

IEEE-UNED



***BOLETÍN  
ELECTRÓNICO***

RAMA DE ESTUDIANTES IEEE-UNED

15-SEPTIEMBRE-2005 (BOLETÍN 3)



6551vascaturas

**RAMA DE ESTUDIANTES IEEE-UNED  
15-SEPTIEMBRE-2005**

**COORDINADOR Y EDITOR:**  
Alejandro Díaz ([adiazh@ieee.org](mailto:adiazh@ieee.org))

**REVISIÓN:**  
Manuel Castro  
Eugenio López  
Alejandro Díaz

**DISEÑO PORTADA:**  
Ignacio García

**AUTORES**

**Alejandro Díaz, Carlos E. Jiménez, José Luís Molina, Agustín Delgado, Microsoft.**

**EN COLABORACIÓN CON EL CAPÍTULO ESPAÑOL DEL  
IEEE EDUCATION SOCIETY**

**AGRADECIMIENTOS**

Agradecemos a nuestro Catedrático de Tecnología Electrónica, Manuel Castro, todo el tiempo y la dedicación que nos ha prestado así como la posibilidad de colaborar con el Capítulo Español del IEEE Education Society para la elaboración del mismo. Agradecemos a todos los autores y a aquellos que han colaborado haciendo posible el Boletín.



# **INDICE**

<b>SUMARIO .....</b>	<b>4</b>
<b>INFORMACIÓN Y URLS.....</b>	<b>5</b>
<b>PROMOCIÓN DE LA DIRECTIVA PROPUESTA DE LA RAMA DE ESTUDIANTES IEEE-UNED PARA EL AÑO 2005 .....</b>	<b>8</b>
<b>SEGURIDAD Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS SISTEMAS DE INFORMACIÓN EN ESPAÑA. ASPECTOS DESTACADOS DE LA LOPD.....</b>	<b>9</b>
<b>TECNOLOGÍA RFID: “UN ÉXITO ASEGURADO” .....</b>	<b>20</b>
<b>SIMULACIÓN ELÉCTRICA DE UN HORNO DE ARCO DE C.A. ....</b>	<b>30</b>
<b>REFRIGERACIÓN DE ALTERNADORES CON HIDRÓGENO PRODUCIDO MEDIANTE ELECTROLIZADORES TIPO PEM (ELECTROLIZADORES DE MEMBRANA POLIMÉRICA) .....</b>	<b>44</b>
<b>MICROSOFT .....</b>	<b>51</b>
<b>INFORMACIÓN GENERAL RESUMIDA .....</b>	<b>59</b>

## SUMARIO

Para comenzar el boletín electrónico nº 3, se presenta como en ediciones anteriores un primer apartado de **Información** general de la Rama y **URLs** de interés general propuestas por los miembros con comentarios.

A continuación se expone un artículo “**Seguridad y Protección de datos de carácter personal en los sistemas de información en España. Aspectos destacados de LOPD**” por *Carlos E. Jiménez*, miembro del IEEE, el cuál resultara de interés a aquellos que deseen profundizar en la Ley Orgánica de Protección de Datos, para poder trabajar de forma legal con información de carácter personal. El cual resulta un tema bastante interesante teniendo en cuenta en uso masivo de información a través de Internet que se viene realizando hoy en día por muchas empresas

El siguiente artículo escrito por el coordinador del boletín electrónico de la rama, *Alejandro Díaz*, es “**Tecnología RFID. Un éxito Asegurado**”. En él, se realiza una introducción a la Tecnología de Identificación por Radio Frecuencia (RFID). La cual esta levantando muchas expectativas en los últimos tiempos para todo tipo de aplicaciones de identificación, pero especialmente en la logística y en la cadena de suministro.

Más adelante, *José Luis Molina*, nos resume el trabajo realizado en su proyecto fin de carrera a través de un interesante artículo “**Simulación Eléctrica de un horno de Arco**”. El cuál consiste en el escalado de la instalación de un horno de arco, su posterior materialización y su uso final para la ejecución de ensayos reproduciendo el comportamiento eléctrico del horno.

Tras ello, Agustín Delgado, nos habla de los métodos de refrigeración en los alternadores mediante su atractivo artículo “**Refrigeración de alternadores con Hidrógeno producido mediante electrolizadores tipo PEM**”. Los alternadores son máquinas que durante su operación producen mucho calor, por lo que se deben utilizar elementos que lo refrigeren, como puedan ser el aire, o el explicado en este artículo, el hidrógeno.

Por último en la sección de experiencias laborales y empresas, la empresa **Microsoft** nos aporta un artículo que esperamos sea de gran valor para todos aquellos que lo lean. En el se nos da información sobre la compañía, productividad, así como datos sobre la política seguida por esta importante empresa del sector informático. A destacar el esfuerzo por estrechar relaciones con las Universidades, o su interés en la difusión de la tecnología entre otros.

## INFORMACIÓN Y URLS

En esta sección se pretende dar información general de la Rama y URLs de interés general propuestas por los miembros.

Tras finalizar el pasado curso con gran satisfacción por la consolidación de la rama de estudiantes de IEEE-UNED, entramos en este nuevo curso (2005-2006) con energías renovadas y la responsabilidad por parte de todos los miembros de mejorar el buen trabajo realizado durante el pasado año por toda la junta directiva de la rama. Intentando poco a poco de mejorar lo máximo posible todas las actividades ya consolidadas como son el boletín, y de iniciar otras como puedan ser seminarios, cursos, etc. Eso sí intentando al igual que durante el 2004 que nuevos miembros se afilien y de esta forma ir creciendo en número y en actividades. La clave del éxito de la Rama de la UNED, al igual que del resto de Ramas de todo el mundo, es el voluntariado. Por tanto, agradecer a todas las personas que están haciendo esto posible y que sin su ayuda no se hubiera podido llevar a cabo. Agradecer a todos los miembros que están en la Rama, que han decidido formar parte de ella y agradecer a todos los voluntarios que han colaborado en las actividades realizándolas y llevándolas a cabo, así como, a todos los autores de los artículos.

Parte de la idea de ofrecer una diversidad cultural diferente entre los estudiantes donde nosotros mismos somos los que dedicamos los esfuerzos voluntarios en pro del bien común en cuanto a conocimientos, contactos y la posibilidad de compartir actividades técnicas, científicas y tecnológicas.

La Rama se consigue consolidar inicialmente con 37 miembros en noviembre del año 2004.

La información general sobre sus actividades e información de cómo hacerse miembro la hemos colocado en la página Web: [www.ieec.uned.es/IEEE](http://www.ieec.uned.es/IEEE) dentro de Rama de Estudiantes.

Las actividades principales que se pretenden realizar son: charlas, cursos, congresos, concursos, actividades educativas, visitas a empresas y organizaciones, interrelación cultural y multidisciplinar y cualquier actividad que quiera desarrollar cada uno de sus miembros.

Actualmente puede participar cualquier estudiante de las carreras de Ingeniería Informática y de Ingeniería Industrial de la UNED.

Las actividades realizadas en el año 2005 se resumen a continuación:

- Creación del Boletín nº 2 con interesantes artículos y experiencias de diferentes miembros de la Rama y el actual Boletín nº 3.
- Contacto con Microsoft para realización de actividades. Colaboran en el boletín nº 3. Contacto con Accenture a través de un miembro de la Rama para tratar de realizar una actividad análoga a la realizada con DMR para fomentar la relación universidad-empresa (pendiente).
- Creación de varios comités dentro de la Rama: Comité de Socios y Bienvenida (coordinador Francisco García Sevilla), Comité de actividades (Coordinador Elio Sancristobal) y comité para el Boletín Electrónico (Coordinador Alejandro Díaz)
- Realización de una presentación en Director para facilitar la forma de hacerse socio por Internet de las personas interesadas. Se establece contacto con Ricardo Varela (representante de alumnos de la Región 8) que se interesa por la aplicación para tratar de establecer un proyecto en la línea de la ayuda a hacerse miembro a las personas interesadas.
- Proyecto UNITeS: Seguimos impulsando el proyecto en colaboración con la Universidad.
- Curso de Robots. Realizado con la Universidad Alfonso X el Sabio en Abril. Participan varias personas de nuestra Rama.
- Se ha establecido el contacto con otras Ramas de manera que nos apoyamos unas a otras en la realización de actividades conjuntas.
- Estamos apuntados para participar en el CNR 2005 que se celebrará en Valencia.

La Web del IEEE en la UNED es: <http://www.ieec.uned.es/IEEE/> donde podéis encontrar información sobre qué es el IEEE y la Rama de estudiantes, cómo hacerse miembro, ver información sobre otras Ramas y una sección de eventos y actividades donde se irán colocando las actividades que se van a ir realizando y que se han realizado. **Todos las personas interesadas en saber más información o en hacerse miembro, escribir un mail a: [elopez@ieec.uned.es](mailto:elopez@ieec.uned.es)**



Las direcciones propuestas por los miembros, para este boletín, se muestran a continuación:

- <http://www.alpertron.com.ar/INTEL.HTM> (28/04/05)

Habla de los microprocesadores Intel 4004, 8008, etc., hasta el Pentium de Intel incluso de algunos lenguajes de programación de los mismos.

- <http://mssimplex.com/microprocesador.htm> (01/05/05)

Página donde relata brevemente el primer microprocesador de Intel 4004 con la teoría de la firma Japonesa Busicom de realizar el encargo a Intel para crear elementos programables para una calculadora.

- <http://voltio.ujaen.es/casanova/simu8085/sim8085.htm> (02/05/05)

Página donde se puede descargar un simulador del microprocesador 8085.

## PROMOCIÓN DE LA DIRECTIVA PROPUESTA DE LA RAMA DE ESTUDIANTES IEEE-UNED PARA EL AÑO 2005



**Eugenio López.** Presidente de la Rama de Estudiantes del IEEE-UNED. Estudiante de Doctorado en el DIEEC. Ingeniero Industrial. [elopez@ieec.uned.es](mailto:elopez@ieec.uned.es)



**Ignacio García.** Vicepresidente de la Rama de Estudiantes del IEEE-UNED. Estudiante de Ingeniería Industrial. [nachogcg@hotmail.com](mailto:nachogcg@hotmail.com)



**Elio Sancristobal.** Secretario de la Rama de Estudiantes del IEEE-UNED. Estudiante de Doctorado en el DIEEC. Ingeniero Informático. [esancr@yahoo.es](mailto:esancr@yahoo.es)



**Javier García.** Tesorero de la Rama de Estudiantes del IEEE-UNED. Estudiante de Ingeniería Industrial. [garciajimenez@hotmail.com](mailto:garciajimenez@hotmail.com)



**Manuel Castro.** Catedrático de Tecnología Electrónica. Profesor Consejero de la Rama de Estudiantes del IEEE-UNED. Miembro Señor del IEEE y actual presidente del capítulo Español de la IEEE Education Society recién creada en España. [mcastro@ieec.uned.es](mailto:mcastro@ieec.uned.es)



**Alejandro Díaz.** Coordinador del Boletín Electrónico de la Rama de Estudiantes del IEEE-UNED. Ingeniero Industrial por la UNED. [adiazh@ieee.org](mailto:adiazh@ieee.org)



**Francisco García Sevilla.** Coordinador del Comité de socios y bienvenida. Ingeniero Industrial. [fgsevilla@ieee.org](mailto:fgsevilla@ieee.org)



# SEGURIDAD Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS SISTEMAS DE INFORMACIÓN EN ESPAÑA. ASPECTOS DESTACADOS DE LA LOPD

## I.- Introducción

Desde un punto de vista técnico, el mantenimiento, actualización, diseño, construcción o implantación de un sistema de información requiere tener en cuenta aquéllos aspectos esenciales que darán al sistema una calidad óptima, así como aquéllos que le otorgarán una serie de características necesarias para su adecuación a los requerimientos y necesidades del usuario y, en definitiva, todos aquéllos que lleven a la materialización final del nuevo sistema proyectado, tanto desde un punto de vista técnico como operativo.

Sin embargo, actualmente, a la hora de realizar determinadas tareas relacionadas con los sistemas de información, no sólo estos aspectos toman relevancia. Con la llegada de las nuevas tecnologías y su aplicación y utilización generalizada en una sociedad en la que la información se ha convertido en recurso y materia prima estratégico, se ha puesto de manifiesto la importancia de regular de forma detallada aspectos de la información que requieren una especial cobertura legal actualizada.

Directivas de la Unión Europea, normas como la ISO 17799:2000 son indicativo de la importancia de lo que aquí se trata. En España, especialmente relevante es la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) que en el año 2000 entra en vigor (modificada por dos Sentencias del Tribunal Constitucional del año 2000).

Fundamentalmente serán aquí objeto de exposición, determinados aspectos de la LOPD y del Reglamento de medidas de seguridad de los ficheros automatizados de titularidad privada que contengan datos de carácter personal.

La importancia de este tema radica fundamentalmente en la directa y estrecha vinculación existente entre ciertos aspectos técnicos y aspectos jurídicos contemplados en la legislación actual sobre los datos de carácter personal, en relación con servicios de la Sociedad de la Información, sistemas de información y Nuevas Tecnologías y que, sin lugar a dudas, un profesional de la informática debe de conocer, máxime cuando va a estar constantemente en contacto con todo tipo de datos, entre los que se encuentran datos con unas características que les hacen ser susceptibles de especiales medidas de seguridad.

Para ver el alcance real de este tema y darse cuenta de la necesidad de comprender y considerar actualmente estos aspectos basta con plantearse, por ejemplo, las siguientes preguntas: ¿qué requisitos debe tener el aviso legal de

una página Web que contiene un formulario para obtener datos de posibles clientes?; ¿es obligatorio comunicar a la Agencia Estatal de Protección de Datos la existencia de un fichero con nombres y direcciones de correo electrónico obtenido con una página Web y que se aloja en una base de datos?; en una empresa con un sistema CRM, ¿el responsable oportuno debería de pedir autorización a los titulares, para que los datos sean compartidos con otro departamento de la misma empresa, distinto del que obtuvo dichos datos?; si una aplicación que confecciona nóminas entre las que se incluye la de un trabajador del que aparecen datos fiscales que, sin lugar a dudas, establecen una correspondencia directa con la identidad de una persona que padece un 33% de minusvalía física ¿se debería aplicar el máximo nivel de seguridad?.

