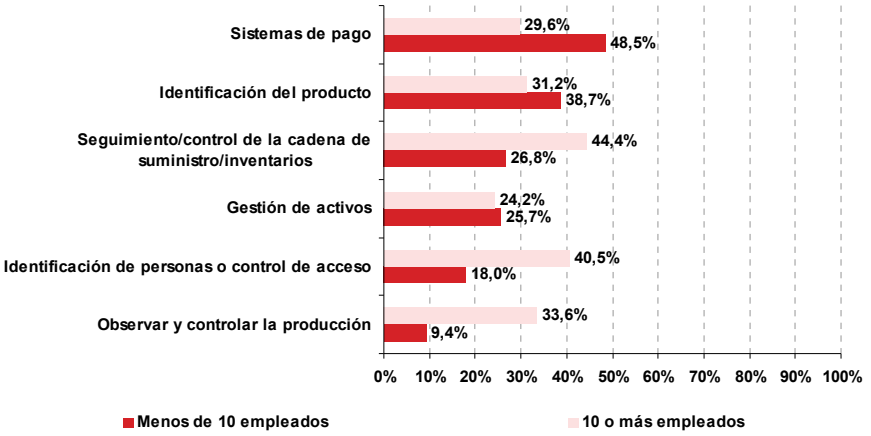
Los objetivos de uso de la tecnología RFID varían también en función del tamaño de la empresa. En el Gráfico 2 se observan las grandes diferencias existentes por número de empleados.

1 *"Tecnologías de la Información y las Comunicaciones en las PYMES y grandes empresas españolas" (2010) y "Tecnologías de la Información y las Comunicaciones en la microempresa española" (2010), ambos del Ministerio de Industria Turismo y Comercio*

Por **sectores**, independientemente del tamaño de la entidad, las empresas con actividades de transporte y almacenamiento son las que más utilizan la tecnología RFID (12,2%). Le siguen el sector financiero (8,2%), la informática, telecomunicaciones y audiovisuales (7,5%) y el comercio mayorista (6,2%) y minorista (5%).

En el caso de las microempresas (menos de 10 empleados), las **aplicaciones mayoritarias de la tecnología RFID** se relacionan con los sistemas de pago – ej: peaje de carreteras o transporte de pasajeros – con un 48,5%, seguido de la identificación de productos (38,7%). En cambio, los principales usos que llevan a cabo las pymes y grandes empresas españolas se centran en el seguimiento y control de la cadena de suministro y de inventarios, en un 44,4%, y la identificación de personas y control de accesos, en un 40,5% de los casos.

Gráfico 2: Objetivos de uso de la tecnología RFID por tamaño de empresa (%)



Fuente: ONTSI a partir de los datos del INE 2009

Los ejemplos de aplicaciones actuales de la tecnología RFID son muchos y las previsiones apuntan a que crezcan de manera exponencial en los próximos años. Todos los entornos donde la identificación automática, fiable, rápida y barata pueda aportar beneficios son campo de aplicación de la tecnología RFID. El día a día está rodeado de diversos y muy variados modos de aplicación de esta tecnología:

- En **tiendas de artículos** para identificar los productos (almacenamiento, precios, etc.) o como medida de seguridad para detectar un intento de hurto. Gestiona y controla el stock entre diferentes tiendas así como mejora la rotación de artículos repercutiendo en mejoras en las ventas de productos.

Ilustración 6: Etiqueta RFID para ropa

- También se usa la tecnología RFID para el control de acceso y cobro en **transportes públicos**. Se incorpora el *tag* a las tarjetas con los abonos de los usuarios o para el control de equipajes.

Ilustración 7: Dispositivo RFID en transporte público

- La identificación electrónica de **mascotas** mediante la implantación subcutánea por un veterinario de un microchip portador de un código numérico único. El código identificativo que se introduce se corresponde con el de un registro en el que van a figurar los datos relativos al animal, al propietario, así como los tratamientos sanitarios.

Ilustración 8: Microchip identificador para perros

- El **pago automático de peajes.** Por ejemplo, en sistemas de telepeaje utilizados en las autopistas para realizar el pago del trayecto sin necesidad de detener el vehículo. Gracias a un dispositivo que se coloca en el coche y otro dispositivo de lectura electrónica situado en las estaciones de peaje, automáticamente se gestiona la apertura de la barrera de seguridad, así como el pago.

  Se usa tecnología de RFID pasiva UHF (ultra alta frecuencia) para realizar un cobro exacto, de modo que no sean necesarios cambios ni devoluciones de efectivo y así no se requiera intervención humana. De esta manera se reduce el congestionamiento vial.

- En las **bibliotecas**, para catalogación, ordenación y protección antirrobo de libros. Se trata de un sistema de almacenamiento y recuperación remota de información a través de etiquetas y lectores, que tienen como fin fundamental transmitir la identidad de un libro mediante sistemas RFID pasivos UHF de largo alcance.

- En los **supermercados**, para realizar la facturación automática de todo un carro de productos sin moverlos del mismo.

  También se usa para el control de su inmovilizado, compuesto por una cantidad de elementos repartidos por sus centros de venta, almacenes y oficinas. Estos elementos deben estar controlados y perfectamente emplazados en todo momento en el caso de que las autoridades competentes realicen inspecciones.

Ilustración 9: Carrito de supermercado con lector RFID

- Toma de tiempos en **eventos deportivos**, por ejemplo, carreras populares o maratones, mediante la entrega de “pulseras chip” a miles de corredores para su seguimiento.

  Estas pulseras llevan integrado un chip y una antena, permitiendo su comunicación con un lector a una distancia de algunos centímetros. Con estas pulseras se consigue la identificación de la persona de manera segura, sin riesgo de error.

Ilustración 10: Dispositivo RFID para transmitir los datos del corredor

- En el **ámbito sanitario**, para el control de medicamentos, seguimiento de instrumental, identificación de muestras médicas o el seguimiento de pacientes en centros de salud. Manteniendo el inventario de fármacos y bolsas de sangre del hospital controlado en tiempo real se evitan errores en las transfusiones o en la administración de fármacos al paciente que pueden ocasionar graves perjuicios.

Ilustración 11: RFID y eSalud

- Como **control de acceso** en zonas residenciales, habitaciones de hoteles, aparcamientos, plantas industriales o entornos que requieran seguridad. El reconocimiento de la identidad de una persona que quiere acceder a un determinado lugar se realiza sin contacto físico, mediante ondas de radio entre un emisor y un receptor a través de un *tag* que se puede presentar en diversos formatos: pulsera, tarjeta, etc.

- En la **logística, almacenamiento y distribución**, en general. Un ejemplo es su implantación en el sistema de inventariado y seguimiento de productos por compañías textiles, o su utilización en la identificación, localización y gestión de grandes piezas de hormigón o en sistemas de gestión postal con el fin de mejorar los plazos de entrega de los envíos y la gestión de la logística.

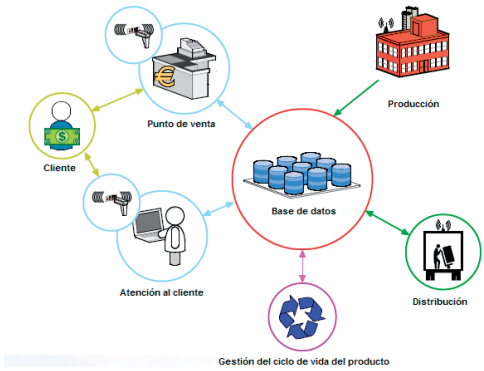


Ilustración 12: Cadena de valor basada en la tecnología RFID

- En el **sector alimentario**, con el fin de que los agricultores puedan asegurar la trazabilidad de sus productos desde su siembra hasta el consumidor final; o en el control e identificación de las reses en las explotaciones ganaderas. Esto permite funcionalidades como el registro automático de la producción o conocer en tiempo real las reservas o la producción de una determinada.

  Esto es posible gracias a *tags* incluidas en los carros que transportan las mercancías de cada una de ellas. Los camiones que transportan los productos disponen de ordenadores con tecnología RFID que mediante Wi-Fi trasladan la información.

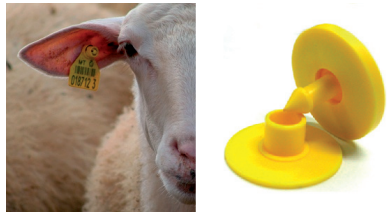


Ilustración 13: Etiqueta en animales

- En el **ámbito militar**, el Departamento de Defensa de EEUU exige a sus proveedores el uso de la tecnología RFID en la cadena de suministro. En este sentido, la Fuerza Aérea de Estados Unidos, USAF, dispone de dispositivos RFID para la seguridad y rastreo de activos a bordo de todos los tipos y clasificaciones de aviones que transportan suministros para el Departamento de Defensa.

Además de estas aplicaciones ya implantadas y sólidamente probadas, **hay otras muchas aplicaciones que se están estudiando**, como por ejemplo:

- Pagos electrónicos con **teléfonos móviles**, a través de la llamada tecnología NFC (*Near Field Communication*) que permite que un teléfono móvil recupere los datos de una etiqueta RFID. Esta tecnología combinada con medios de pago electrónicos para móviles (como *Mobipay*, *Paybox*, *etc*.) permite comprar productos y pagarlos con tan sólo acercar el teléfono al punto de información del producto de donde RFID extrae la información que necesita.

- En muchos países ya se utilizan los **pasaportes electrónicos**, que almacenan la información del titular y la fotografía o la huella dactilar en un chip RFID.

Ilustración 14: Pasaporte electrónico

- **Activación de vehículos y maquinaria industrial**. En este caso, la etiqueta RFID actúa como control de verificación personal, permitiendo la activación sólo en presencia de dicha etiqueta.

3. Regulación y estandarización

La estandarización de esta tecnología posibilita que exista interoperabilidad entre aplicaciones y ayuda a que los diferentes productos no interfieran, independientemente del fabricante.

Antes de que se desarrollaran estándares que regularan la comunicación entre etiquetas y lectores, cada compañía poseía un sistema diferente, por lo que las etiquetas de un fabricante sólo podían ser leídas por los lectores de ese mismo fabricante.

De todas las frecuencias con las que se empezó a trabajar en el mundo de RFID, la única banda con aceptación mundial fue la de 13,56MHz, que llegó a convertirse en un estándar ISO.

La estandarización en el mundo de RFID comenzó por la competencia de dos grupos competidores: ISO y *Auto-ID Center* (más conocida como *EPC Global*).

3.1. ELECTRONIC PRODUCT CODE

La organización EPC Global es la organización mundial que asigna dichos códigos RFID a las entidades y empresas, asegurándose que el número asignado sea único. Además de regular el sistema, se encarga de asesorar y homologar las aplicaciones disponibles en la industria así como las empresas reconocidas como integradoras

La EPC Global ha desarrollado el **EPC o Código Electrónico de Producto** (en inglés *Electronic Product Code*), que resuelve el problema de estandarización en lo que a codificación se refiere. El código EPC es un número único (con una longitud de 24 dígitos hexadecimales) diseñado para identificar de manera exclusiva cualquier objeto a nivel mundial. Ello permite la mejora y la eficiencia en los procesos del manejo físico de las mercancías tales como recepción, contabilización, clasificación y embarque. Los proveedores obtienen información en tiempo real sobre el consumo y status de sus mer-

cancías dentro de la cadena de suministros, pudiendo estimar los plazos de entrega y solventar en gran medida el robo de mercancías.

Un elemento fundamental de esta organización es el EPC Gen2 (*EPCGlobal UHF Generation 2*), estándar definido por más de 60 de las principales compañías de tecnología. Incluye 2 normas básicas: una que delimita los requisitos físicos y lógicos para la transmisión de información entre las etiquetas y los lectores, y la otra que identifica los esquemas de codificación específicos de EAN.UCC[2].

3.2. ESTÁNDARES ISO RFID

Los estándares para RFID son un tema con una complicación añadida, ya que muchas de las aplicaciones están relacionadas con pago electrónico o documentación personal. Los **estándares RFID** tratan los siguientes temas:

- Protocolo de interfaz aire: la forma en la que las etiquetas y los lectores se pueden comunicar.
- Contenido de los datos: organización de los datos que se intercambian.
- Conformidad: pruebas que los productos deben cumplir para reunir los requisitos del estándar.
- Aplicaciones: cómo se pueden utilizar las aplicaciones con RFID.