Si no existe un asesor experto en Derecho de las Nuevas Tecnologías, un asesor legal experto en la materia, o una persona directamente designada como responsable de seguridad que apoye las tareas de actualización de sistemas de información, o las tareas de diseño, desarrollo, implantación y, sobretodo, mantenimiento del sistema, será realmente necesario que el ingeniero comprenda y tenga muy en cuenta la correspondiente normativa legal aplicable, en aras del cumplimiento de la legalidad y de una garantía de calidad en la prestación de los servicios contratados.

Incluso en mayor medida, los responsables de los ficheros y, en general, aquéllos que sean responsables en alguno de los niveles establecidos, respecto de datos de carácter personal, deberán de cumplir estrictamente con una serie de requisitos establecidos por la LOPD. No debemos olvidar que dicha ley regula derechos fundamentales recogidos en la Constitución Española, los cuales son susceptibles de especial protección. Por ello, nos encontramos ante una normativa enormemente restrictiva, que hace que sea necesaria una especial atención a la hora de trabajar con datos que por sus características se encuentren dentro de los supuestos establecidos por dicha ley: los datos de carácter personal.

Teniendo en cuenta la casuística que se puede presentar, llegados a este punto es importante señalar - en orden a determinar un contexto y marco general de aplicación de lo que aquí se expone- que se supondrán dadas aquí ciertas premisas en relación con determinados aspectos la LOPD y la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico que, en otro caso, sería necesario analizar individualmente, a saber: los ficheros, servidores, equipos y, en general, sistemas físicos y sus aplicaciones, así como las personas físicas y jurídicas titulares de los mismos y, en general, los distintos responsables, se encuentran en territorio español, y es en dicho territorio donde se desarrollan las distintas actividades y servicios que se prestan.

## II.- Aproximaciones conceptuales y principios en la LOPD

La LOPD será de aplicación cuando existan ficheros con datos de carácter personal, cuyo tratamiento sea efectuado en territorio español en el marco de actividades de un establecimiento del responsable del tratamiento o, cuando el responsable del tratamiento no establecido en territorio español le sea de aplicación la legislación española según las normas de Derecho Internacional público o, cuando el responsable del tratamiento –aunque no esté en territorio de la Unión Europea- utilice en el tratamiento de datos medios situados en territorio español.

Es muy importante señalar aquí que con el concepto de “datos de carácter personal” se está aludiendo a cualquier información concerniente a personas físicas identificadas o identificables, lo que hace que el alcance de la LOPD se extienda de modo generalizado y, por ello, sus restricciones y medidas de seguridad, también.

Asimismo, destacar la definición que dicha ley establece para los términos de tratamiento de datos, fichero, responsable del fichero, afectado o interesado y encargado del tratamiento.

- “Tratamiento de datos”, comprende la recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación y cesión.
- “Fichero” comprende todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de creación, almacenamiento, organización y acceso.
- “Responsable del fichero” es aquella persona física o jurídica que decida sobre la finalidad, contenido y uso del tratamiento.
- “Afectado o interesado” es la persona física titular de los datos objeto de tratamiento.
- “Encargado del tratamiento”, es aquella persona que trate datos personales por cuenta del responsable.

Señalar, igualmente, que se establecen una serie de requisitos sobre la calidad de datos. Así, partiendo de la base de que los datos poseen unas cualidades que les hacen ser susceptibles de la aplicación de la LOPD, su contenido o extensión, en todo caso, se ajustará a la finalidad para la que se recogen y, única y exclusivamente, podrán ser utilizados con la autorización del titular de los mismos –al que le asisten una serie de derechos de consulta, acceso, rectificación y cancelación-.

Como acabo de indicar, los datos podrán ser utilizados exclusivamente para el fin con el que se recogen. Sin embargo, la ley permite realizar con los datos determinados procesos como, por ejemplo, los estadísticos. No obstante,

es claro que si dicho tratamiento estadístico implicara un acceso a los datos por personas distintas a las autorizadas, sería necesario extender el nivel de seguridad a éstos o bien, realizar un proceso de disociación en los datos, para poder utilizar parte de dichos datos en otro tipo de procesos, siempre y cuando los datos dejen de poseer las cualidades y características que les hacen susceptibles de aplicación de la LOPD.

### **III.- Algunos aspectos relevantes acerca de la seguridad de los datos de carácter personal y de los ficheros de titularidad privada**

Existe una clasificación que agrupa los tipos de datos de carácter personal en tres grupos, existiendo así tres niveles de seguridad distintos. Cada grupo debe tener aplicadas una serie de medidas de seguridad y cumplir con una serie de requisitos establecidos por la LOPD y el Reglamento de Seguridad.

Para todos los grupos, el responsable del fichero y, en su caso, el encargado del tratamiento, están obligados al deber de secreto respecto de los datos, y al deber de guardarlos, debiendo adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal; no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones establecidas respecto de su integridad, seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

La LOPD establece que toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal, lo deberá notificar previamente a la Agencia de Protección de Datos debiéndose, asimismo, comunicar a dicha Agencia los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

Si se pretende realizar una cesión de los datos, el responsable del fichero debe informar de ello a los afectados, indicando la finalidad y el nombre y dirección del cesionario y, en lo referente a las transferencias internacionales de datos, la LOPD resalta la obligación, con alguna excepción, de que exista autorización previa del Director de la Agencia de Protección de datos, la cual, sólo se otorgará si existen garantías de un adecuado nivel de protección en el país de destino.

Las exigencias anteriores, -junto con aquéllas otras que la ley establece y que, por extensión, no están detalladas aquí- provocan la necesidad de poner en marcha una serie de dispositivos y medidas de seguridad e, incluso, la creación de una figura responsable de seguridad encargada específicamente de velar por los distintos aspectos que se requieren, en relación con los datos de carácter personal.

Especialmente interesante resulta el “traspaso de obligaciones” que surge de una prestación de un servicio a un cliente, que implique el tratamiento de este tipo de ficheros. En este caso, se deberá de celebrar un contrato de modo que se pueda acreditar su celebración y contenido. En dicho contrato se deberá establecer de forma expresa que el encargado del tratamiento sólo tratará los datos conforme a las instrucciones del responsable del tratamiento y conforme a lo establecido en el contrato y, aún más, el prestador del servicio deberá de adoptar las medidas de seguridad establecidas para el tipo de fichero, las cuales deberán de figurar en el contrato.

#### **IV.- Niveles, procedimientos y medidas de seguridad**

Es en el Reglamento de Medidas de Seguridad, donde se establecen las características y requisitos de seguridad que van a exigirse para aquéllos ficheros en los que existan datos de carácter personal, estableciéndose incluso un régimen de trabajo fuera de los locales de la ubicación del fichero, requisitos de seguridad para ficheros temporales, etc.

Las medidas de seguridad que se exigen están clasificadas en tres niveles (nivel básico, nivel medio y nivel alto), dependiendo del tipo de información que contengan los ficheros.

Se establece un nivel básico para todos los ficheros de carácter personal excepto aquéllos que contengan:

- Datos relativos a comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, conjunto de datos que permitan obtener una evaluación de la personalidad del individuo y los demás establecidos en la ley, los cuales deberán reunir, además de las medidas del nivel básico, las del nivel medio.
- Datos que la LOPD califica de especialmente protegidos, relativos a ideología, afiliación sindical, religión, creencias, origen racial o étnico, salud y vida sexual, así como los datos recabados para fines policiales sin consentimiento de las personas interesadas, que deberán de reunir, además de las medidas de nivel básico y medio, las de nivel alto.

Estos niveles se califican como “mínimos exigibles”.

Asimismo, las redes de comunicaciones a través de las cuales se accede a los datos, deberán de garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

## 1.- Procedimientos y medidas de seguridad de nivel básico

### a) Documento de Seguridad

El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos de carácter personal y a los sistemas de información. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Dicho documento deberá contener:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido el Reglamento.
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Señalar que las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de Información estarán claramente definidas y documentadas, de acuerdo con lo previsto en el documento y que, asimismo, el responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

En cuanto al registro de incidencias, el procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

### b) Identificación y autenticación

El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso. Se establece, además, que cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.



Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y, mientras estén vigentes, se almacenarán de forma ininteligible.

#### c) Control de acceso

Se resalta la obligación de que los usuarios tengan acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, debiendo el responsable del fichero establecer los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

La relación de usuarios actualizada de la que se habla en el punto b) de este epígrafe contendrá el acceso autorizado para cada uno de ellos. Asimismo, exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

#### d) Gestión de soportes

Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

#### e) Copias de respaldo y recuperación

El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. Estos procedimientos, deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Se señala que deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

## 2.- Procedimientos y medidas de seguridad de nivel medio

#### a) Documento de seguridad

El documento de seguridad deberá contener, además de lo indicado para el nivel básico, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

#### b) Responsable de seguridad

El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. Esta figura es obligatoria tanto en el nivel medio como en el alto.

#### c) Auditoría

Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años. Esta auditoría es un híbrido entre auditoría informática y auditoría jurídica. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas. Asimismo, los informes quedarán a disposición de la Agencia de Protección de Datos.

#### d) Identificación y autenticación

El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

#### e) Control de acceso físico

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Es importante señalar aquí que esto tiene unas implicaciones realmente importantes, en relación con los distintos niveles de seguridad y la ubicación física de los equipos y ficheros. Así, si dos personas distintas tienen –para el acceso físico- privilegios de acceso autorizado de niveles distintos (por ejemplo, uno de nivel básico y otro de nivel medio), serán necesarios dos locales físicos distintos, uno para nivel básico y otro para nivel medio.



#### f) Gestión de soportes

Deberán establecerse sistemas de registros, tanto de entrada como de salida, de soportes informáticos. El registro de entrada deberá permitir conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

El registro de salida de soportes informáticos permitirá conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar también debidamente autorizada.

Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a proceder a su baja en el inventario.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

#### g) Registro de incidencias

En el registro de incidencias deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Además, será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

#### h) Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

### 3. Procedimientos y medidas de seguridad de nivel alto

#### a) Distribución de soportes

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

#### b) Registro de accesos

De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

Para el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. Los mecanismos que permiten el registro de los datos, que se han detallado anteriormente, estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos. El período mínimo de conservación de los datos registrados será de dos años.

El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

#### c) Copias de respaldo y recuperación

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan cumpliendo, en todo caso, las medidas de seguridad exigidas en el Reglamento.

#### d) Telecomunicaciones

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

## V.- Sanciones

Por último, sin entrar específicamente en el elenco de infracciones existente, señalar aquí que las infracciones tipificadas en la ley y su reglamento se clasifican en tres tipos: leves, graves y muy graves.

La Agencia Española de Protección de datos ha expresado en repetidas ocasiones que las sanciones por infracciones de la LOPD y su reglamento, cumplen un importante papel disuasorio. No en vano, el importe de las sanciones es el más alto de la Unión Europea siendo, además, compatibles con las acciones civiles y penales que el interesado pudiera ejercitar.

Así, las infracciones leves serán sancionadas con multas de 601,01 € a 60.101,01 €, las infracciones graves, serán sancionadas con multas de 60.101,01 € a 300.506,05 € y las infracciones muy graves, se sancionarán con multas de 300.506,05 € a 601.012,10 €.

Carlos E. Jiménez Gómez

## **TECNOLOGÍA RFID: “Un éxito asegurado”**

La tecnología **RFID** ("Radio Frequency Identification"), o identificación por radiofrecuencia, esta considerada por muchos expertos en la nueva tendencia tecnológica, comparable por algunos al “boom” que ocasionó la red Internet hace unos años. Los sistemas RFID hacen uso de ondas de radio para transmitir datos desde un lector a la tarjeta o etiqueta, la cual lleva incorporado un dispositivo electrónico donde se almacena la información. Sus aplicaciones pueden variar desde la identificación de animales o el control de accesos, hasta el pago de peajes en autopistas. Pero la verdadera aplicación que marcará el éxito de la tecnología será la implantación de RFID en la cadena de suministro.

### **I. INTRODUCCIÓN**

La tecnología RFID no se trata de una tecnología nueva, en realidad su nacimiento surgió durante la Segunda Guerra Mundial, cuando el ejército británico lo implantó para distinguir sus aviones de los aviones enemigos. El sistema fue conocido como IFF o “Friend or Foe”. Pero su verdadero uso se empezó a dar a raíz de grandes avances en electrónica (circuitos integrados, microprocesadores, etc.) y del desarrollo de redes de comunicación. Durante la década de los 90 surgieron los primeros estándares mundiales, y a partir de entonces y en un periodo corto de tiempo, el mundo entero se verá invadido por todo tipo de etiquetas RFID o "transponders".

Su mercado durante los últimos años ha crecido de una forma considerable, hace tan sólo unos años parecía increíble pensar que la tecnología tuviera cabida en tan diversas aplicaciones. Pero, por una parte los grandes y continuos avances tecnológicos, así como el esfuerzo por establecer estándares han facilitado su expansión. Hoy en día tiene aplicación en la identificación animal, o de personas en controles de acceso. En sistemas inmovilizadores de vehículos, pago de peajes, como método de pago en el transporte público, para el rastreo de objetos durante la cadena de suministro, en bibliotecas, para aplicaciones médicas, en la industria farmacéutica, etc. Y actualmente se están llevando a cabo numerosos proyectos pilotos en todo el mundo para implantar la nueva tecnología en otras muchas aplicaciones, y beneficiarse así de sus numerosas ventajas.

RFID es un sistema de identificación, la cual no necesita de contacto para poder comunicarse. La comunicación se realiza a través de ondas electromagnéticas. El sistema está basado en un lector o interrogador ("transceiver"), y en un "transponder" o "tag" localizado sobre el objeto a identificar. A menudo el lector, que puede ser fijo o manual, dispone de un interfaz adicional (RS232 o RS485) para comunicarse con un host donde reside una base de datos.

El "transponder" consiste en un chip unido a una antena, el cual trabajará a una determinada frecuencia dependiendo de las necesidades del sistema. El lector es el dispositivo que maneja la comunicación entre lector y el PC (host) y su antena posee diferentes tamaños y tipos, según requiera el sistema mayor o menor distancia de comunicación.

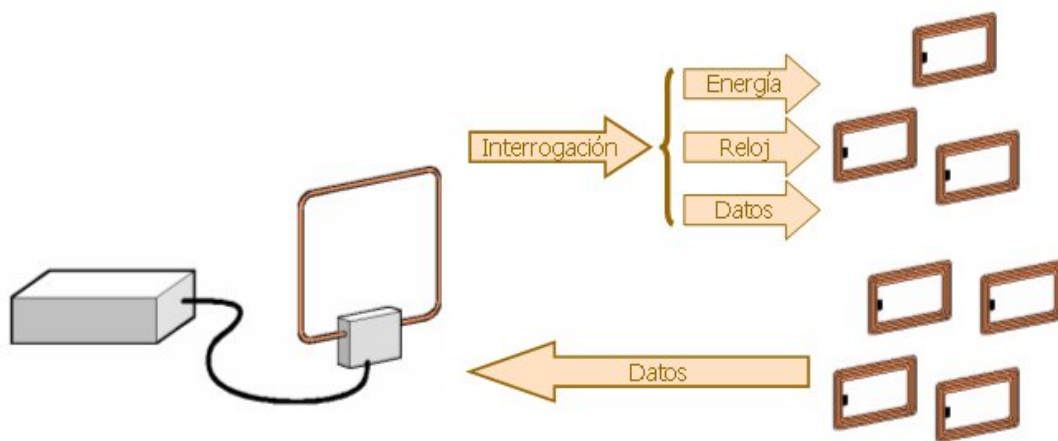


Figura representativa del modo de operación de la tecnología RFID entre el lector y los tags

## II. PRINCIPALES CARACTERÍSTICAS

Entre las principales características de los sistemas RFID podemos destacar:

- **No necesitan línea directa de visión:** Los "transponders" no necesitan estar visibles para poder ser leídos o grabados con datos.
- **Son Robustos:** Al no tener que estar visibles, los "tags" pueden ser encapsulados en el interior de materiales, protegiéndolos de ambientes agresivos que pudieran perjudicar el funcionamiento del dispositivo.

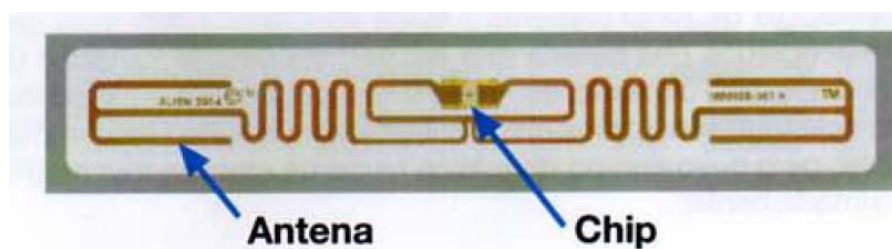
- **Velocidad de lectura:** Los "transponders" o "tags" poseen capacidades de lectura bastante rápidas, la cuáles varían según la banda de frecuencia utilizada. Característica especialmente útil en aplicaciones donde el objeto a identificar se encuentre en movimiento, como por ejemplo en el pago de peajes en autopistas.
- **Lectura simultánea de objetos:** Es una característica que aporta a la tecnología la capacidad de tratar numerosos objetos a la vez dentro del campo de lectura de radio frecuencia.
- **Son Seguros:** Los "tags" resultan más difíciles de falsificar que otras tecnologías. Éstos poseen desde el proceso de fabricación de un único número identificador distinto al resto de los transponders en todo el mundo.
- **Son programables:** Algunos "tags" son únicamente de lectura, mientras otros poseen la capacidad de lectura/escritura. Lo cual significa que la información puede ser grabada en el "tag", tras por ejemplo un cambio en el estado del producto durante un determinado proceso.

### III. HARDWARE EN LOS SISTEMAS RFID

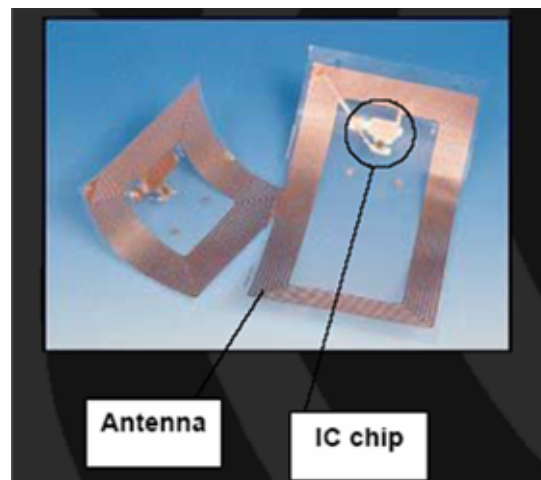
En todo sistema RFID se puede hablar de hardware como por ejemplo, los "transponders", lectores, antenas, etc.

Los "transponders" de identificación por radiofrecuencia, también conocidos como RFID tags, se han utilizado de varias formas durante muchos años. Estos se pueden clasificar en dos grupos:

- **"Transponders" pasivos:** Los cuales no poseen fuente de alimentación externa, y donde la energía necesaria para poder establecer la comunicación entre "tag" y lector la recoge del campo eléctrico o magnético generado por el lector. Como principal ventaja frente a los "transponders" activos destacan, su bajo coste, su pequeño tamaño y su durabilidad. Pero por otro lado su alcance es menor y la potencia requerida por el lector es mayor.



Etiqueta o tag UHF (868-915 MHz)



Tag de HF (13,56 MHz) obtenido del fabricante Texas Instruments, donde se puede observar antena y IC Chip.

- **"Transponders" activos:** Son aquellos que poseen su propia fuente de alimentación o batería. Sus características son, largo alcance, inmunidad al ruido y ratios de transmisión de datos más elevados. Y sus desventajas son su elevadísimo precio, su tamaño y su relativa corta vida. Por el momento sus mayores aplicaciones se dan en el rastreo de aquellos bienes que justifiquen el elevado coste del tag.

Una vez explicados los dos tipos de "tags", debemos mencionar que estos transponders son encapsulados en diferentes tipos de formatos como pueden ser:

- **Discos o monedas:** Formato muy común, con diámetros desde unos pocos mm hasta 10 cm aproximadamente. Fabricados usualmente con un agujero para poderlos atornillar al objeto a identificar.
- **Alojado en cristal:** Formato creado para ser inyectado bajo la piel de animales con propósitos de identificación.
- **Alojado en plástico:** Creado para aplicaciones con altas prestaciones mecánicas, fácilmente integradas en otros productos como en las llaves de los coches para los sistemas electrónicos de inmovilización.
- **ID-1:** Formato característico de las tarjetas inteligentes sin contacto, usado típicamente en las tarjetas telefónicas y de crédito. Con dimensiones de 85,72 mm x 54,03mm x 0,76 mm.

- **"Smart Label" o etiquetas inteligentes:** Consiste en un "tag" encapsulado en delgado papel de solo 0,1 mm de grosor con un adhesivo. Lo suficientemente flexible para ser pegado en equipajes, paquetes y bienes de todo tipo.



Ejemplos de diferentes tags o transponders

El "transponder" es un dispositivo electrónico, que puede contener o una pura memoria o un microprocesador dependiendo de las necesidades del sistema. Los "transponders" con solo memoria contienen memorias RAM, ROM, EEPROM o FRAM y un interfaz HF para proporcionar energía y permitir la comunicación con el lector.

Por una parte el "transponder" esta formado por un circuito resonante o antena, constituido por una bobina y un condensador conectados en paralelo, la cual emite y recibe las ondas usadas para la comunicación entre lector y tags.

También contiene un interfaz HF, formado por el canal de transmisión de alta frecuencia entre lector y tag, y los circuitos digitales del transponder. Al realizarse la comunicación en ambos sentidos, el "transponder" desempeña las funciones de un clásico MODEM (modulador-demodulador) usado en las convencionales líneas telefónicas.



Por último podemos nombrar al circuito digital, donde la lógica de direccionamiento y seguridad forma el corazón del "transponder". Acompañado por un bloque de registro de entradas y salidas ("I/O register"), la memoria de datos compuesta por una ROM para datos permanentes como el número de serie y una EEPROM o FRAM, y una opcional unidad de criptografía ("Crypto Unit").

Mientras que otros "transponders" prescinden de las poco flexibles maquinas de estados al poseer un microprocesador. Cuyas memorias están estructuradas en bloques de tamaños de 16 bits, 4 o 16 bytes, para facilitar el direccionamiento de la memoria en el chip.

El lector o "tranceiver" es un dispositivo que activa y da potencia al "transponder" y recupera la información contenida en la misma. Compuesto por una antena y un controlador, que codifica, decodifica, verifica y almacena datos, administra las comunicaciones con los "transponders" y se comunica con la fuente ("host"). Algunos dispositivos solo pueden leer, mientras otros pueden leer y escribir. Pueden ser manuales o fijos. Todos los lectores pueden reducirse a dos bloques funcionales: el sistema de control y la interfaz HF.

La unidad de control se basa en un microprocesador, para la comunicación con el software de la aplicación y ejecución de comandos, codificación y decodificación de señales, control de la comunicación con las etiquetas, ejecución de algoritmos anticolidión, autenticación entre etiqueta y lector, y encriptación y desencriptación de la información transmitida...

El interfaz HF genera la energía suficiente para activar las etiquetas, también realiza la modulación de la señal de transmisión para enviar datos al "transponder" y recibe y demodula las señales transmitidas por una etiqueta

Por ultimo hablaremos del último dispositivo que interviene en todo sistema RFID, y del cual ya nos hemos referido anteriormente. En todo sistema RFID existen dos antenas, la antena del lector, y otra la del "transponder". Podemos decir que las antenas son los dispositivos que controlan la adquisición de datos y comunicación del sistema. Su ubicación depende de la aplicación.

#### IV. FRECUENCIAS UTILIZADAS

Los sistemas RFID se pueden clasificar como sistemas de radio al radiar y generar ondas electromagnéticas. Por lo tanto se debe considerar que éstos no interfieran en otros servicios de radio (policía, servicios de seguridad, televisión, móviles,...) situados en su perímetro de acción. Por esta razón el rango de frecuencia reservados a los sistemas RFID queda restringido a los rangos utilizados en aplicaciones médicas, científicas o industriales (ISM o "International Scientific & Medical"). Que pueden ser resumidas en las cuatro siguientes:

- **LF ("Low Frequency"):** Se tratan de sistemas que trabajan a frecuencias por debajo de 135 kHz. Normalmente con "transponders" pasivos de solo lectura o lectura/escritura de tamaño superior que otras tecnologías. Con rangos de lectura más cortos, y antenas requeridas de mayor tamaño y precio.
- **HF ("High Frequency"):** Tecnología utilizada en bastantes aplicaciones. Cuya frecuencia es 13.56 MHz. Con "transponders" de solo lectura, lectura/escritura, o escritura una vez y lectura muchas (WORM). Con costes menores que la anterior y con rangos de hasta 1 m. Estandarizadas a través del ISO 15693 o el ISO 14443.
- **UHF ("Ultra-High Frequency"):** Cuyo banda de frecuencia oscila de 868 a 915 MHz, dependiendo del país donde se este trabajando. Con posibilidad de "transponders" pasivos o activos, de largos alcances y velocidades de transmisión rápidas. Estándares EPC e ISO 18000-6.
- **SHF (Microondas o "Microwaves"):** Su banda de frecuencia esta comprendida entre 2,45 y 5,8 GHz. Los "transponders" pueden ser activos o pasivos, de lectura, lectura/escritura, o WORM. Las características de esta tecnología es similar a la UHF, pero con mayor velocidad de transmisión. Aunque por otro lado su coste se dispara al doble que las otras frecuencias explicadas anteriormente. Poseen problemas de absorción por el agua y son reflejados por metales.

## V. ESTÁNDARES

La creación de estándares es responsabilidad del comité técnico de la ISO. En este apartado se hablará de algunos de los más conocidos estándares existentes por el momento en los sistemas que integran tecnología RFID.

Dos de los más conocidos por todos son el ISO 14443 y el ISO 15693, utilizados por las tarjetas inteligentes sin contacto. Y adoptada por los principales fabricantes, como "Texas Instruments" y "Philips Semiconductors", para los transponders RFID. El primero de ellos se utiliza en tarjetas inteligentes de acoplamiento próximo (0-10 cm), y el ISO 15693 en tarjetas inteligentes con acoplamiento de vecindad (0-1m).

La existencia de estándares internacionales es vital en la maduración de cualquier tecnología emergente. Ya que de lo contrario siempre existiría la dependencia por parte del cliente del fabricante de hardware elegido en un primer momento. La existencia de interoperabilidad asegura una mayor competencia de mercado entre los fabricantes de RFID, lo que conlleva un mayor número de vendedores, costes más bajos, mejor calidad del producto, en definitiva un mercado más competitivo donde cada proveedor tiene que periódicamente mejorar sus productos para mantenerse o mejorar su situación.

Por último se debe mencionar el estándar para la identificación de productos en logística y en la cadena de suministro, el EPC ("Electronic Product Code"). Creado por "MIT Auto-ID Center", la compañía "Gillete", "Procter & Gamble", y otras. Basado en identificar cada objeto a través de una transponder con una "matricula" electrónica. El EPC consiste en la nueva generación de identificación de objetos, similar al UPC ("Universal Product Code") de los códigos de barras, los cuales serán en un futuro próximo sustituidos por los tags RFID, según la opinión de multitud de expertos. El EPC contiene como número de serie 96 bits, único e inmodificable.

## VI. APLICACIONES

A día de hoy, los campos de aplicación son muy variados, y durante los próximos años estos serán aún mayores. Los "transponders" de baja frecuencia, LF, se utilizan para la identificación de animales, seguimiento de barricas de cerveza, incorporadas en las llaves de los automóviles con sistema antirrobo, etc. También se suelen insertar en mascotas para evitar sus pérdidas. Los "tags" de HF se utilizan en bibliotecas y seguimientos de libros, seguimiento de pallets, en control de accesos a edificios, o seguimiento de artículos de ropa. Los "transponders" UHF se utilizan para seguimiento de pallets, camiones y remolques. Mientras que los "tags" de microondas se utilizan en el control de accesos en vehículos de gama alta.