La *International Organization for Standardization* (ISO) es una organización internacional no gubernamental integrada por una red de institutos

2 *El sistema EAN.UCC es un conjunto de estándares que permite la administración eficiente de las cadenas de distribución multi-sectorial y mundial mediante la identificación inequívoca de productos mediante el etiquetado de los productos a través de códigos de barras estándar. Permitiendo la automatización de los procesos, hace posible el conocimiento de la trayectoria y la ubicación de los productos mediante una lectura automática de códigos de barras.*

nacionales en 160 países, cuya aportación es igualitaria (un miembro por país). Su función principal es buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

Las **normas ISO** relativas a la RFID son:

- ISO/IEC 11784-11785, ISO 10536, ISO 18000: sobre privacidad y seguridad a los datos.
- ISO 14223/1: identificación por radiofrecuencia de animales, transpondedores avanzados e interfaz radio.
- ISO 14443: orientadas a los sistemas de pago electrónico y documentación personal. Es muy popular el estándar HF, que es el que se está utilizando como base para el desarrollo de pasaportes que incorporan RFID.
- ISO 15693: estándar HF, también muy extendido, se utiliza en tarjetas sin contacto de crédito y débito.
- ISO 18000-7: estándar industrial para UHF (para todos los productos basados en RFID activa) es promovido por el Departamento de Defensa de EEUU, la OTAN y otros usuarios comerciales de RFID activa.
- ISO 18185: estándar industrial para el seguimiento de contenedores, a frecuencias de 433 MHz y 2,4 GHz.
- ISO/IEC 15961: se encarga del protocolo de datos e interfaz de aplicación.
- ISO/IEC 15962: sobre el protocolo de codificación de datos y funcionalidades de la memoria de la etiqueta RFID.

- ISO/IEC 15963: sobre el sistema de trazado y monitorización que afecta a la etiqueta RFID.

- ISO 19762-3: establece los términos y definiciones únicas de identificación por radiofrecuencia (RFID) en el campo de la identificación automática y captura de datos técnicos.

- ISO 23389: estándar para los contenedores (normas de lectura/escritura).

- ISO 24710: técnicas AIDC para gestión de objetos con interfaz ISO 18000.

Si bien las especificaciones y la terminología se actualizan continuamente, los estándares de RFID creados por la ISO establecen todos los requisitos reguladores a nivel mundial. Por otro lado, los gobiernos de cada país regulan las frecuencias permitidas, las emisiones y otras características de funcionamiento.

La falta de estandarización es uno de los factores más importantes a tener en cuenta a la hora de la implantación definitiva de RFID. Gracias a ISO y a la EPC Global la estandarización es un hecho. Sin embargo, el verdadero problema es que los estándares actuales no son interoperables al cien por cien ni entre sí, ni con otras tecnologías.

4. Otros sistemas de identificación automática

La tecnología RFID se encuadra dentro del grupo de los **sistemas de identificación automática**, se utilizan en aplicaciones que requieran identificar y realizar el seguimiento de productos, artículos, objetos o seres vivos y además se desea automatizar dicho seguimiento mediante el uso de tecnología de la información.

La mayoría de las tecnologías para la identificación automática están ampliamente aceptadas por los usuarios y son muy conocidas. Dado que la tecnología RFID está llamada a sustituirlas en algunos casos se describirán brevemente.

4.1. CÓDIGOS DE BARRAS

Es el sistema de identificación más utilizado. Se trata de un código comprendido por una serie de barras y espacios configurados paralelamente. El diseño de estos campos representa unos datos relacionados con un elemento. La secuencia puede ser interpretada de forma numérica o alfanumérica, es leída por un escáner óptico láser y procesada por una computadora.

El código de barras es la tecnología preferida de los comercios para identificar los productos pese a las limitaciones que presenta:

- Requiere visibilidad directa para funcionar.
- Sirve para identificar un tipo de producto, no unidades en particular.
- Se daña o rompe fácilmente, ya que normalmente se adhiere a la superficie del producto; y al dañarse no puede ser leído.

Ilustración 14: Código de barras

En la actualidad hay varios tipos de códigos, con varias filas de barras superpuestas, de igual longitud o distinta, de varios colores o incluso bidimensionales. Cada una de estas variantes mejora alguna de las características del sistema original.

4.2. RECONOCIMIENTO ÓPTICO DE CARACTERES (OCR)

El sistema OCR (*Optical Character Recognition*) fue utilizado por primera vez en la década de los 60.

Los sistemas OCR identifican automáticamente símbolos o caracteres, a partir de una imagen para almacenarla en forma de datos. Algunas de sus aplicaciones, entre otras, son: reconocimiento de matrículas a través de radares, registro de cheques por parte de los bancos, etc. Los inconvenientes de este sistema de identificación residen en su alto precio y la complejidad de los lectores en comparación con otros sistemas de identificación.

4.3. SISTEMAS BIOMÉTRICOS

Son sistemas que identifican personas por comparación de características unívocas[3]. Su principal cualidad es que transforman una característica biológica, morfológica o de comportamiento del propio individuo, en un valor numérico y lo almacenan para su posterior comparación.

Se puede hablar de sistemas identificadores por huella dactilar, por voz, por pupila, por forma de la cara, por forma de la oreja, por forma corporal o por patrón de escritura, entre otros. En sistemas de autenticación se suelen utilizar diferentes factores como por ejemplo "lo que tengo (Ej.: una tarjeta), lo que sé (Ej.: un número PIN) y lo que soy (Ej.: mi huella dactilar)". Los sistemas biométricos representarían el tercer factor: "lo que soy".

3 *La tecnología tiene inherentes ciertas tasas de error.*

4.4. TARJETAS INTELIGENTES

Una tarjeta inteligente o *smart card*, es un sistema de almacenamiento electrónico de datos con capacidad para procesarlos (*microprocessor card*). Por seguridad está instalado dentro de una estructura de plástico similar, en forma y tamaño, a una tarjeta de crédito.

Una de las principales ventajas de las tarjetas inteligentes es que aportan protección frente a posibles accesos indeseados ya que poseen características de seguridad avanzadas y además son más económicas.

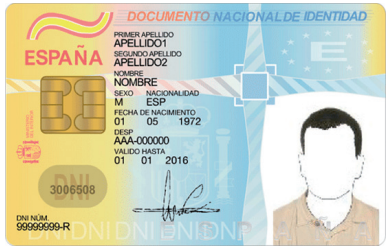


Ilustración 16: Chip insertado en DNI electrónico

4.5. COMPARATIVA CON RFID

RFID está llamado a sustituir o competir con estas cuatro tecnologías y con otras en determinadas aplicaciones y en determinados entornos. Comparándola con cada una de las tecnologías anteriores, podemos decir que:

- En la mayoría de los estudios y encuestas realizadas, se muestra una clara predisposición por el uso de RFID sobre el código de barras. Se prevé que ambas tecnologías coexistan pero en general, la tecnología RFID se impondrá a los códigos de barras, ya que ahorra tiempo y personal, es más eficiente y minimiza las pérdidas y los errores.

- Sobre la lectura con OCR, sólo se mantendrá en situaciones en las que sea imprescindible, ya que la tecnología RFID es claramente superior.

- Los sistemas biométricos aportan una gran versatilidad en la identificación pero precisan del manejo de información privada del individuo. En cambio, la tecnología RFID permite utilizar menos cantidad de información. Por tanto, en entornos donde no sea necesario un nivel de seguridad extremo, esta tecnología es una buena alternativa que se está utilizando.

- Por último, si se compara con las tarjetas inteligentes, éstas no contienen baterías, siendo el lector, por contacto eléctrico, el que suministra la energía necesaria para su funcionamiento; al contrario de la tecnología RFID, que no requiere contacto con el dispositivo de lectura.

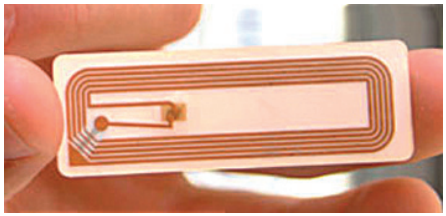


Ilustración 17: Otro modelo de etiqueta

5. Riesgos del uso de RFID

La tecnología RFID plantea nuevas oportunidades de mejorar la eficiencia y comodidad de los sistemas de uso diario. Estas mejoras, que afectan a muchas facetas de la vida, desde la personal a la profesional, en ocasiones plantean nuevos riesgos para la seguridad y nuevos retos para evitarlos. Para identificar los nuevos riesgos que se plantean, hay que tener en cuenta los dos tipos de usuarios de esta tecnología:

- Entidades que utilizan RFID para optimizar sus procesos internos de gestión, de almacén, de inventario, de producción, de gestión de personal, de seguridad, etc.

- Entidades que ofrecen un servicio a usuarios internos de la organización, como control de accesos, o a usuarios particulares, como venta de productos, prestación de servicios sanitarios, etc.

En ambos casos, existen riesgos derivados de las características de la tecnología que son comunes aunque las aplicaciones sean tan dispares en sus beneficiarios y objetivos. Estos riesgos comunes tienen que ver con ataques o averías que afectan al servicio, bien interrumpiéndolo, bien alterándolo, bien realizando algún tipo de fraude. Se analizan estos riesgos en el siguiente apartado bajo el título **riesgos para la seguridad**.

Por otro lado, existe también la posibilidad de que la tecnología se use de forma maliciosa para acceder de forma fraudulenta a información personal de los usuarios del sistema. Este segundo tipo de riesgo está principalmente asociado a los sistemas que dan servicio a usuarios y puede tener una repercusión muy importante para las organizaciones responsables. Se tratan estos riesgos en el apartado **riesgos para la privacidad.**

Además de estos dos tipos, existen **otros riesgos** que pueden condicionar el uso de la tecnología RFID. Así, en torno a la tecnología RFID se vuelve a plantear el debate sobre los riesgos de exposición de los seres humanos a

las radiaciones. Este problema ha sido abordado por la OMS. Su Comisión ICNIRP (*International Commission on Non Ionizing Radiation Protection*) ha publicado normas de exposición a las radiaciones que detallan tiempos máximos de exposición y niveles de potencia de los campos electromagnéticos presentes. Los riesgos para la salud que presentan los campos creados por los lectores y etiquetas RFID que hoy se usan comercialmente son mínimos. Como dato ilustrativo, apuntar que la potencia emitida por un teléfono móvil es de 2W y la de una etiqueta RFID oscila entre 10 y 200 μW, esto es, entre 200.000 y 10.000 veces menos potencia que la emitida por un teléfono móvil.

Los riesgos derivados del uso de RFID deben ser afrontados con la mayor atención dada su importancia. En la prevención de estos riesgos, todos los participantes de la tecnología tienen responsabilidad, desde los encargados de desplegar la tecnología y los organismos que deben velar por los ciudadanos hasta los propios usuarios.

En cada uno de sus ámbitos, los agentes implicados deben desarrollar políticas activas. El papel de las autoridades es clave en esta tarea, creando legislación, normativas y recomendaciones. También el de las instituciones de investigación mediante soluciones técnicas que mejoren la seguridad. Las organizaciones proveedoras que utilizan la tecnología deben aplicar estas recomendaciones y desarrollar buenas prácticas. Por último, los usuarios deben conocer y exigir sus derechos para preservar su privacidad.

6. Riesgos para la seguridad

Los riesgos para la seguridad de la tecnología RFID son aquellos derivados de acciones encaminadas a deteriorar, interrumpir o aprovecharse del servicio de forma maliciosa. Con este tipo de actos se perseguirá un beneficio económico o bien un deterioro del servicio prestado.

Los riesgos para el servicio se concretan en los tipos de "ataque" más habituales que puede sufrir la instalación, cada uno de ellos con una finalidad y un impacto diferente. La forma más simple de ataque a un sistema RFID es evitar la comunicación entre el lector y la etiqueta, pero también existen otras formas de ataque más sofisticadas, cuyo blanco son las comunicaciones en radiofrecuencia:

- **Aislamiento de etiquetas:** El ataque más sencillo a la seguridad en RFID consiste en impedir la correcta comunicación lector-etiqueta. Esto se puede conseguir introduciendo la etiqueta en una "*jaula de Faraday*[4]" o creando un campo electromagnético que interfiera con el creado por el lector.