Las principales aplicaciones por el momento son en el transporte público como sistema de pago, o como pases de acceso a zonas restringidas en sistemas de control de accesos. En las cuales se utilizan tarjetas inteligentes sin contacto. También está extendido utilizar tecnología RFID en el cobro de peajes en autopistas, con la cual se consigue reducir una tercera parte el tiempo empleado, con respecto a los métodos tradicionales de pago.

Otra aplicación típica se da en la identificación animal, utilizándose para el mantenimiento de ganado, o el rastreo del origen de los animales. Con dichos "transponders" se controlan las posibles epidemias y se asegura cierta calidad del género. Echo sumamente importante para la industria cárnica, cuyas perdidas pueden ser notables si no se palian epidemias como las surgidas en el Reino Unido ("La fiebre de las vacas locas").

Pero la verdadera aplicación que marcará el éxito de la tecnología se dará en logística y en la cadena de suministro. Ya que con la consolidación de estándares mundiales, surgirán grandes pedidos de "transponders" en masa. Y esto junto a los continuados avances tecnológicos, producirán un radical descenso en los precios de los tags. La implantación de la tecnología RFID mostrará una reducción entre el 3-5% en los costes de la cadena de suministro, y entre 2-7% de aumento en los ingresos debido a la visibilidad del inventario.

## VII. REFERENCIAS

- [1] **“RFID Handbook. Fundamentals and applications in contactless Smart Cards and Identification”**. Segunda edición. Klauss Finkenzeller. Wiley & Sons. Munich, 2003.
- [2] **“Fundamentos de compatibilidad electromagnética”**. José Luís Sebastián. Addison-Wesley.
- [3] **“Fundamentos de electromagnetismo para Ingenieros”**. David K. Cheng. Addison-Wesley. 1997.
- [4] **“Transmisión por radio”**. Jose María Hernando Rábanos. ETSI de Telecomunicación (UPM). Editorial Centro de Estudios Ramón Areces S.A. 1998.
- [5] **“Sistemas de Identificación y control”**. Juliá Monsó i Bustio. Marcombo. 1993.
- [6] **“Caja de medicinas empleando etiquetas RFID”**. Victor Antonio Pérez Laso. PFC. 2003

- [7] “**Aplicación MOBY usando sistema de RFID**”. David Domingo Gil. PFC. 2003.
- [8] “**Sistema Icode de Identificación por Radiofrecuencia**”. Manual del programa demo del RIDE500 de Softrónica, Ing. Electrónica Software y Comunicaciones.
- [9] “**Sistema Icode de Identificación por Radiofrecuencia**”. Manual de desarrollo y técnico Software RIDE5000 de Softrónica, Ing. Electrónica Software y Comunicaciones

Alejandro Díaz Hortelano  
Coordinador del Boletín Electrónico y miembro del IEEE  
[AdiazH@ieee.org](mailto:AdiazH@ieee.org)

# **SIMULACIÓN ELÉCTRICA DE UN HORNO DE ARCO DE C.A.**

## **1. INTRODUCCIÓN**

Actualmente existen en la red de distribución numerosas cargas que podríamos llamar polucionantes. Estas cargas son así denominadas debido a su efecto nocivo sobre la red eléctrica. Sin duda el ejemplo más característico de carga polucionante es el horno de arco eléctrico o EAF (*Electric Arc Furnace*), al cual se le atribuye fundamentalmente la producción de armónicos, desequilibrios y *flicker* o parpadeo.

Además de provocar estas perturbaciones eléctricas, el horno tiene otras características que lo convierten en un candidato idóneo para su estudio y simulación. Podemos destacar la aleatoriedad de su comportamiento, la gran potencia que consume y la dificultad de trabajar o ensayar en un entorno industrial de estas características.

La posibilidad de poder reproducir a escala de pequeña potencia en un laboratorio el comportamiento eléctrico de un horno de este tipo, abre un abanico de posibilidades en lo que se refiere a la investigación y desarrollo de equipos electrónicos de corrección de perturbaciones.

Esta reproducción o simulación además tiene una serie de ventajas importantes sobre un horno real, como puede ser la posibilidad de repetir el fenómeno todas las veces que sean necesarias, con o sin compensación electrónica, y disponer de esta forma de un banco de registros basados en un horno real sin la necesidad de hacer medidas en campo.

En este artículo se resume el trabajo realizado para un proyecto fin de carrera [20] consistente en el escalado de la instalación de un horno de arco, su posterior materialización y su uso final para la ejecución de ensayos reproduciendo el comportamiento eléctrico del horno.

Este proyecto ha sido desarrollado en el departamento de Ingeniería Eléctrica, Electrónica y de Control de la ETS de Ingenieros Industriales de la UNED bajo la dirección de Salvador Martínez García. El proyecto pertenece a una línea de investigación en la que se colabora con la Universidad de Oviedo, (Juan Carlos Campo) y con la Universidad Politécnica de Madrid (Julio García Mayordomo).

## **2. EL HORNO DE ARCO DE C.A.**

Desde su invención a mediados del siglo XIX hasta la época actual, el horno de arco ha sufrido una evolución paralela en incremento de potencia, uso e importancia como carga no lineal de la red.

Hasta la década de los sesenta del siglo XX, los hornos de arco sólo se empleaban en la fabricación de aceros de muy alta calidad, pero a partir de 1962 se desarrollaron los llamados hornos UHP (*Ultra High Power*). Con estos hornos se alcanzaron potencias de 165 MVA y capacidades de producción de 360 t, todo ello con unos rendimientos más que aceptables que propiciaron el desarrollo y extensión de estos hornos para la fabricación de más tipos de aceros. Actualmente la mayoría de los aceros se fabrican con este tipo de hornos.

Básicamente, un horno de arco eléctrico de corriente alterna consiste en una cuba fabricada en un material refractario, en la que se introduce la chatarra a fundir y tres electrodos (uno por fase) que suelen estar hechos de grafito y que se introducen en el baño provocando el establecimiento de arcos eléctricos de alta intensidad que funden la chatarra.

Los electrodos mencionados suelen estar conectados a unos cables flexibles y sujetos por los llamados portaelectrodos. Estos cables flexibles provienen del secundario de un transformador trifásico, que es probablemente el elemento más importante de la instalación.

Sobre este transformador hay que comentar que reduce el nivel de tensión de media (normalmente 30 kV) a baja tensión (1 kV), que su secundario siempre se conecta en triángulo para tratar de encerrar los armónicos triples y que dispone de un cambiador de tomas en el primario para adaptar la tensión del secundario al nivel adecuado en cada fase de la colada.

Una colada se puede componer de varias cestas, entendiendo por cesta cada una de las cargas de chatarra que se producen en la cuba del horno, siendo la colada el conjunto de todos los procesos desde que se realiza la primera carga hasta que se cuela el acero por las lingoteras.





**Figura 1.** Horno de arco de c.a. Se pueden apreciar en la parte superior de la imagen los electrodos que se introducen en la cuba, así como los portaelectrodos que los sujetan y los cables flexibles que provienen del secundario del transformador. Cortesía de DANIELI.

Dentro de una colada, y con objeto de caracterizar eléctricamente el horno, los expertos definen diferentes regiones de funcionamiento denominadas ventanas. Estas ventanas son periodos de tiempo correspondientes a 10 ciclos de red (200 ms) y han sido elegidas de esta duración con el fin de proporcionar una resolución de 5 Hz para la transformada de Fourier.

Cada una de estas ventanas corresponderá a una situación o modo de operación del horno en función de las perturbaciones medidas en esa ventana. Los criterios para realizar esta elección forman parte del trabajo del grupo de investigación del departamento de ingeniería eléctrica de la ETSII de la UPM.

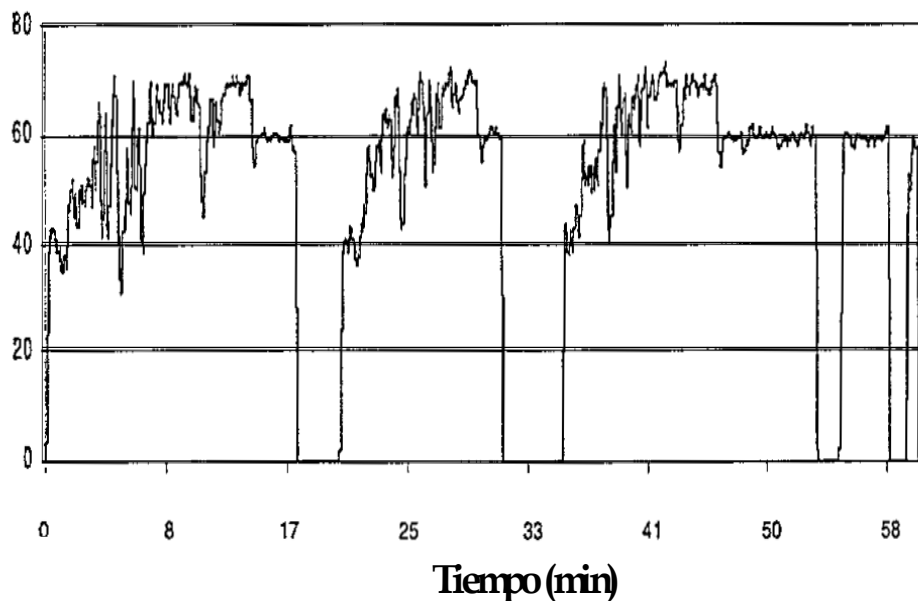
En el caso que nos ocupa fueron seleccionadas 4 ventanas, 2 de ellas correspondientes a la parte inicial de la colada de un horno (llamadas ventanas 1 y 2), otra en una fase intermedia (ventana 3) y una correspondiente a la fase final de la colada (ventana 4). Cada una de estas ventanas presenta unas características acordes al instante de la colada al que corresponden.

En las ventanas correspondientes a las fases iniciales se observa una elevada fluctuación de corriente en cada una de las fases del horno. La causa de estas fluctuaciones es que la chatarra está comenzando a fundir y hay numerosos huecos, lo que hace que los arcos que se establecen entre los electrodos y el baño sean muy desiguales. En estas ventanas aparecerán unos niveles muy elevados de perturbaciones.



En las ventanas de la parte final de la colada el baño es muy homogéneo, siendo muy pequeñas las variaciones de corriente en cada fase y apareciendo pocas perturbaciones. Todo esto lo podemos ver resumido en la figura 2, en la que se muestran los diferentes niveles de consumo de potencia activa durante la duración de una colada de 1 hora.

### P(MW) Consumo de potencia activa en una colada con tres cestas



**Figura 2.** Consumo de potencia activa en una colada con tres cestas. Se observa como en el instante inicial de cada carga del horno aparecen unas elevadas variaciones del consumo de potencia para posteriormente establecerse. Estas variaciones se producen debido a las elevadas fluctuaciones de corriente y de tensión y nos indican el nivel de perturbaciones en cada fase de la colada.

Ya se ha mencionado al comienzo del artículo cuales son las perturbaciones que se atribuyen a estos hornos. Vamos a explicar brevemente en que consisten.

- *Armónicos e interarmónicos:* Los armónicos son componentes de frecuencia múltiplo de la de red que provocan una deformación de la onda de tensión o de corriente alejándola de su carácter idealmente senoidal.

Los interarmónicos son un caso particular en el que la frecuencia de estas componentes es inferior a la frecuencia de la red. En el caso de hornos de arco se consideran de gran importancia los múltiplos de 5 Hz

- *Desequilibrios:* Los desequilibrios consisten en la aparición de asimetrías en un sistema trifásico. Esto puede ser debido a la existencia de cargas desequilibradas como es el caso del horno y

provoca que tanto los ángulos de desplazamiento entre fases, así como las amplitudes de cada una de las fases sean diferentes.

- *Flicker o parpadeo*: Consiste en la variación de baja frecuencia (1 a 10 Hz.) de la envolvente de la onda de tensión. Este fenómeno se denomina así debido a que se suele manifestar como un parpadeo en las lámparas de incandescencia.

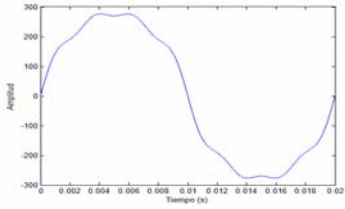
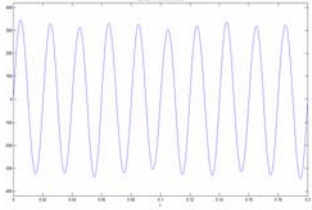
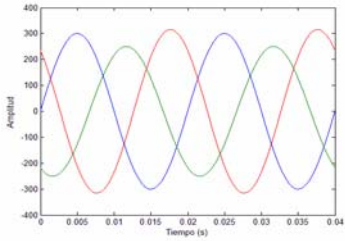
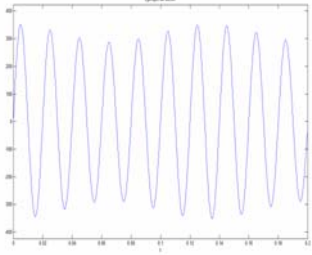
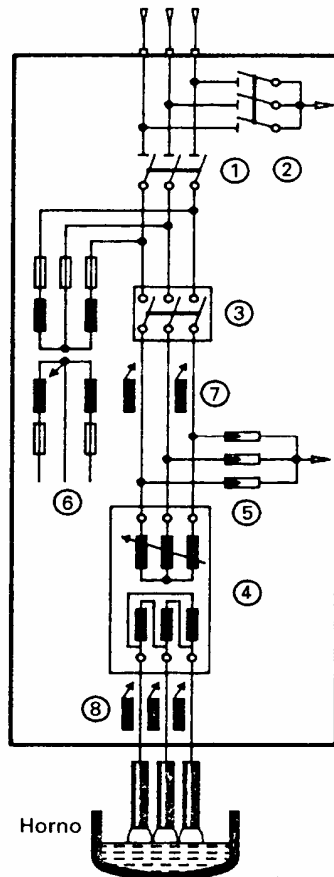
Perturbación	Ejemplo	Caracterización EN 50160
Armónicos		<ul style="list-style-type: none"> <li>El THD ha de ser inferior en todo momento al 8%, además de otras restricciones detalladas en la norma.</li> </ul> $THD = \sqrt{\frac{\sum_{h=2}^{40} (U_h)^2}{U_1^2}}$
Interarmónicos		<ul style="list-style-type: none"> <li>No hay estudios suficientes del tema como para que se incluyan límites en la citada norma.</li> <li>La banda entre 35 y 85 Hz se considera de especial relevancia para la aparición de flicker.</li> </ul>
Desequilibrios		<ul style="list-style-type: none"> <li>Durante el periodo de una semana, el 95% de los valores eficaces promediados en 10 min de la componente inversa de tensión debe ser inferior al 2% de la componente directa.</li> </ul>
Flicker		Se definen dos términos: <ul style="list-style-type: none"> <li>Severidad de corta duración, <math>P_{st}</math> medida en periodos de 10 min con un medidor de flicker.</li> <li>Severidad de larga duración, <math>P_{lt}</math>, calculada a partir de una secuencia de 12 valores de <math>P_{st}</math> según la siguiente ecuación:</li> </ul> $P_{lt} = \sqrt[3]{\sum_{i=1}^{12} \frac{P_{st}^3}{12}}$

Tabla 1. Ejemplos y caracterización según la norma EN UNE 50160 de algunas perturbaciones.