  Este ataque puede ser utilizado para sustraer productos protegidos por etiquetas RFID. También puede ser una medida de protección de usuarios ante lectores de etiquetas ilegales. **Un ejemplo muy relevante de este caso es el del pasaporte electrónico**, para el que existen fundas especiales con hilos de metal que crear una "*jaula de Faraday*" evitando lecturas incontroladas de su información.

- **Suplantación:** Este ataque consiste en el envío de información falsa que parece ser válida. Por ejemplo, se podría enviar un código electrónico de producto (EPC) falso, cuando el sistema espera uno correcto.

  Este tipo de ataque puede servir para sustituir etiquetas lo cual puede permitir la obtención de artículos caros con etiquetas suplantadas de

4 *Una jaula de Faraday es un espacio cerrado revestido metálicamente que imposibilita la influencia de los campos eléctricos exteriores en el interior del mismo. Las ondas de radio no pueden adentrarse en el interior de la jaula.*

productos más baratos. Además, aplicado a la cadena de distribución, puede llegar a acarrear un fraude de grandes dimensiones por la sustitución de grandes volúmenes de mercancías. Este ataque puede utilizarse en otros entornos, como puede ser el del tele-peaje.

Ilustración 18: Control de acceso mediante RFID

3 **Inserción**: Este ataque consiste en la inserción de comandos ejecutables en la memoria de datos de una etiqueta donde habitualmente se esperan datos. Estos comandos pueden inhabilitar lectores y otros elementos del sistema. La finalidad de este tipo de ataque será la desactivación del sistema o la invalidación de parte de sus componentes, permitiendo algún tipo de fraude, o una denegación de servicio.

Repetición: Consiste en enviar al lector RFID una señal que reproduce la de una etiqueta válida. Esta señal se habrá capturado mediante escucha a la original. El receptor aceptará como válidos los datos enviados. Este ataque permitirá suplantar la identidad que representa una etiqueta RFID.

5 **Denegación de servicio (DoS):** Este tipo de ataque, satura el sistema enviándole de forma masiva más datos de los que este es capaz de procesar (por ejemplo colapsando la funcionalidad de backscattering o señal de retorno de la tecnología RFID). Asimismo, existe una variante, el *RF Jamming*, mediante el cual se consigue anular o inhibir la comunicación de radiofrecuencia emitiendo ruido suficientemente potente. En ambos, casos, se invalida el sistema para la detección de *tags*. Con este ataque se consigue que los objetos etiquetados, escapen al control del sistema en su movimiento. Puede ser utilizado para la sustracción de mercancía a pequeña o gran escala.

- **Desactivación o destrucción de etiquetas:** Consiste en deshabilitar las etiquetas RFID sometiéndolas a un fuerte campo electromagnético. Lo que hace este sistema es emitir un pulso electromagnético que destruye la sección más débil de la antena, con lo que el sistema queda inutilizado. Si se dispone de los medios técnicos necesarios, se pueden inutilizar las etiquetas de protección antirrobo de los productos, favoreciéndose así su sustracción. Este ataque también se puede utilizar en los sistemas utilizados para la cadena de distribución.

- **Clonación de la tarjeta RFID**: A partir de la comunicación entre una etiqueta y el lector, se copian dichos datos y se replican en otra etiqueta RFID para ser utilizados posteriormente.

- **Riesgo de ataque mediante inyección de lenguaje de consultas SQL**: Por medio de la comunicación entre la etiqueta y el lector, se pasa lenguaje SQL hacia el soporte físico que lee la etiqueta, el cual, debido a dicho ataque, ejecuta las órdenes incluidas en la etiqueta y esto puede ser introducido en una base de datos.

- **Código malicioso (malware)**: Otro posible riesgo de la tecnología RFID consiste en la infección y transmisión de códigos maliciosos incluidos dentro de etiquetas RFID. Para ello el código malicioso debe entrar en la etiqueta, lo que supone un hecho complicado, dado que la capacidad de almacenamiento de algunas etiquetas no es muy grande.

- ***Spoofing***: Caso particular para etiquetas activas (de lectura y escritura). En este caso se escriben datos reales en una etiqueta RFID para suplantar la información original. Es más habitual en las etiquetas RFID de las prendas de vestir. Se puede suplantar la información tantas veces se quiera, siempre que éstas sean de lectura.

- **Ataques *Man in the Middle* (MIM)**: Vulnera la confianza mutua en los procesos de comunicación y reemplaza una de las entidades. Ya que la tecnología RFID se basa en la interoperabilidad entre lectores y etiquetas es vulnerable a este tipo de ataques.

- **Inutilización de etiquetas**: Si se somete la etiqueta RFID a un fuerte campo electromagnético ésta se inhabilita. Esta técnica es usada para sustraer productos ya que si se dispone, por ejemplo, de una antena altamente direccional, se pueden inutilizar las etiquetas del producto.

La posibilidad de estos ataques y la facilidad técnica de alguno de ellos, se debe a lo maduro de la tecnología que permite el acceso a lectores y grabadores de RFID a precio muy asequible. Por este motivo, la tecnología debe mejorar aún más, aumentando el nivel de protección de accesos y minimizando las posibilidades de fraude.

Una de las características que la tecnología debe mejorar para aumentar la seguridad es la capacidad de memoria y procesamiento de las etiquetas, la cual limita las posibilidades de implementar mecanismos avanzados de seguridad y cifrado.

Para evitar de una forma sencilla la modificación de la información en las etiquetas es recomendable utilizarlas de sólo lectura, o no escribir los datos directamente en ellas. De esta manera se incluye un código en la etiqueta y el resto de la información se traslada a una base de datos que disponga de mayores medidas de seguridad.

Los métodos de autentificación previos al borrado o desactivación de las etiquetas pueden evitar estas acciones no autorizadas. El cifrado en las etiquetas es otra buena práctica si éstas contienen información privada.

En el caso de medidas de seguridad para el lector, se pueden llevar a cabo técnicas de autentificación para realizar la comunicación entre lector y la etiqueta evitando así la falsificación de identificadores de lector.