### 3. DESCRIPCIÓN DE LA INSTALACIÓN Y REALIZACIÓN DE LOS ENSAYOS

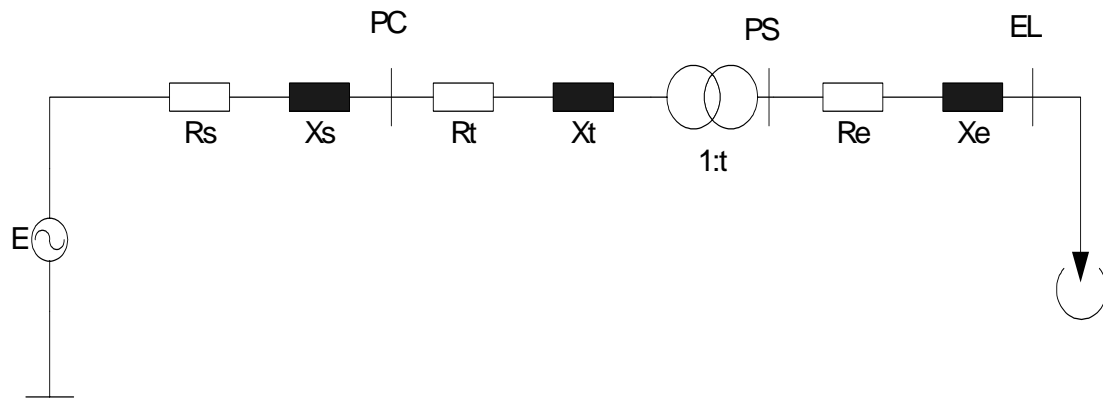
La instalación que se utilizó para la ejecución de los ensayos está basada en la de un horno real. En la figura 3 se pueden ver los componentes típicos de la subestación de un horno de arco de c.a.



1. Seccionador de entrada de la instalación.
2. Seccionador de puesta a tierra de la instalación.
3. Interruptor general.
4. Transformador del horno.
5. Pararrayos.
6. Transformadores de medida de media tensión.
7. Transformadores de medida de intensidad.
8. Transformadores de medida de baja tensión.

**Figura 3.** Esquema típico de la subestación de un horno de arco conectado a un nudo de M.T. Los elementos 1, 2, 3 y 5 constituyen los elementos de protección y maniobra de la instalación. Los elementos 6, 7 y 8 son empleados por el equipo de control del horno para monitorizar las corrientes y tensiones del mismo. El transformador principal (4) está conectado en estrella-triángulo con un cambiador de tomas en el primario.

A continuación se muestra el esquema unifilar equivalente del horno real que fue tomado como punto de partida para el modelado de la instalación.

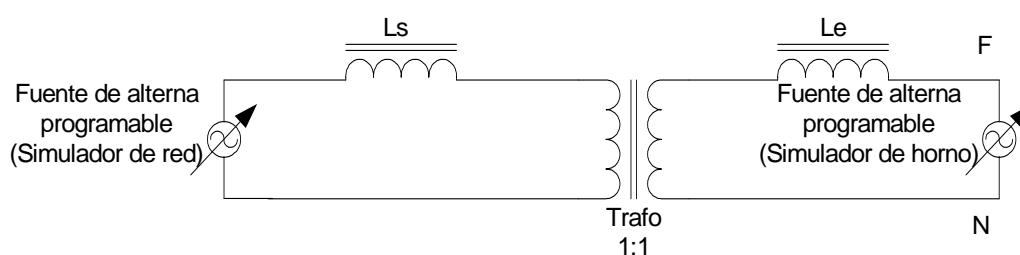


**Figura 4.** Esquema unifilar de la instalación a estudio. E, Rs y Xs representan el equivalente Thévenin de la red aguas arriba del punto de conexión común (PC). Rt y Xt representan la impedancia de cortocircuito del transformador de tomas (representadas por t). Re y Xe representan la impedancia de los cables flexibles y de los electrodos que se introducen en el baño.

A partir de datos proporcionados por REE (Red Eléctrica de España) al DIE de la UPM se estimaron los parámetros del esquema unifilar de la figura 4, los cuales fueron escalados desde sus condiciones nominales ( $S=100$  MVA,  $U_{PC}=30$  kV,  $U_{EL}=1$  kV) a unas condiciones manejables en laboratorio ( $S=1$  kVA,  $U=178$  V).

La instalación escalada para el laboratorio reproduce los elementos de la instalación original mediante el uso de una pareja de bobinas, un trafo y 2 fuentes de alterna programables.

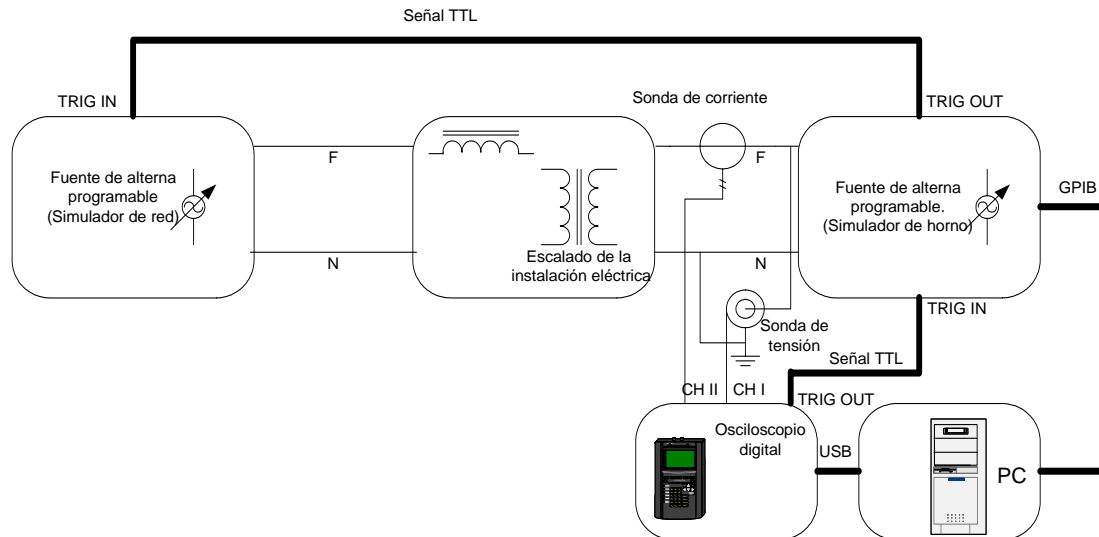
El esquema eléctrico de la instalación del laboratorio es el indicado en la figura 5. La bobina  $L_s$  modeliza la impedancia de cortocircuito de la red, el transformador monofásico hace lo propio con el trafo real de la instalación y finalmente la bobina  $L_e$  simulará la impedancia de los electrodos.



**Figura 5.** Esquema simplificado del circuito eléctrico empleado para ensayar. Dicho circuito consiste básicamente en dos fuentes de tensión programables, dos bobinas de núcleo de hierro con tomas para poder variar la inductancia según sea necesario y un transformador.

En este esquema vemos como hay una pareja de fuentes de tensión, una de ellas (la del primario del transformador) simula el comportamiento de la red ideal, mientras que la otra se comporta como carga (simulando el comportamiento del horno). Además se puede apreciar que se ha prescindido de las resistencias que aparecían en el esquema original, ya que al ser de pequeño valor podían ser modeladas por la propia resistencia serie de las bobinas.

En el esquema anterior solo están los elementos de la instalación eléctrica, pero obviamente hay otros elementos imprescindibles, tanto de medida como de control, sin los cuales resultaría imposible realizar los ensayos. En la figura 6 podemos ver un esquema completo con todos los elementos necesarios para ejecutar los ensayos, así como el modo en el que se conectan e interactúan entre si.



**Figura 6.** Esquema completo del sistema. Se incluyen la instalación eléctrica, los elementos de medida y control, y la forma de interconectar los diferentes equipos tanto para su programación, como para su sincronización.

Tal y como se indica en la figura, se midieron la tensión en bornes del simulador de horno y la corriente absorbida por este. Esta corriente es el dato fundamental a estudiar, ya que será la forma de comparar nuestros resultados con las mediciones reales del horno.

El PC indicado en el esquema desempeña una doble tarea. Por un lado hace funciones de control, enviando comandos *SCPI (Standard Commands for Programmable Instruments)* tanto a la fuente programable que simula el horno, como al osciloscopio. Por otro lado se emplea para descargar los registros obtenidos de los ensayos y su posterior tratamiento matemático.

## 4. RESULTADOS EXPERIMENTALES

De todos los ensayos que se realizaron, 15 fueron completamente caracterizados y sometidos a estudio.

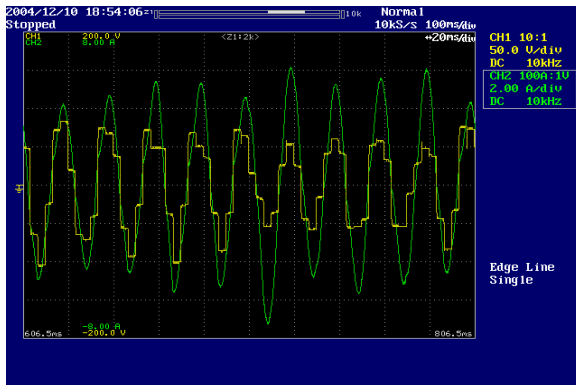
En concreto se adoptaron dos criterios para comparar los resultados, el dominio del tiempo y el de la frecuencia.

El estudio en el dominio del tiempo se basa en la comparación de la corriente medida en nuestro ensayo con la que se midió en el horno objeto de la reproducción. Esta comparación fue realizada tras la adecuada normalización de ambos registros de corriente (real y simulado) basándonos

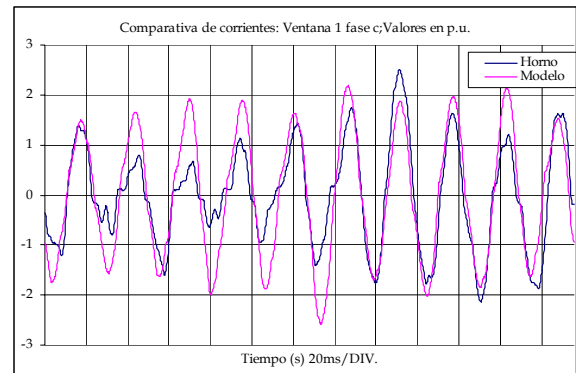
para ello en los valores nominales de cada una de las instalaciones y calculando la corriente por unidad (normalizada) en cada caso. De esta forma podemos comparar las corrientes de kiloamperios del horno con las de unos pocos amperios manejadas en el laboratorio.

El estudio o comparación en el dominio de la frecuencia consiste en el cálculo y normalización de las componentes armónicas e interarmónicas de ambos registros (real y simulado). Para la normalización en este caso se tomará como base la amplitud de la componente de 50 Hz y se realizarán 2 comparaciones, la primera tendrá como objeto los armónicos de corriente múltiplos del fundamental hasta el undécimo (550 Hz) y la segunda se ocupará del estudio de los interarmónicos, restringiendo el rango de estudio en las frecuencias entre 35 y 85 Hz.

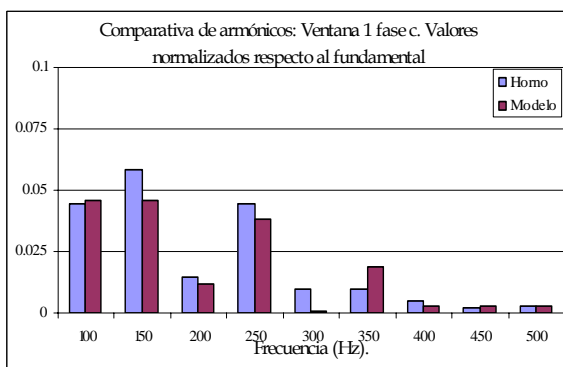
El modo de operación descrito se repitió en todos los ensayos realizados. En este artículo como casos ejemplares vamos a mostrar las formas de onda de los ensayos y las comparaciones de una fase de la ventana 1 y de la ventana 4.