7. Riesgos para la privacidad

Además de la posibilidad de ataque a los elementos tecnológicos existe riesgo para la privacidad de los usuarios. Este consiste en el **acceso no autorizado a información personal de los usuarios** utilizando la tecnología RFID. En este caso, se trata de ataques que utilizan técnicas similares a las vistas en los riesgos para la seguridad pero que acceden a este tipo de información, bien porque está incluida en la etiqueta, bien porque está asociada a la misma y se accede al sistema central para consultarla.

La Comisión Europea en 2006 llevó a cabo una consulta pública sobre RFID que expuso la opinión de los ciudadanos europeos acerca de esta tecnología. La posición mayoritaria expresaba la preocupación ante posibles intromisiones en su intimidad.

Las amenazas más relevantes a la privacidad personal son:

- **Accesos no permitidos a las etiquetas:** Éstas pueden contener datos personales, como nombres, fechas de nacimiento, direcciones, etc. Pueden contener también datos personales de cualquier tipo, dependiendo de la aplicación.

- **Rastreo de las personas y/o de sus acciones, gustos, etc.:** Una persona, portando una etiqueta RFID con sus datos y usándola para pagar compras, transportes públicos, accesos a recintos, etc., podría ser observada y clasificada.

- **Uso de los datos para el análisis de comportamientos individuales:** Utilizando técnicas de "minería de datos", este análisis permitiría definir perfiles de consumo basados en las preferencias de los clientes, utilizando esta información para diseñar y orientar la estrategia de marketing y publicidad de las empresas.

Ilustración 19: Otro tipo de etiqueta RFID

La perspectiva de los usuarios sobre estos sistemas es un factor muy importante para el éxito de los mismos. El principal motivo de desconfianza se relaciona con las amenazas a la privacidad y la percepción de no tener un control sobre esta tecnología y sus usos.

Es perfectamente posible, por ejemplo, que el usuario al adquirir un artículo desconozca la presencia del *tag* y éste puede ser leído a cierta distancia sin que el consumidor sea consciente de ello. Si además se paga con tarjeta de crédito, es posible asociar de manera única el artículo con el comprador y almacenar esta información en una base de datos.

Por tanto, la desconfianza se alimenta por las propias características que la tecnología RFID permite. No se trata de una cuestión meramente subjetiva. Por ello, las **medidas para evitar los riesgos para la privacidad** son una tarea prioritaria para las organizaciones y requieren de una correcta planificación del sistema de información. Como norma general se procurará no almacenar datos personales en las etiquetas, evitando así una buena parte de los riesgos. Si no se adoptan medidas para garantizar el respeto a la vida privada se corre el riesgo de generar una percepción social negativa de las tecnologías basadas en RFID.

8. Cumplimiento normativo

La problemática sobre la privacidad de la tecnología RFID despierta gran interés en el seno de la Unión Europea, lo que se refleja en el trabajo de seguimiento realizado por el "Grupo de Trabajo del Artículo 29[5]", en el cual España está representada a través de la Agencia Española de Protección de Datos. En sus informes se puede apreciar un creciente número de trabajos relacionados con la protección de datos en RFID.

Además, la Comisión Europea ha aprobado una Recomendación sobre Privacidad en Comunicaciones RFID denominada "*on the implementation of privacy and data protection principles in applications supported by radio-frequency identification SEC(2009) 3200 final*[6]" de fecha 12 de mayo de 2009. En este documento se establecen recomendaciones y buenas prácticas a la hora de implementar comunicaciones RFID en el marco de la UE.

De los distintos documentos emanados de las autoridades europeas se deriva una conclusión clara. En aquellos casos en los que la etiqueta contiene información personal, o pueda relacionarse con recursos que la vinculen con información de esta naturaleza, serán de aplicación las normas sobre protección de datos personales. Ello ocurrirá por ejemplo cuando:

- Las etiquetas sirvan para recopilar información vinculada con datos personales, por ejemplo relacionando una determinada compra con un código de cliente o una tarjeta de fidelización.

- Las etiquetas sean usadas para almacenar información personal.

- Las etiquetas se usen con la finalidad de rastrear información de los usuarios en ausencia de otro tipo de identificadores. Por ejemplo, si un comercio rastrea los *tags* que se han incorporado a la ropa que viste un

5 *Disponible en: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp146_es.pdf*
6 *Disponible en: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf*

cliente, o a los productos que ha comprado, con la finalidad de trazar perfiles de consumidores. Mucho más obvio sería el supuesto en el que se utilizase el *tag* de algún producto de uso diario, como un reloj, como identificador del cliente para sucesivas entradas en el establecimiento.

Por tanto, aunque exista una regulación específica, la **Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD)** es directamente aplicable a las RFID y con ello cada uno de los principios, derechos y obligaciones que regula.

Por ello tanto los productores o desarrolladores de este tipo de productos, como las organizaciones que los utilicen, sin perjuicio de la plena aplicación del conjunto de la LOPD, deben tener muy en cuenta que:

- Son de plena aplicación los principios del artículo 4 LOPD y por tanto debe realizarse un juicio previo sobre la necesidad de utilizar la tecnología RFID, definir claramente las finalidades y usos de las mismas que además deberán ser proporcionales a las finalidades perseguidas. Además, deberán adoptarse previsiones en relación con la cancelación posterior de los datos personales recopilados cuando no resulten necesarios.

- Los afectados, -como clientes, trabajadores y en general cualquier persona cuya información se indexe mediante el uso directo o indirecto de estas etiquetas-, deberán ser informados de la existencia del tratamiento en los términos del artículo 5 LOPD. Para ello deberán tenerse en cuenta de modo muy específico las siguientes recomendaciones sobre la información:

  a) Debe ser clara, y sobre todo accesible cuando las etiquetas se empleen en ámbitos como el comercial utilizando, cuando sea necesario, carteles claramente visibles.

b) Debe indicar el uso de etiquetas, su localización en el producto, la existencia de lectores y si los *tags* serán objeto de monitorización.

c) Debe indicar el modo de desactivar las etiquetas o extraerlas de los objetos.

d) Debe incluir todos y cada uno de los contenidos requeridos por el artículo 5.1 LOPD.

3 Debe analizarse previamente en qué casos podrán utilizarse las etiquetas con consentimiento y en cuales éste no resulta necesario. El consentimiento debe ser previo, libre, específico e informado. Debe guardarse un especial cuidado cuando se trate de ámbitos especialmente sensibles ya sea por las características de los afectados, como los menores, o por la naturaleza de los datos como por ejemplo los relacionados con la salud.

Debe garantizarse la seguridad de todos y cada uno de los recursos personales, organizativos y técnicos, hardware y software, relacionados con los tratamientos de datos personales vinculados a las RFID. En éste sentido, debe señalarse que la implantación de este tipo de tecnologías en territorio español debe respetar escrupulosamente las previsiones del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Las medidas de seguridad serán particularmente relevantes en aquellos casos en los que la naturaleza de los datos exija aplicar un nivel alto, y cuando debido a la interoperabilidad de este tipo de productos la información pudiera ser leída por organizaciones ajenas a la del responsable de los tratamientos debiéndose evitar a toda costa accesos no autorizados.

En particular pueden deducirse de esta normativa ciertos **parámetros de diseño y seguridad a tener siempre en cuenta:**

- Toda etiqueta RFID debe ser automáticamente desactivada si pasa a manos de un consumidor final.

- No se pueden tomar datos de etiquetas RFID desde dicho momento.

- Se debe informar al consumidor o usuario del momento en que un producto o tecnología incluye etiquetas RFID.

- Debe poder incluirse la opción de mantener informado al usuario de modo automático, mediante pantallas o leds que muestren el estado de activación de la etiqueta.

- No se pueden incluir en etiquetas RFID datos de naturaleza sensible, como por ejemplo, datos relativos a ideología política, religión, o datos de salud, salvo que se trate de una finalidad lícita y legítima y se hayan adoptado medidas de seguridad.

- Se debe posibilitar la desactivación individual, y a requerimiento del usuario, de la etiqueta.

Por último deberá tenerse muy en cuenta el futuro desarrollo de la Directiva 2009/136/CE[7] que indica la necesidad de velar por la protección de los derechos fundamentales, y en particular del derecho fundamental a la protección de datos, cuando las etiquetas RFID estén conectadas a redes públicas de comunicaciones electrónicas o utilicen servicios de comunicaciones electrónicas como infraestructura básica. En este caso, deberán aplicarse las disposiciones pertinentes de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas), incluidas las relativas a seguridad, datos de tráfico y de localización, y a la confidencialidad.

7 **Directiva 2009/136/CE del Parlamento Europeo** *y del consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores. DOUE L377/11 de 18/12/2009.*

9. Recomendaciones para usuarios

Los usuarios domésticos ya utilizan la tecnología RFID y la usarán cada vez más, en tiendas de ropa como sistema antirrobo, en bibliotecas, en sistemas de identificación personal en el acceso a recintos, en los pasaportes, para identificación de mascotas, e incluso como implantes en humanos. Este uso de RFID será beneficioso como otros avances tecnológicos, siempre que se asegure su correcta utilización.

> Los usuarios deben conocer la tecnología, interesarse por el uso que se va a hacer de ella, conocer el modo de ejercer sus derechos y trasladar a los responsables del uso de estas tecnologías la necesidad de respetar su derecho fundamental a la protección de datos en los procesos de diseño de nuevos servicios de RFID.

El principal ataque que puede sufrir la **privacidad** del usuario mediante esta tecnología es el intento de lectura de la información personal y privada almacenada en un dispositivo RFID que se encuentra bajo su posesión.

Para evitar este acceso indeseado a la información existen distintas medidas cuya aplicación dependerá de las necesidades de cada perfil de usuario, ya que no van a ser las mismas las del cliente de un comercio minorista que adquiere una prenda de ropa que las de un industrial que invierte en maquinarias o productos cuyo conocimiento le pueda hacer vulnerable a ciertos riesgos. Estos sistemas son:

- **Utilización de etiquetas *watchdog***: (en inglés “perro guardián”) Estas etiquetas informan de intentos de lectura y escritura que se hagan en su área de actuación.

- **Aislamiento.** Evitando la lectura de las etiquetas salvo en los momentos que se desee. Para ello, sólo hay que introducir la etiqueta en una funda de material metálico o plástico, que haga la función de “*jaula de Faraday*”.

- **Uso de dispositivos que creen una zona segura alrededor del usuario mediante la emisión de ondas que anulen la efectividad de RFID.** Se denominan firewall RFID o también inhibidores de radiofrecuencia. Esta solución es aplicable a entornos de máxima seguridad no compatible con situaciones en las que ciertas lecturas deben ser permitidas y otras no.

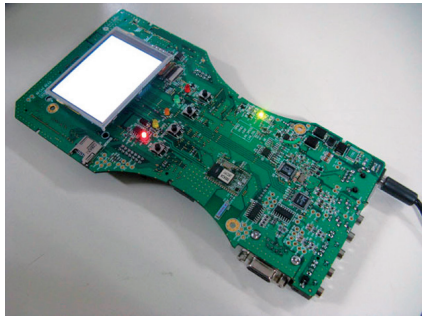


Ilustración 20: Prototipo de Firewall RFID

- **La inutilización de las etiquetas una vez se haya realizado la transacción**, destruyéndola físicamente, o mediante el comando KILL (código incluido en el *tag* que en el momento de su activación a través de un lector lo deshabilita permanentemente).

  Así se limita la rastreabilidad del usuario una vez realizada la compra de productos, garantizando su privacidad.

10. Recomendaciones para proveedores

Muchas organizaciones ya han optado por implantar la tecnología RFID y las previsiones indican que muchas más lo harán en breve. Por este motivo, es de gran utilidad la existencia de una referencia de buenas prácticas que orienten la forma correcta de desarrollar y utilizar estos sistemas.

En primer lugar, es fundamental tener muy presente la privacidad de la información de los usuarios porque **si no se tienen en cuenta los aspectos relacionados con la protección de datos personales podría causarse un daño a los usuarios**, así como perjuicios reputacionales para la entidad, e incluso costes económicos asociados a la pérdida de imagen pública, indemnizaciones, sanciones etc.