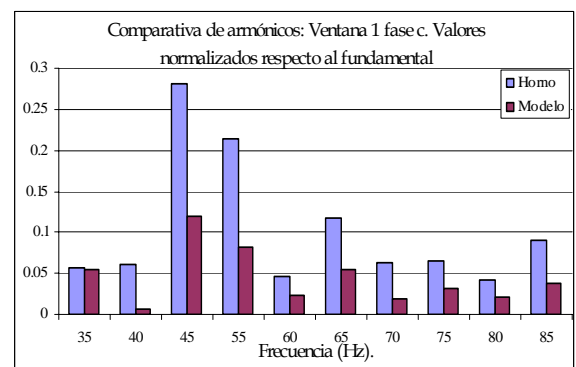
(a)



(b)

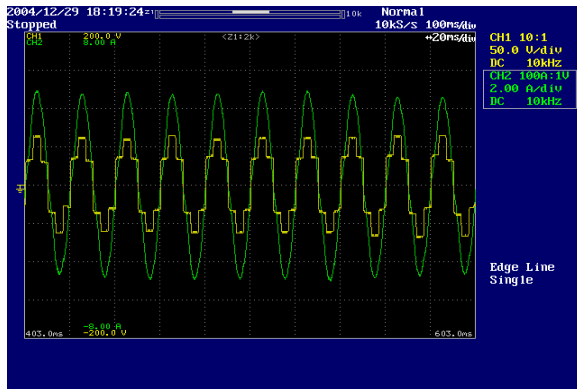


(c)

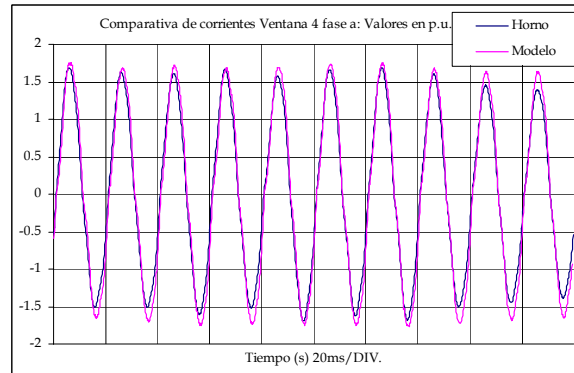


(d)

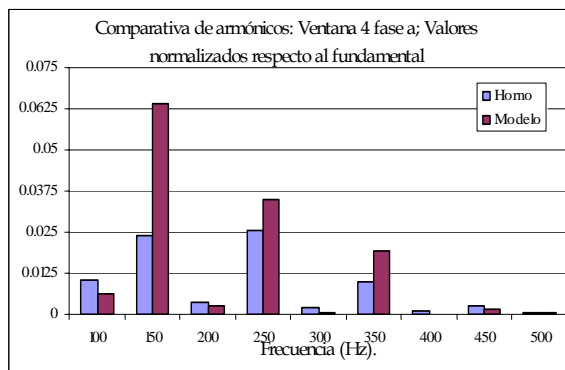
**Figura 7.** Ventana 1. (a) Formas de onda del ensayo. (b) Comparación de las corrientes real del horno y simulada en laboratorio. (c), (d) Comparación de armónicos e interarmónicos respectivamente.



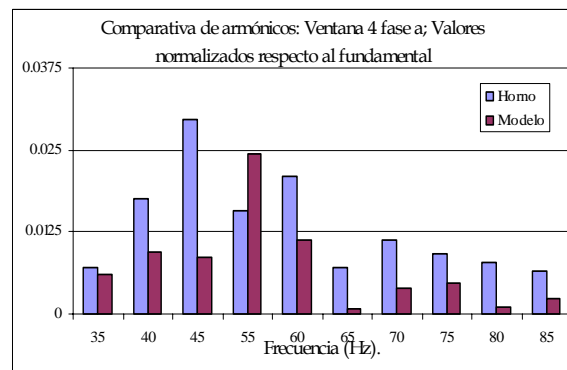
(a)



(b)



(c)



(d)

**Figura 8.** Ventana 4. (a) Formas de onda del ensayo. (b) Comparación de las corrientes real del horno y simulada en laboratorio. (c), (d) Comparación de armónicos e interarmónicos respectivamente.

## 5. CONCLUSIONES

Un simple vistazo a las gráficas de las figuras 7 y 8, nos muestran que el modelo es capaz de reproducir de forma más que aceptable el comportamiento del horno.

La comparación en el dominio del tiempo (figuras 7 y 8 (b)), nos muestra que en ventanas con pocas fluctuaciones el modelo no tiene dificultad para reproducir la corriente del horno. Sin embargo en una ventana con un alto nivel de variación de corriente como es la ventana 1, el modelo muestra un comportamiento menos fiable desde el punto de vista del dominio del tiempo.

En cuanto al dominio de la frecuencia, vemos que nuestro modelo, al igual que el horno, genera armónicos e interarmónicos con una desviación en torno al 30%. Estas desviaciones se pueden achacar tanto a errores de modelado como a los propios de ejecución de los ensayos y de medida. Para dar más señas, el fabricante de la sonda de corriente especifica un error del 5%.



Los resultados experimentales mostrados confirman la viabilidad del procedimiento empleado para simular en el dominio del tiempo. Además debemos tener en cuenta que en este proyecto se ha abordado la simulación en una primera aproximación, para comprobar la bondad del método y posteriormente depurarlo.

Esta simulación o reproducción del horno, nos permitirá experimentar con correctores electrónicos de flicker escalados en pequeña potencia. A partir de los resultados de esos experimentos se podrán comparar diferentes topologías y estrategias de control para posteriormente diseñar equipos de gran potencia con las garantías necesarias.

Por último cabe destacar que se siguen estudiando las posibles mejoras de estas simulaciones, y que dichas mejoras pretenden ser puestas en práctica en virtud de la solicitud de una ayuda para el desarrollo de un proyecto CICYT al Ministerio de Ciencia y Tecnología que incluirá los citados estudios.

## **6. BIBLIOGRAFÍA**

- [1] Akdag, Alper y otros. "Effects of main transformer replacement in the performance of an electric arc furnace system". *IEEE Transactions on Industry Applications*. Marzo 2000.
- [2] Astigarraga Urquiza, Julio: *Hornos de arco para fusión de acero*. McGraw Hill 1995.
- [3] Barrero, Fermín. "Sistemas de energía eléctrica". Thomson 2004.
- [4] Collantes Bellido, Rafael. "Modelos de perturbaciones inyectadas por hornos de arco en la red de suministro y métodos para su compensación". Tesis Doctoral. Universidad Pontificia de Comillas ICAI 1999. Director de tesis: J. A. García Cerrada.
- [5] Fernández Beites, L y otros. "Harmonics, interharmonics and unbalances of arc furnaces: A new frequency domain approach". *IEEE Transactions on Power Delivery*. Octubre 2001.
- [6] Fernández Beites, Luis. "Modelado en el dominio de la frecuencia de hornos de arco de corriente alterna para la estimación de armónicos, flicker y desequilibrios". Tesis Doctoral. Universidad Politécnica de Madrid 1999. Director de tesis Julio García Mayordomo.
- [7] Fran, Joan. "Sistemas de análisis y gestión de redes eléctricas". *Automática e instrumentación*. Septiembre 2001.
- [8] García Cerrada, J.A y otros. "Comparison of thyristor controlled reactors and voltage source inverters for compensation of flicker"

- caused by arc furnaces". *IEEE Transactions on Power Delivery*. Octubre 2000.
- [9] García Mayordomo, Julio y otros. "A new frequency domain arc furnace model for iterative harmonic analysis". *IEEE Transactions on Power Delivery*. Octubre 1997.
- [10] García Mayordomo, Julio. "A unified theory of uncontrolled rectifiers, discharge lamps and arc furnaces. Part II: Analog model for educational purposes". *ICHQP'98*.
- [11] Hernández Bayo, Araceli. "Medida y evaluación en el dominio de la frecuencia del flicker producido por hornos de arco y análisis de su propagación en la red". Tesis Doctoral. Universidad Politécnica de Madrid 2000. Director de tesis: Julio García Mayordomo.
- [12] Hernández Bayo, Araceli. "A new frequency domain approach for flicker evaluation of arc furnaces". *IEEE Transactions on Power Delivery*. Abril 2003.
- [13] Hewlett Packard. "HP Series 6800: AC Power Source/Analyzers Programming Guide".
- [14] Hewlett Packard. "HP Series 6800: AC Power Source/Analyzers User's Guide".
- [15] Martínez García, Salvador. "Alimentación de equipos informáticos y otras cargas críticas". McGraw Hill 1997.
- [16] Martínez García, Salvador. "Electrónica industrial: Técnicas de potencia". Marcombo 1992.
- [17] Martínez García, Salvador. "Prontuario para el diseño eléctrico y electrónico". Marcombo 1989.
- [18] Martínez García, Salvador. "Estabilizador de C.A. por pasos con intensidad compartida". *Mundo electrónico* nº166. 1986.
- [19] Martínez García, Salvador. "Estabilizadores de C.A. de tomas e intensidad de corriente limitada". 1º Congreso internacional de electrónica de potencia. CIEP'92-Cenidet.
- [20] Molina Casla, José Luis. "Simulación eléctrica de un horno de arco de C.A." Proyecto fin de carrera. UNED 2005. Director de proyecto: Salvador Martínez García.
- [21] Morcos M.M y Gómez J.C. "Flicker sources and mitigation". *IEEE Power Engineering Review*. Noviembre 2002.
- [22] Rogóz, Marek. "The IEC flickermeter model" AGH University of Science and Technology. AGH-UST Marzo 2003.

- [23] *Tung Xin Zheng y otros. "An adaptive arc furnace model". IEEE Transactions on Power Delivery. Julio 2000.*
- [24] *Wierda, Reno. "Flicker o parpadeo de las fuentes luminosas" Cuaderno Técnico nº176. Schneider Electric.*
- [25] *Wolf Albrech y Thanodharan Manoharan. "Reactive power reduction in three phase electric arc furnaces". IEEE Transactions on Industrial Electronics. Agosto 2000.*

José Luis Molina Casla.

[jlmolina@ieec.uned.es](mailto:jlmolina@ieec.uned.es)

## **Refrigeración de alternadores con hidrógeno producido mediante electrolizadores tipo PEM (Electrolizadores de Membrana Polimérica)**

### El aire y el hidrógeno como refrigerantes en los alternadores

Los alternadores durante su operación producen una gran cantidad de calor originado por dos causas:

- El efecto Joule debido a las altas corrientes que circulan por los arrollamientos del mismo.
- Las pérdidas por rozamiento con el aire (conocidas por su término inglés como “windage loss”) que se producen cuando el rotor, que gira a altas velocidades, debe vencer la resistencia de la atmósfera que existe en el interior del alternador.

Es necesario, por tanto, proporcionar un método efectivo para eliminar todo este calor, de tal forma que no se someta a los distintos componentes a un esfuerzo térmico excesivo, a la vez que se intentan minimizar las pérdidas por el rozamiento entre el rotor y el refrigerante usado para transmitir el calor. Estas premisas reducen el abanico de opciones a los dos gases que se han usado tradicionalmente: aire e hidrógeno.

El hidrógeno presenta mejores propiedades refrigerantes que el aire por los siguientes motivos:

- Por una parte ofrece una conductividad térmica 7 veces mayor que el aire, permitiendo una eliminación eficaz del calor producido y un menor tamaño del alternador.
- Por otra parte presenta una menor fricción (su densidad es el 7% de la del aire) que redunda en una operación más eficiente del generador al reducir las “windage loss” (siempre que la pureza del hidrógeno se mantenga por encima del 90%). La eficiencia de un alternador por este concepto puede llegar a aumentar en un 0,2%.
- Además, el diseño necesario para el uso del hidrógeno como refrigerante proporciona a su vez protección intrínseca contra la humedad y la polución (aceite o polvo) que pudieran entrar en el interior del alternador produciendo fallos en el mismo.

Sin embargo, su uso no está exento de desventajas que deben ser tenidas en cuenta:

- El encapsulado de la máquina refrigerada con hidrógeno debe ser a prueba de explosiones (Esto incrementa el coste, ya que la ingeniería es más compleja y el diseño de la planta requiere precauciones contra el riesgo de incendio o explosión por hidrógeno)
- Es necesario instalar equipos auxiliares que permitan asegurar el correcto sellado de la máquina en los extremos del eje y proporcionen

una distribución efectiva del hidrógeno, una correcta presión del mismo y una monitorización de su pureza.

- Es necesario rellenar y presurizar el alternador cada cierto tiempo (aproximadamente un año), requiriendo esta operación de procedimientos de llenado y purga que necesitan de personal cualificado.
- Es necesario disponer de grandes cantidades de CO<sub>2</sub> y aire comprimido para las operaciones de llenado y purga (estas operaciones se realizan cada 3,4 o incluso 5 años), con sus sistemas asociados, en muchas ocasiones duplicados para evitar la mezcla con el hidrógeno.

La elección del hidrógeno viene determinada por la influencia de estas ventajas e inconvenientes en la operación del alternador. Para generadores grandes (por encima de 300 MVA) el aumento de eficiencia es un factor decisivo que compensa generalmente la complejidad inherente a la refrigeración con este gas, mientras que para alternadores entre 80 y 300 MVA la decisión ya no es tan clara y existe margen para uno y otro sistema en función de las características de la central.

### Suministro de hidrógeno en las centrales

Si la elección para la refrigeración del alternador ha sido el hidrógeno, es necesario asegurarse el suministro del mismo, no sólo para el llenado inicial sino para la operación diaria de la planta. Esta necesidad de suministro diario, se debe a que los alternadores necesitan mantener un determinado nivel de presión de hidrógeno (típicamente entre 40 y 80 psi) siendo necesario reponer las pérdidas que se producen a través de las juntas del eje debidas a esta sobrepresión.

Asimismo, siempre que se realice una parada de la central para mantenimiento (normalmente se programa una cada año), es necesario vaciar el alternador de hidrógeno para prevenir que una posible mezcla con aire forme una atmósfera explosiva. (Esta operación de vaciado/llenado para el mantenimiento, consume además grandes cantidades de CO<sub>2</sub>).

La forma más habitual para obtener el hidrógeno necesario para la operación de la central es mediante su abastecimiento en tanques y botellas suministrado por parte de una empresa gasista. Sin embargo, la producción de hidrógeno "in situ" puede, con la tecnología actual, sustituir fácilmente al suministro externo de hidrógeno. Esta sustitución acarrea las siguientes ventajas:

- Ofrece costes competitivos del hidrógeno con retornos de inversión inferiores a dos años en algunos casos.
- Mejora la pureza del hidrógeno en el interior del alternador, reduciéndose las pérdidas por rozamiento del rotor.
- Asegura la fiabilidad del suministro de hidrógeno, proporcionando una ventaja operativa a la planta al disminuir la dependencia exterior de un suministro necesario para la operación de la misma.

- Mejora la seguridad de la planta, reduciendo los stocks de hidrógeno y reduciendo la necesidad de la operación de los tanques de hidrógeno. Además se eliminan los posibles riesgos asociados al suministro y transporte del gas hasta la planta.
- Reduce los costes asociados al hidrógeno al disminuir la necesidad de personal para su operación y eliminar el inventario de botellas y los costes asociados a su mantenimiento. Estos costes pueden, en algunos casos llegar a triplicar los costes del hidrógeno.
- Evita las fluctuaciones de presión en el alternador al poder estar conectado el sistema de generación a la línea de alimentación de hidrógeno.

Además la generación in situ de hidrógeno puede llegar a ser muy beneficiosa en centrales localizadas en áreas remotas o poco desarrolladas, con insuficiente infraestructura para el suministro de hidrógeno. Paradójicamente alguna de estas situaciones también pueden producirse en centrales situadas en zonas densamente pobladas que pueden tener limitaciones respecto al transporte de gases inflamables, limitaciones que van desde restricciones al tráfico, hasta requisitos más estrictos en el almacenamiento por motivos de seguridad.

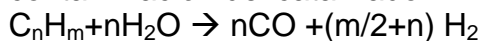
### Sistemas de generación de hidrógeno “in situ”

El hidrógeno es el elemento más abundante de la naturaleza, pero no existe en ella en estado puro, siendo necesario por tanto “fabricarlo” a partir de hidrocarburos (mediante su reformado, oxidación parcial o pirolisis), o a partir del agua mediante su electrolisis.

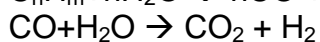
### Reformado de hidrocarburos

Con el reformado de hidrocarburos se rompen los enlaces del hidrógeno y el carbono en determinadas condiciones de presión y temperatura y en presencia de agua, para posteriormente generar hidrógeno y CO<sub>2</sub>. Existen dos métodos para la generación de hidrógeno mediante reformado: el reformado con vapor de agua y el reformado autotérmico.

El reformado con vapor de agua es una tecnología madura y usada en la industria para la producción a gran escala de hidrógeno. Las reacciones de reformado se producen normalmente sobre un catalizador de níquel a temperaturas típicamente por encima de los 500 °C. Para mejorar la pureza del hidrógeno es necesario aplicar al gas resultante (con un alto contenido en CO) reacciones de desplazamiento de agua-gas y en último término reacciones de oxidación preferencial o filtros basados en PSA (membranas). Además hay que tener en cuenta que si el hidrocarburo contiene azufre como en el caso del gas natural, es necesario realizar una desulfuración previa para evitar la contaminación del catalizador.



Reacción de reformado (oxigenolisis)



Reacción de desplazamiento de agua-gas.

## Electrolisis del agua

La electrolisis es un proceso por el cual se produce oxígeno e hidrógeno a partir de la ruptura de la molécula de agua mediante una corriente eléctrica que rompe el enlace químico proporcionando dos iones.

La electrolisis es el método preferido en las centrales, debido a la disponibilidad de electricidad, a la posibilidad de modular la producción en función de la demanda de forma sencilla, a la capacidad de producir el hidrógeno a la presión necesaria en la central (alrededor de 4 bares) sin necesidad de compresor y a la baja temperatura de trabajo que permite arranques rápidos del sistema de producción de hidrógeno.

El proceso de electrolisis se lleva a cabo en equipos denominados electrolizadores, o cubas electrolíticas. Estas cubas están compuestas por dos electrodos (cátodo y ánodo), encargados de suministrar la energía eléctrica, necesaria para la ruptura de la molécula de agua, separados por un electrolito (líquido o sólido), en el seno del cual se producirá la reacción de disociación. El empleo de electrolitos se hace necesario para vencer la resistencia eléctrica del agua (100 Ohm/cm, para agua pura).

Los electrolitos más utilizados son ácidos ( $\text{H}_2\text{SO}_4$ ), bases (NaOH), y sales (NaCl), los cuales favorecen el movimiento eléctrico de los electrones en el seno del recipiente de reacción.

De forma alternativa, o como apoyo al empleo de electrolitos, la elevación de la temperatura del agua en el interior de la cuba electrolítica (700-1000°C), disminuirá la resistencia eléctrica del agua.

Son dos los principales tipos de electrolizadores utilizados: los electrolizadores de tipo alcalino, de tecnología más madura y los de membrana polimérica (en adelante PEM), que iniciaron su desarrollo con las misiones espaciales y que alcanzaron la madurez tecnológica cuando se usaron en los submarinos, en este caso, para producir oxígeno. Ambos se diferencian en el tipo de electrolito que utilizan: en los electrolizadores alcalinos el electrolito es una disolución acuosa de hidróxido potásico, y un polímero sólido para los de tipo PEM, (Figura 1).

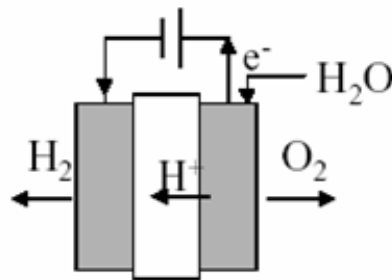


Figura 1. Esquema de la reacción de electrolisis en un electrolizador tipo PEM.

También existen diferencias en el tipo de membrana separadoras de gases que utilizan uno y otro tipo de electrolizadores. En el caso de los electrolizadores alcalinos utilizan membranas de amianto más o menos evolucionadas, pero en los de tipo PEM la membrana de tipo polimérico hace las veces de separador y de electrolito, participando de forma activa en el proceso de disociación de la molécula de agua.



Los electrolizadores con membrana polimérica presentan varias ventajas respecto a los basados en electrolitos alcalinos (KOH principalmente).

- El uso de membranas de naturaleza polimérica, evita la utilización de disoluciones líquidas de naturaleza cáustica, eliminando de este modo los problemas de seguridad que comporta la preparación y manipulación de este tipo de preparados, altamente corrosivos. Debido a su naturaleza corrosiva las disoluciones de KOH utilizadas como electrolitos atacan a los materiales de construcción de los electrolizadores, disminuyendo la vida útil de estos. Además el uso de electrolitos líquidos hace necesario el uso de una bomba de recirculación del electrolito, aumentando el número de componentes mecánicos del sistema.
- Físicamente los electrolizadores de membrana polimérica tienen una disposición similar a la de los electrolizadores alcalinos. Sin embargo su peso y tamaño son mucho menores (menos de la mitad en algunos casos) debido a que el electrolito es un polímero de espesor similar al de un folio de papel.
- Los sistemas de purificación del hidrógeno producido en un electrolizador tipo PEM consisten básicamente en equipos de deshumidificación de la corriente de gas, consiguiéndose purezas del orden de 99,999% mientras que los electrolizadores alcalinos necesitan también equipos que eliminen el oxígeno que inevitablemente, aunque en pequeñas cantidades, se produce en los cátodos.
- El mantenimiento de los electrolizadores PEM se limita al cambio de filtros anual (no siendo necesario realizar medidas gravimétricas diarias) y al cambio del “stack” una vez cada cinco años (el conjunto Ánodo-Membrana-Cátodo se denomina MEA. La asociación en serie de las MEAs mediante placas bipolares que sirven de conexión entre las mismas se denomina “stack”). En la actualidad este cambio debe ser realizado por personal cualificado.
- Los electrolizadores tipo PEM tienen una instalación sencilla y no modifican la clasificación del lugar donde son instalados, ni precisan de la elaboración de un proyecto.

### Análisis económico del uso de electrolizadores tipo PEM en las centrales

Las necesidades de hidrógeno de una central se deben tal y como ya se ha comentado a dos factores:

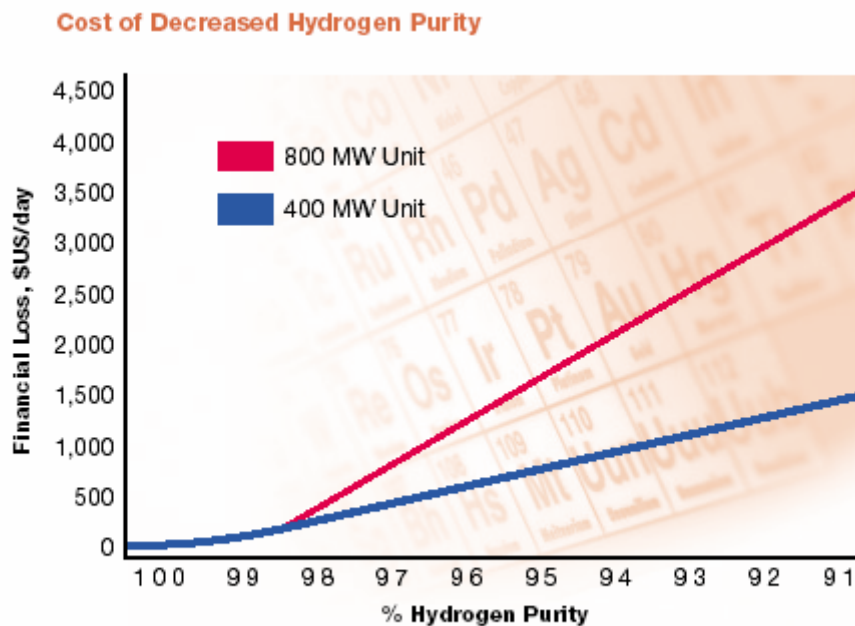
- La reposición de las pérdidas de hidrógeno a través de las juntas del alternador. Típicamente estas pérdidas son del orden de  $1\text{Nm}^3$  de  $\text{H}_2$  para los grupos de 400 MW.
- El llenado anual del circuito de refrigeración cuando se realiza el mantenimiento del alternador. En este caso es necesario disponer de una gran cantidad de metros cúbicos normales almacenados en recipientes en el exterior de la central.

La generación in situ puede abordar ambas necesidades, aunque el llenado anual obliga a disponer de un gran almacenamiento de hidrógeno en los terrenos de la central y a sobredimensionar el equipo de generación de hidrógeno local, para que pueda generar todo el hidrógeno del circuito de refrigeración en un corto periodo de tiempo (no más de 15 días típicamente). Existen ejemplos de este tipo, pero suele resultar más interesante dejar el cometido de la recarga anual al gasista que habitualmente suministra el hidrógeno a la central, dejando para el equipo de generación “in situ” la responsabilidad de reponer las pérdidas diarias.

### Efectos de la pureza del hidrógeno sobre la eficiencia del generador

La eficiencia en la refrigeración de un alternador con hidrógeno, está directamente vinculada a la pureza del mismo en su interior, por eso es tan importante la monitorización de la misma y el recambio del hidrógeno en el alternador si esta no alcanza los niveles adecuados.

Según un estudio realizado por ABB (uno de los suministradores de los sensores de pureza del hidrógeno), las pérdidas pueden alcanzar hasta los 3.500 \$/día para unidades de 800 MW si la pureza del hidrógeno cae por debajo del 90%, (Figura 2).



*Data based on typical power station operating conditions.*

**Figura 2. Costes de la disminución de la pureza del hidrógeno. Fuente *Hydrogen Analyzer systems ABB*.**

La pureza del hidrógeno en el interior está directamente relacionada con la pureza del hidrógeno suministrado. El suministro en botellas del hidrógeno con pureza 99,5% suele dar lugar a concentraciones del gas en el alternador del orden del 97%, mientras que la generación “in situ”, con electrolizadores tipo PEM, produce hidrógeno de gran pureza (99,999%) incrementándose la concentración en el alternador hasta el 99,5%.

## Referencias

- ABB, "Hydrogen analyzer System", <http://www.abb.com/>, 2004.
- Ayoub M. Kazim "Exergetic efficiency of a PEM electrolyser at various operating temperatures". Int. J. Exergy, Vol. 1, No. 1, 2004.
- Electric Energy On-Line, News, <http://www.elecricenergyonline.com/>, 2004.
- EPRI CT Center, <http://www.eprictcenter.com/>, 2004.
- Larminie, J. Dicks A. "Fuel Cell System Explained". Wiley New York, 2003.
- Peavy M.A. "Fuel From Water". Merit Inc Louisville, 1998.
- Sensidyne, Inc, "New gas sensors simplify power plant leak detection", <http://www.sensidyne.com/>, 2005.

Agustín Delgado  
Estudiante de Doctorado – UNED  
[adelgado@besel.es](mailto:adelgado@besel.es)

## MICROSOFT

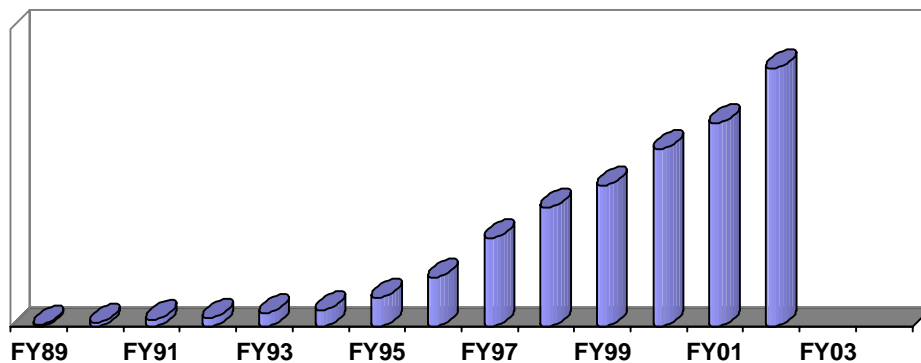
### Información sobre la empresa

Microsoft es líder mundial de software para informática personal y de empresas, la compañía ofrece un amplio abanico de productos y servicios diseñados para contribuir al desarrollo del talento de las personas y al potencial de las empresas aumentando su eficacia, productividad y capacidad competitiva.

Desde sus comienzos en 1975, la misión de Microsoft ha sido crear software para usuarios y empresas, con el fin de facilitar el acceso y el uso de la información en cualquier momento, desde cualquier lugar y a través de cualquier dispositivo.

Como líder mundial fabricante de software, Microsoft invierte 6.800 millones de dólares en I+D, y se esfuerza en crear productos y soluciones innovadoras que satisfagan las cada vez mayores y más complejas necesidades de los consumidores. Ello, unido a su fuerte compromiso de atención al cliente, permite a la compañía ofrecer avances tecnológicos que aseguran productos de software de la mayor calidad.

Microsoft se estableció en España en diciembre de 1987. Desde entonces, la subsidiaria ha evolucionado rápidamente, en facturación y en número de empleados.



Evolución de la facturación de Microsoft Ibérica

### Productividad

Microsoft desarrolla productos y soluciones que aportan valor a las empresas y a los usuarios, tanto en sus inversiones y en su negocio, como en sus proyectos personales. El software de Microsoft facilita:

- A las empresas, soluciones tecnológicas que les ayudan a incrementar su productividad, a ser más rentables y a obtener un rápido retorno de sus inversiones.
- A los profesionales, herramientas para realizar su trabajo de manera más rápida y eficaz, mejorando sus procesos y su capacidad para llevar a cabo sus ideas.
- A los usuarios en general, una experiencia de uso satisfactoria y una mayor calidad y posibilidades a la hora de disfrutar de su tiempo de ocio.

### **Ciudadano responsable**

El negocio de Microsoft está construido sobre las relaciones que la compañía mantiene con sus clientes, partners, inversores, empleados y demás miembros de la comunidad que nos rodea.

Comprometidos con estrechar su relación con los ciudadanos, Microsoft muestra de forma abierta sus prácticas de negocio, siendo transparentes en cuanto a sus actuaciones y manteniendo una conducta responsable.

### **Community Affairs**

Microsoft tiene como compromiso combatir el desfase entre las personas y colectivos que tienen fácil acceso a las tecnologías de la información y aquellos que no lo tienen. Por ello desarrolla una serie de programas en colaboración con empresas, instituciones y ONGs dirigidos a potenciar el uso de las nuevas tecnologías en los sectores más desfavorecidos, a fin de que puedan beneficiarse de ellas y aprovecharlas como un factor de integración social.

La compañía entiende que, proporcionando formación y herramientas, es posible ayudar a crear oportunidades sociales y económicas que transformen las comunidades y ayuden a la gente a desarrollar todo su potencial.

### **Accesibilidad**

Microsoft entiende que la informática es una importante y poderosa herramienta para la gente que tiene alguna discapacidad. Las soluciones de tecnología accesible de la compañía permiten que toda aquella gente que tenga algún talento pueda desarrollar su potencial.

- **Liderazgo y compromiso.** Desde hace más de diez años, Microsoft ha venido explorando y haciendo evolucionar las soluciones de accesibilidad que van integradas en sus productos. En este sentido, la compañía reconoce su responsabilidad a la hora de desarrollar tecnologías que puedan ser utilizadas por todo el mundo, incluidas las personas con alguna discapacidad.

- **Atención a las necesidades y prioridades individuales.** Como líderes en la industria tecnológica, Microsoft trabaja para incrementar su conocimiento acerca de la tecnología accesible y sobre cómo mejorar la vida de cada persona, por lo que activamente pide sugerencias acerca de cómo mejorar sus productos.
- **La mejor accesibilidad.** El software de Microsoft tiene integradas sus funciones de accesibilidad; no obstante, la compañía trabaja para seguir aumentando la compatibilidad con todo tipo de tecnologías de accesibilidad utilizadas por clientes con cualquier discapacidad.
- **Soporte legal.** Microsoft entiende que el desarrollo de las leyes sobre accesibilidad ayuda a reforzar el trabajo de la compañía y de toda la industria de cara a mejorar continuamente la accesibilidad.

### **Década digital**

Microsoft, a través de su visión y liderazgo tecnológico, está ayudando a dar forma a la informática y a las comunicaciones del mañana para las empresas y las personas.

Durante esta década se harán realidad muchas de las propuestas tecnológicas que se han ido avanzando en años precedentes, a partir del desarrollo de los servicios Web y de las nuevas iniciativas alrededor de la seguridad y la privacidad.

El desarrollo de la década digital implica cumplir los siguientes desafíos:

- Derribar las barreras entre los sistemas y las organizaciones
- Ofrecer mayores niveles de fiabilidad de los sistemas
- Eliminar los problemas de comunicación entre las personas
- Poner fin a las limitaciones relacionadas con la gestión del conocimiento

### **Modelo de negocio**

El modelo de negocio en el que se basa Microsoft implica trabajar en España con 15.000 empresas que generan beneficios desarrollando productos y servicios sobre la plataforma de la compañía, y dando empleo a más de 50.000 personas. Por cada euro que factura Microsoft, su modelo de negocio es capaz de generar 12 euros.

La tecnología de Microsoft ofrece a sus clientes el valor añadido que supone tener una plataforma en constante evolución y sobre la que trabajan 800.000 compañías que ofrecen productos y servicios en torno a ella.

La tecnología de Microsoft ofrece un alto retorno de la inversión gracias a:

- El rápido incremento de la productividad
- Porque reduce los costes de propiedad
- Debido a su alto grado de interoperabilidad con sistemas y aplicaciones
- Por su facilidad de uso y el ahorro en costes de formación que ello supone

### **Liderazgo responsable**

Microsoft es consciente de su posición en la industria y, por lo tanto, de su papel a la hora de contribuir a la estandarización de todas aquellas tecnologías que pueden reportar un beneficio a los usuarios, a las empresas y a la sociedad en general.

Responsable en el modo en que desarrolla su plataforma, la compañía se preocupa por comunicar de una forma clara su agenda de lanzamientos, por mantener el ritmo de innovación y por colaborar con otros para garantizar la interoperabilidad de sus respectivas tecnologías.

Parte de esa responsabilidad se refleja en el continuo interés de Microsoft por colaborar en la modernización de la sociedad española, a través de diversas actividades y acuerdos:

- La compañía comparte el código fuente de sus tecnológicas con universidades para que puedan realizar migraciones a otros entornos.
- Trabaja en la implementación con partners españoles de las políticas de privacidad y seguridad, al tiempo que colabora con las Administraciones Públicas.
- Mantiene un programa de Community Affairs orientados a evitar la brecha digital.

### **Seguridad**

Microsoft se toma muy en serio su responsabilidad en una industria que tiene el desafío de ofrecer a los usuarios y a las empresas entornos fiables y seguros en el desarrollo de las TI. Las acciones de la compañía se realizan siempre teniendo muy presente garantizar la privacidad de los datos y mejorar la seguridad de los sistemas de la información.

Las iniciativas en seguridad de la compañía comprenden:

- Procesos, políticas y tecnologías mejoradas para ayudar a los clientes a mantenerse actualizados y seguros.
- Programas globales de educación que proporcionarán un mejor asesoramiento y herramientas para asegurar los sistemas.



- Actualizaciones de sus productos con nuevas tecnologías de seguridad que les permitan ser más resistentes a ataques externos.

La iniciativa Trustworthy Computing, lanzada oficialmente en enero de 2002, es una acción a largo plazo que se puso en marcha en todas las áreas de negocio de Microsoft para proporcionar una experiencia informática segura, privada y fiable a todo el mundo. Trustworthy Computing se basa en cuatro pilares fundamentales:

- **Seguridad** frente a los ataques, garantizando la protección de los datos y su confidencialidad.
- **Fiabilidad** para que los sistemas informáticos funcionen cuando se les necesite, y rindan lo que se espera de ellos.
- **Privacidad** de la información ajustándose a las presencias de los usuarios.
- **Integridad de los datos** para que los usuarios y las empresas tengan siempre disponible la información que necesiten, en el momento preciso.

Microsoft mantiene una política de inversiones en tiempo, dinero y recursos para formar a sus empleados, instituir nuevas políticas y controlar los procesos, así como para crear herramientas de desarrollo innovadoras para mejorar la seguridad del software.

### **Partners in learning**

La iniciativa Partners in Learning reconoce el valor educacional de la tecnología en las escuelas, ofreciendo una inversión continuada para cubrir las prioridades de educación local y haciendo el software accesible, a costes reducidos, para aquellos que lo necesitan y que, de otro modo, no podrían acceder a él.

Este tipo de acciones comprenden el uso de la tecnología y la enseñanza en las escuelas y permite poner en contacto a profesores locales, expertos en educación y responsables de políticas de formación.

No se trata de una donación puntual de tecnología, sino de un compromiso a largo plazo de Microsoft para asociarse con escuelas locales, profesores y empresas, estableciendo una fundación para el avance continuo en educación y enseñanza.

## Comunidad de desarrolladores

Microsoft mantiene un fuerte compromiso con la comunidad técnica de desarrolladores españoles. Para ello mantiene una serie de programas, recursos e iniciativas que pretenden ayudar a este colectivo a desarrollar tanto sus productos como su negocio sobre la plataforma Microsoft.

- **TechNet.** Programa dirigido a la comunidad de profesionales de TI para ofrecerles los recursos que les permitan conocer las últimas novedades en innovación tecnológica.
- **MSDN.** Esta iniciativa de Microsoft tiene como principal objetivo satisfacer las demandas y ofrecer recursos a las comunidades técnicas y de desarrolladores.
- **MCP.** Proyecto con recursos, formación y diferentes propuestas para la red de empresas certificadas que comercializan, implantan y ofrecen soporte sobre la tecnología Microsoft.
- **Action Pack.** Programa de recursos e iniciativas para todas aquellas empresas certificadas que ofrecen servicios de valor añadido sobre la tecnología Microsoft.

## Universidades

Microsoft tiene un fuerte compromiso con la docencia y la investigación, y como muestra de ello tiene en marcha una serie de iniciativas para acercar su tecnología tanto a estudiantes como a profesores de las universidades españolas.

La compañía mantiene actualmente una estrecha relación con personal docente e investigadores de 130 departamentos en 65 universidades de nuestro país.

Microsoft mantiene acuerdos para incorporar la tecnología .NET en sus programas de master y docencias de postgrado, con las siguientes universidades:

- UOC
- Universidad de Deusto
- Universidad de Castilla La Mancha
- Universidad Pontificia de Salamanca
- Universidad Antonio de Nebrija
- Universidad Carlos III de Madrid
- Universidad de Cantabria

Microsoft cuenta con un portal para estudiantes:

<http://www.microsoft.com/spanish/MSDN/estudiantes>



## **Difusión de la tecnología**

Con el fin de acercar su tecnología a la sociedad, facilitar el trabajo de las personas y potenciar el desarrollo y la investigación en el área de las TI, Microsoft pone en marcha toda una serie de proyectos y acciones dirigidas a fomentar la expansión tecnológica.

- **MSDN Academic Alliance**

Dirigido especialmente a departamentos universitarios de Ingeniería Técnica y Superior en Informática y a los centros de FP que imparten ciclos de grado superior, este proyecto pone a disposición de los profesores y alumnos toda la gama de herramientas de desarrollo y productos de Microsoft, así como librerías de información con fines educativos.

Los profesores y alumnos reciben de forma gratuita las actualizaciones mensuales y nuevas versiones de productos en CD-ROM.

A día de hoy, 60 departamentos están suscritos a este programa.

- **University Tour**

A través del programa University Tour Microsoft pretende acercarse y mostrar su tecnología .NET a los estudiantes universitarios de toda España.

Este proyecto lleva 3 años funcionando en nuestro país, con un total de 15.000 participantes activos de 65 universidades españolas. El 96% de los estudiantes encuestados manifestó su deseo de que Microsoft mantenga una presencia continuada en su universidad.

- **Microsoft Research**

Microsoft ha invertido 6.800 millones de dólares en Investigación y Desarrollo, más del 20% de su facturación en todo el mundo.

La labor investigadora de la compañía se centra en la división Microsoft Research, que cuenta con centros en Redmond, California, Beijing y Cambridge.

Microsoft Research trabaja en proyectos a largo plazo relacionados con las tecnologías del futuro. Su organización responde a un modelo académico similar al universitario y aproximadamente el 90% de los resultados de sus proyectos e investigaciones son de dominio público.

Microsoft Research Cambridge, fundado en 1997, es el laboratorio europeo de Microsoft y el primero establecido fuera de Estados Unidos. Cuenta con 75 investigadores europeos que trabajan en proyectos relacionados con:

- La mejora de los lenguajes de programación y herramientas de desarrollo
- Conseguir formas más intuitivas y productivas de interactuar con los ordenadores
- Aplicar sofisticadas teorías matemáticas para responder a los nuevos retos de la informática
- Reconocimiento de voz

Los proyectos de Microsoft Research se centran en avanzar en la informática más innovadora mediante un incremento de la productividad de los programas, ayudando a las empresas a operar de forma más eficaz y enriqueciendo las experiencias de las personas que usan la tecnología.

- **Imagine Cup**

Imagine Cup es la competición internacional de tecnología para estudiantes universitarios organizada y patrocinada por Microsoft Corporation, que pretende ser un estímulo y un reto para la creatividad e inteligencia tecnológica de los alumnos. El concurso, que se encuentra en su tercera edición a nivel internacional y segunda en nuestro país, repartirá este año más de 85.000 dólares en premios en metálico para los ganadores. El lema a seguir durante la presente edición en el desarrollo de los proyectos es *imagina un mundo donde la tecnología disuelva las fronteras*

## **INFORMACIÓN GENERAL RESUMIDA**

La Rama de Estudiantes recién creada en la Universidad Nacional de Educación a Distancia (UNED) tiene por objetivo principal **la difusión de la ciencia y la tecnología**.

Se ha consolidado inicialmente con 37 miembros en noviembre del año 2004.

La información general sobre sus actividades e información de cómo hacerse miembro se puede ver en la página Web: [www.ieec.uned.es/IEEE](http://www.ieec.uned.es/IEEE) dentro de Rama de Estudiantes.

Las actividades principales que las Ramas de España realizan son: charlas, cursos, congresos, concursos, actividades educativas, visitas a empresas y organizaciones, interrelación cultural y multidisciplinar y cualquier actividad que quiera desarrollar cada uno de sus miembros.

Actualmente puede participar cualquier estudiante de las carreras de Informática y de Industriales de la UNED. Para conocer más información sobre el IEEE, las Ramas de España y sus posibilidades leer los primeros artículos de éste Boletín y visitar la página Web. De todas formas cualquier información o consulta puede dirigirse a Eugenio López: [elopez@ieec.uned.es](mailto:elopez@ieec.uned.es).

Esperamos que os haya gustado a todos éste segundo Boletín y agradecer una vez más a todos los autores el haber participado en el mismo haciéndolo posible.

UN SALUDO

*Eugenio López*  
*Presidente de la Rama de Estudiantes IEEE-UNED*



**Hazte socio  
De la Rama de Estudiantes  
del IEEE en la UNED**

Web IEEE-UNED

<http://www.ieec.uned.es/IEEE/>

Charlas, conferencias,  
cursos, visitas, empresa,  
Boletín Electrónico, etc.



**RAMA DE ESTUDIANTES IEEE-UNED  
15-SEPTIEMBRE-2005 (BOLETIN)**