En segundo lugar, las organizaciones deben tener en cuenta al crear sus sistemas que están "siguiendo" objetos, no a las personas que los portan. Cumpliendo con esta idea, disminuye la posibilidad de que terceros puedan aprovecharse de la tecnología RFID para acceder a información privada de usuarios.

Las **recomendaciones** se resumen en tres principios generales que son los siguientes:

- **No centrarse sólo en las etiquetas o la tecnología a la hora de valorar un sistema RFID.**

- **Hay que analizar el sistema en su conjunto** ya que los problemas de seguridad o falta de privacidad pueden derivarse de combinaciones en el sistema o de elementos no vinculados directamente a los lectores/emisores RFID.

- **La privacidad y seguridad se debe "trabajar" desde el planteamiento inicial del sistema**, considerándolo una pieza clave del mismo.

- **Es preciso el máximo compromiso, participación y consentimiento de los usuarios del sistema**. Esto se consigue mediante el conocimiento y la participación.

De este modo, las **directrices** para las organizaciones con el fin de proteger la privacidad, son cuatro:

- **Información.** Los consumidores deben ser advertidos claramente de la presencia de códigos electrónicos en los productos o envases.

- **Elección.** Los consumidores deben ser informados de la utilización de RFID en un producto, por si desean descartar o quitar las etiquetas RFID.

- **Educación.** Los consumidores deben tener la posibilidad de informarse correctamente sobre el uso de las etiquetas electrónicas, sus posibilidades técnicas y sus aplicaciones.

- **Registro.** Las empresas deben almacenar registros de uso, mantenimiento y protección de la información obtenida con esta tecnología, y deben publicar sus políticas al respecto.

Este conjunto de recomendaciones parciales deben inspirar un modo de hacer basado en la implementación de procedimientos de evaluación de impacto en la privacidad *(Privacy Impact Assessment-PIA-)*[8] que permitan adoptar decisiones sobre:

1) La elección del producto más respetuoso con la privacidad.

2) La definición de su ámbito de aplicación.

3) La implementación de las medidas de seguridad técnicas y organizativas necesarias.

4) Las metodologías de cumplimiento normativo que garanticen el pleno respeto de lo dispuesto por la LOPD.

8 *Véase ICO (2009): Privacy Impact Assessment (PIA) handbook (Version 2). Disponible en http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html*

11. Buenas prácticas

11.1. BUENAS PRÁCTICAS PARA GARANTIZAR LA SEGURIDAD

Existen soluciones que permiten reforzar la seguridad de los sistemas RFID mejorando sus características técnicas. Además, será necesario un enfoque específico sobre la seguridad global de cada sistema.

- **Renombrado:** Evitando la suplantación de una etiqueta o ataques similares. En este caso, las etiquetas RFID contienen un conjunto de pseudónimos de modo que emite uno diferente cada vez que es interrogado por el lector, de esta forma, un lector malicioso que quisiera suplantar la etiqueta tendría que conocer todos los pseudónimos para realizar la suplantación.

  Esta defensa se puede contrarrestar mediante un lector malicioso que lea cada etiqueta posible muchas veces hasta que se repitan los códigos. Para evitarlo, se controla la respuesta de la etiqueta ralentizando la respuesta en el caso de una secuencia rápida de interrogaciones.

Ilustración 21: Chip RFID

- **Cifrado:** Impidiendo que las partes no autorizadas puedan entender la información enviada utilizando técnicas de cifrado de la información. Los algoritmos de cifrado a usar no son los clásicos, ya que la

capacidad de procesamiento de las etiquetas es limitada. Los fabricantes tienden a crear algoritmos de cifrado.

- **Autenticación:** Evitando así la falsificación de lectores o etiquetas, debiendo introducirse una clave secreta para validar la comunicación lector-etiqueta se consigue que no puedan participar en la comunicación elementos ajenos al sistema.

- **Reducción de la información contenida en las etiquetas:** Grabando en la etiqueta un único código identificador del producto. El resto de la información sensible (precio, tipo de producto, etc.) se almacenará asociada a ese código en un servidor central, minimizando así el riesgo de reescritura de las etiquetas.

- **Otras soluciones no técnicas:** Todas las medidas técnicas citadas anteriormente deberían ser acompañadas de la supervisión humana, esto es, la correcta vigilancia en los comercios, evitando la introducción de dispositivos grabadores de etiquetas, el intercambio de etiquetas de distintos productos, o el empleo por parte de los clientes de jaulas de Faraday para sustraer los productos.

11.2. BUENAS PRÁCTICAS PARA GARANTIZAR LA PRIVACIDAD

Las principales **medidas para proteger la privacidad** de los usuarios son:

- **Notificar el uso de RFID,** de forma clara y mediante símbolos expuestos: en los productos, en los lectores y en las zonas de alcance de los lectores.

- **Dar a conocer en todo momento a los usuarios cuándo, dónde y por qué se va a leer un *tag*.** Incluso indicar la lectura con algún tipo de señal luminosa poco llamativa para evitar molestias, pero indicativa de la actividad.

- **Tener una política de privacidad relativa a la obtención, uso y eliminación de la información personal asociada a RFID,** que deberá ser pública para los usuarios, ofreciendo a estos la posibilidad de conocer, acceder y modificar la información personal asociada a RFID que se almacene.

- **Disponer de personal formado en RFID que conozca las características del sistema instalado y accesible al público,** siendo capaz de responder a las cuestiones de seguridad y privacidad correctamente.

- **No almacenar en los *tags* RFID información personal,** destruyendo lo antes posible dicha información, reduciendo así el riesgo de intromisión en la privacidad del usuario.

- **Retirar, destruir o desactivar los *tags* cuando hayan cumplido su misión.** Si se desea mantener el beneficio del servicio postventa se debe **permitir que la devolución de un producto implique la eliminación de la asociación del *tag* con el usuario.**

- **Ofrecer al usuario facilidades para la retirada, destrucción o desactivación de los *tags*** asociados a productos cuando va a abandonar las instalaciones.

- **No ceder a terceras partes** información asociada a RFID que pueda ser usada para crear perfiles o realizar vigilancia de usuarios.

- **Realizar auditorías de seguridad de sistemas RFID** de forma periódica para garantizar su nivel de seguridad.

más información

http://www.inteco.es

http://observatorio.inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación