



# Aurrera!

Nº 42

junio de 2011

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico

Dirección de Informática y Telecomunicaciones

## ÍNDICE

- La tecnología RFID  
Pág. 2
- Filtrado de contenidos web  
Pág. 6
- Alboan:  
UDA - Utilidades de Desarrollo de Aplicaciones  
Pág. 10
- Breves:  
Modificación LOPD  
KZgunea cumple 10 años  
Pág. 12

**S**eguro que todas las personas que están leyendo este ejemplar conocen los códigos de barras: qué uso se les da, para qué sirven, etc. Ya que están mucho más habituados a verlos en cualquier sitio, entre otros, en un *tetra-break* de leche o en una caja de zapatos. Sin embargo, si les preguntamos si han usado alguna vez la tecnología RFID, casi seguro que la respuesta es no. Es muy posible que se lleven una sorpresa cuando lean nuestro primer artículo, dedicado a [“La tecnología RFID”](#).

En muchas organizaciones el acceso a Internet, o mejor dicho, la salida a Internet, suele estar restringida mediante alguna aplicación informática para controlar el buen uso de ese recurso. Nuestra organización, como no podía ser de otra forma, desde hace unos años, también emplea un software que permite filtrar el acceso a algunas páginas webs con contenidos dudosos. En el artículo [“Filtrado de contenidos web”](#), os explicaremos cuál es la principal función de esos programas, qué características tienen y, además, os hablaremos del que se usa en el Gobierno Vasco.

Dentro del apartado “Alboan” queremos daros a conocer el fruto del trabajo realizado durante los últimos meses por los técnicos de EJIE. En concreto os hablaremos de las [“Utilidades de Desarrollo de Aplicaciones”](#), que se han desarrollado bajo las siglas UDA.

Por último, en la contraportada, hemos incluido dos noticias importantes. La primera de ellas, titulada [“Modificación LOPD”](#), nos informa de las novedades que ha introducido la Ley de Economía Sostenible en varios artículos de la Ley Orgánica de Protección de Datos.

Como segunda noticia, hemos incluido una referida a un viejo conocido, como es el proyecto KZ, del cual ya hemos hablado en varias ocasiones en boletines anteriores. Sin embargo, en esta ocasión lo hacemos por un motivo muy especial: el proyecto KZ cumple este año su décimo aniversario. Por ello hemos elaborado el artículo [“KZgunea cumple 10 años”](#).

Desde el Gabinete Tecnológico del Gobierno Vasco, y a través de estas páginas, queremos felicitar a todas aquellas personas que han hecho posible que el proyecto KZ cumpla 10 años. Felicidades a KZ y que cumpla muchos más.

## La tecnología RFID



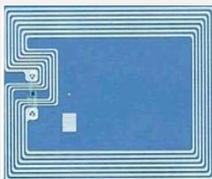
Hoy en día, el método más utilizado para identificar muchos artículos es el código de barras. De todas formas, los códigos de barras tienen algunas desventajas como pueden ser, entre otras, que almacenan poca información, ó que no pueden ser reprogramadas. Con objeto de superar todas esas barreras, los investigadores desarrollaron hace muchos años la tecnología conocida como RFID<sup>1</sup>.



### DICCIONARIO

<sup>1</sup> **RFID:** (son las siglas de *Radio Frequency Identification*, en castellano Identificación por Radiofrecuencia).

RFID se basa en un concepto similar al del sistema de código de barras; la principal diferencia entre ambos reside en que el segundo utiliza señales ópticas para transmitir los datos, y RFID, en cambio, emplea señales de radiofrecuencia.



Wikipedia (Sdepare)

• Sitio web de la Comisión Europea: descripción de las políticas y actividades de RFID dentro de la Unión Europea.

[http://ec.europa.eu/information\\_society/policy/rfid/index\\_en.htm](http://ec.europa.eu/information_society/policy/rfid/index_en.htm)

**P**oder controlar o identificar correctamente las cosas de nuestro entorno es muy importante. Muchas veces es necesario saber, por ejemplo, si tenemos en el almacén el material suficiente para concluir nuestro trabajo, dónde están las herramientas que necesitamos, etc. Hoy en día, la tecnología RFID se utiliza en muchos ámbitos, gracias a las ventajas que ofrece, y que comentaremos a lo largo de este artículo. En otros ámbitos, por el contrario, es totalmente desconocida. Por ello, a través de este artículo queremos informaros de en qué consiste y cuales son sus principales características.

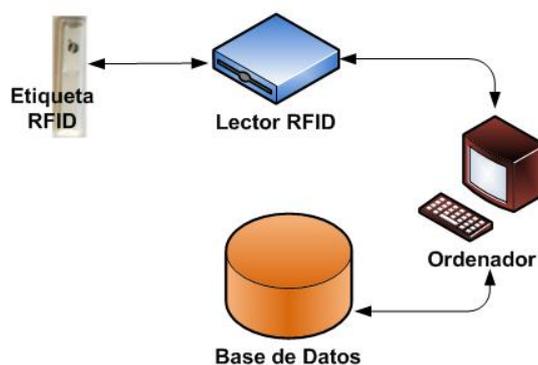


### ELEMENTOS

Uno de los aspectos más destacables de esta tecnología es que es capaz de gestionar la información de un elemento de forma remota, es decir, sin tener contacto físico con él. La tecnología RFID tiene los siguientes componentes:

1. **Etiqueta (tag):** es similar a una pegatina, va adherida al producto que se quiere identificar y consta de un microchip que almacena los datos y una pequeña antena que permite la comunicación por radiofrecuencia. El tipo de antena utilizada dependerá de la aplicación para la que está diseñada y de la frecuencia de operación.
2. **Lector:** está compuesto por una antena y un decodificador. El lector envía periódicamente señales para ver si hay alguna etiqueta en su rango de acción. Cuando capta la señal de alguna "extrae" su información y se la pasa al sistema de procesamiento de datos.
3. **Ordenador (host):** recibe la información de uno o varios lectores y se la comunica al sistema de información correspondiente.
4. **Sistema de procesamiento de datos (middleware):** procesa y almacena los datos

recibidos. Normalmente será un sistema ERP.



### ETIQUETAS

Las etiquetas son uno de los elementos más importantes de todo el sistema y, básicamente, pueden ser de 2 tipos:

- **Etiquetas pasivas:** éstas no poseen ningún tipo de alimentación eléctrica. La señal que les llega de los propios lectores es suficiente para activar su circuito integrado CMOS, de forma que pueden generar y transmitir la información que almacenan, y que, normalmente, serán muy pocos datos (p.ej., un número de identificación).

Los tags pasivos suelen tener una cobertura máxima de 1 metro, según la frecuencia de funcionamiento y el tamaño de la antena. Por otro lado, como no precisan de alimentación energética, esta etiqueta puede ser muy pequeña: tanto es así que, en algunos casos, puede insertarse bajo la piel de una persona o un animal.

Los tags pasivos transmiten información sólo cuando los lectores se la solicitan (tarea bajo demanda). Por esa razón, no son adecuados para labores de seguimiento o monitorización continua donde es necesario intercambiar muchos datos continuamente.

- **Etiquetas activas:** éstas disponen de una pila o un sistema de alimentación interno. Gracias a

esa la pila se puede dar corriente a los circuitos internos de la etiqueta de forma continua, propagar su señal al lector y que ésta esté siempre en funcionamiento. Muchos tags activos tienen rangos efectivos desde 10 m. hasta cientos de metros y una vida útil de sus baterías de hasta 10 años.

Si comparamos las etiquetas activas con las etiquetas pasivas podemos destacar las siguientes ventajas/desventajas:

- Los tags activos son mucho más fiables (tienen menos errores). Gracias a su fuente de energía son capaces de transmitir señales más potentes que las de los tags pasivos, lo que les lleva a ser más eficientes en entornos difíciles para la radiofrecuencia, como por ejemplo, cuando están rodeados de **agua** o **metal**.
- Si hay accesos muy frecuentes, si existen requerimientos de tiempo real (on-line) o hay procesamiento de datos, los expertos recomiendan usar tags activos.
- Las etiquetas activas suelen ser más grandes, más caras y su vida útil es, en general, mucho más corta.

Características principales de las etiquetas:		
Características:	Etiqueta Pasiva	Etiqueta Activa
Tiene batería	No	Sí
Coste	Menor	Mayor
Vida útil	Muy grande (casi ilimitado)	Limitado (según batería)
Cobertura	Menor (1 metro máx.)	Mayor (decenas de metros)
Capacidad datos	Menor	Mayor

Si analizamos la **frecuencia** a la que trabajan las etiquetas, se tienen los siguientes grupos (o bandas de frecuencias):

- ✓ **LF**: frecuencia baja (entre 125 y 134,2 KHz). (cobertura de muy corta distancia, varios cms.). Esta frecuencia está aceptada en todo el mundo y puede operar cerca de los metales.
- ✓ **HF**: alta frecuencia (13,56 MHz). (de 1 a 3 m.). La radiación a esta frecuencia no es absorbida por el agua ni por la piel humana, de ahí que se use mucho para la identificación de animales y de barriles con líquidos.
- ✓ **UHF**: frecuencia ultra alta (868 - 956 MHz). (larga distancia). Estas etiquetas no pueden ser utilizadas en todo el mundo porque no existen regulaciones globales para su uso y,

además, presentan problemas en determinadas superficies.

- ✓ **Microondas**: comprende las frecuencias de funcionamiento en las bandas de 2,45 GHz y 5,4 GHz., siendo su rango superior a 10 m.



“En octubre de 1948 el científico Harry Stockman publicó un artículo que muchos consideran que estableció las bases de la actual tecnología RFID y, por lo tanto, el origen de ella.”



**DICCIONARIO**

<sup>2</sup> **EPCglobal**: es la entidad que hoy en día gestiona todos los aspectos referentes al código electrónico de producto (EPC) a escala global y, por lo tanto, es la encargada de proporcionar a las empresas que lo solicitan un código único para cada producto.

EPCglobal es subsidiaria de la organización sin ánimo de lucro GSI, que desde los años 70 ha administrado estándares como el código de barras y el EDI.

[www.epcglobalinc.org](http://www.epcglobalinc.org)

EL ORIGEN

Una vez vistas las características y los elementos que componen la tecnología RFID veamos cual fue su origen. De entre todas las teorías existentes, hoy en día la más aceptada es que en 1939, durante la **Segunda Guerra Mundial**, los británicos desarrollaron una tecnología muy similar a ella, el sistema *IFF* (*identification: friend or foe* = identificación: amigo o enemigo). Los aliados usaron esa tecnología, principalmente, para identificar de una manera más fiable los aviones detectados en el radar y, de esa forma, saber si esos aviones eran aliados o no mucho antes.

Una vez acabada la guerra, los científicos e ingenieros continuaron sus investigaciones sobre estas tecnologías. En octubre de 1948 el científico **Harry Stockman** publicó un artículo titulado “*Communications by Means of Reflected Power*”, que muchos consideran que estableció las bases de la actual tecnología RFID y, por lo tanto, el origen de ella.

CASOS DE USO Y APLICACIONES

Durante las siguientes décadas esta tecnología tuvo una lenta pero continua evolución. En los años 80 la tecnología RFID se empezó a aplicar en varios ámbitos: en Estados Unidos, por ejemplo, se orientó, principalmente, hacia la logística (control de transportes y mercancías). En Europa, por el contrario, inicialmente se usó sobre todo para el control y seguimiento del ganado.

En 2003 se fundó **EPCglobal**<sup>2</sup> y de ahí surgió el



## DICCIONARIO

<sup>3</sup> **Estándares:** En la década de los 90 comenzaron a aparecer los primeros estándares que regulaban algunos aspectos de la tecnología RFID.

Dado que los estándares EPC eran incompatibles con los estándares de ISO (en concreto con la **serie 18000**), la organización EPCglobal empezó a desarrollar una nueva generación de estándares llamados **Gen2** (abreviatura de "EPCglobal UHF Generation 2"), con el objetivo de conseguir la interoperabilidad entre ambos estándares y, de esta forma, potenciar los sistemas RFID.

estándar EPC<sup>3</sup>. [Ver el cuadro "El código EPC"]

También en 2003 RFID tuvo otro importante respaldo: la empresa Walmart y el Departamento de Defensa estadounidense decidieron adherirse definitivamente a esta tecnología.

Hoy en día la tecnología RFID se está extendiendo a otros ámbitos, como pueden ser:

- **Tiendas de ropa:** los tags facilitan el seguimiento de todos los artículos. El uso de esta tecnología ha causado una importante polémica, ya que en algunos casos las etiquetas RFID siguen funcionando incluso después de que se hayan comprado los productos y se hayan llevado a casa, y podrían ser rastreados para otros propósitos sin relación alguna con sus funciones de inventario.
- **Bibliotecas:** Muchos libros que hoy en día nos podemos encontrar en nuestras bibliotecas ya incorporan en su interior estas pequeñas etiquetas. Estos tags, además de mejorar las operaciones de préstamo y devolución, favorecen el archivo correcto de los libros y reducen la carga de trabajo de los servicios bibliotecarios, ya que los sistemas RFID proporcionan un mejor control frente al robo o extravío. La primera biblioteca que empleó RFID fue la Farmington Community Library



de Michigan (EE.UU.), en 1999.

- **Hospitales:** otro ámbito con mucho potencial es el sanitario, donde se puede usar para el control de medicamentos, identificación y seguimiento de muestras médicas o, incluso, la localización de los propios pacientes dentro de los centros de salud. Esta última utilidad no ha tenido de momento mucho éxito, ya que el usuario debe llevar una pequeña etiqueta o pulsera que lo identifique, lo cual resulta invasivo para muchas personas.
- **Autopistas:** Hoy en día, muchas autopistas ya utilizan sistemas RFID para gestionar el paso de los vehículos y el cobro del peaje. Los vehículos llevan en sus parabrisas unas tarjetas que son leídas mientras estos atraviesan los peajes y es esa información la que se utiliza después para completar el cobro del peaje. Este sistema ayuda a disminuir los atascos causados por las cabinas de peaje tradicionales. La primera aplicación para peajes o aduanas se realizó en 1987, en Noruega.
- **Pasaportes y carnets de conducir:** Varios países han propuesto ya la implantación de dispositivos RFID en sus nuevos pasaportes, aumentando la eficiencia en las máquinas de lectura de datos biométricos. Sin embargo, muchos la rechazan porque la consideran una clara amenaza tanto para la seguridad personal como para la privacidad. El estado de Virginia (EE.UU.) ha pensado en poner etiquetas RFID en los carnets de conducir con el objetivo de

### El código EPC

El EPC (*Electronic Product Code* o Código Electrónico de Producto) es un número único diseñado para identificar de manera inequívoca cualquier objeto.

Este código es un sistema de identificación y seguimiento de las mercancías «en tiempo real». El número se encuentra almacenado en un chip, denominado «tag», que puede leerse mediante radiofrecuencia RFID y puede proporcionar más datos que el clásico código de barras. Ya que al código EPC es posible asociarle datos dinámicos referentes al ítem que identifica, tales como: fecha y lugar de fabricación, fecha de vencimiento, medidas del artículo (longitud, anchura y altura), etc. Con la

utilización de este código electrónico se facilita el seguimiento de los productos a lo largo de la cadena de abastecimiento o el canal de distribución.

#### Estructura del código EPC

Sus principales características son:

1. El sistema de codificación es igual para todos los países del mundo.
2. La codificación usa la numeración hexadecimal, por lo que es perfectamente inteligible por los ordenadores.
3. Está compuesto por 24 dígitos hexadecimales.
4. Los últimos 9 números hacen de numerador, de tal forma que es posible numerar más de 68 billones de un mismo producto sin repetir el código.



que la policía realice sus comprobaciones de una forma más rápida.

## CONCLUSIONES

Según los expertos, si bien la tecnología RFID tiene muchas ventajas<sup>4</sup>, no se prevé que ésta sustituya o elimine por completo al código de barras, sino que serán dos tecnologías que coexistirán en el tiempo. Algunas razones que impiden que la tecnología RFID se implante de forma masiva pueden ser las siguientes:

- **Estándares:** todavía no existe un estándar único en todo el mundo, como ocurre con los códigos de barras. Se hace necesario un estándar único y una codificación unívoca de la información a escala global, es decir, conseguir la estandarización de EPCglobal, ISO, ETSI.
- **Fiabilidad:** actualmente RFID no es la solución idónea para cualquier producto, ya que tiene un mal funcionamiento en presencia de líquidos y metales. Por ejemplo, en la industria farmacéutica, hay muchas sustancias que contienen líquidos, por lo que la señal puede verse alterada y dar información errónea.
- **Costes:** sigue resultando cara la implantación masiva de RFID. El objetivo de los fabricantes es llegar a 0,05 euros de coste por etiqueta.
- **Frecuencias:** Existen cuatro posibles bandas de frecuencia, cada una con sus restricciones de potencia y cobertura. Por lo que se hace necesaria su regulación global.

- **Confianza:** aceptación de la tecnología RFID por parte de la sociedad. De hecho, diversos estudios de mercado constatan el bajo conocimiento y en algunos casos desinformación que existe entre los consumidores sobre la tecnología RFID.

“Muchos rechazan la tecnología RFID porque la consideran una clara amenaza tanto para la seguridad personal como para la privacidad.”

- **Seguridad:** Este punto es quizá el aspecto más polémico de todos los que rodean a la tecnología RFID. Tanto es así que la Comisión Europea publicó el 12 de mayo de 2009 una recomendación sobre la aplicación de los principios relativos a la **protección de datos** y la **intimidación** en las aplicaciones basadas en la identificación por radiofrecuencia. En dicha recomendación, la Comisión estableció el requisito de que el grupo de trabajo sobre protección de datos del artículo 29 aprobara un marco para evaluar el impacto de las aplicaciones RFID sobre los datos personales y la intimidación ([http://ec.europa.eu/information\\_society/policy/rfid/documents/pia-es.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/pia-es.pdf)). Se trata de las denominadas «evaluaciones del impacto sobre la intimidación» o **PIA** (por las siglas en inglés de *privacy impact assessment*). □

### RFID en el Gobierno Vasco

En el proyecto de despliegue de las nuevas tarjetas electrónicas corporativas que se ha llevado a cabo recientemente entre todo el personal del Gobierno Vasco, y que han sido suministradas por Izenpe, se ha diseñado una tarjeta que dispone de elementos tecnológicos seguros. Por una parte, incluye un chip criptográfico con certificado electrónico reconocido; y, por otra parte, se las ha dotado de la tecnología RFID para facilitar el acceso organizado y cómodo a las dependencias en los diferentes edificios del Gobierno.



Izenpe

Gracias al chip de proximidad integrado de RFID, siguiendo el estándar *Mifare*, al acercarlo a menos de 10 centímetros de uno de los sistemas de acceso, éste dará permiso o no, en función de si se tiene autorización para acceder a la zona.

El uso de este tipo de tecnología está permitiendo la **homogeneización corporativa** y la extensión de uso para el control de acceso (sedes, parking, comedor, zonas restringidas) y para el control de presencia. Por otra parte, agilizará y facilitará al personal su identificación en entradas y salidas de una forma segura y fácil.



### DICCIONARIO

#### <sup>4</sup> Tecnología RFID vs Código de Barras:

- ✓ **Más datos:** Las etiquetas RFID pueden almacenar más datos sobre un artículo (lote, peso, etc.) que un código de barras.
- ✓ **Ratio de lectura:** Las etiquetas RFID ofrecen un mayor ratio de lectura en las operaciones de alta velocidad (clasificación de paquetes, etc.)
- ✓ **Visión directa:** La lectura de los códigos de barra requiere que exista “visión directa” entre el scanner y el código de barras. Las etiquetas RFID pueden ser leídas a través de materiales sin tener visión directa.
- ✓ **Capacidades de escritura:** Las etiquetas RFID pueden ser “reprogramadas” con nuevos datos.



## Filtrado de contenidos Web



Hoy día, el acceso a contenidos y servicios utilizando Internet es un valioso recurso, que se usa tanto desde el ámbito particular como desde el ámbito empresarial, y que, bien utilizado, es de gran ayuda en infinidad de situaciones; sin embargo, debemos vigilar a qué contenidos se accede, con el objetivo de utilizar Internet de un modo correcto y seguro. Es aquí cuando aparece el concepto *filtrado de contenidos Web*.



### DICCIONARIO

<sup>5</sup> **copyrightware**: es uno de los términos utilizados en el mundo anglosajón para denominar al filtrado de contenidos web, pero siendo un término que genera controversia, se prefieren utilizar los términos *Internet filter* o *URL Filter*.

**E**l filtrado de contenidos Web, o filtrado de URLs, se realiza a través de herramientas software que, básicamente, lo que hacen es **bloquear los accesos a páginas Web inapropiadas**, a través de un administrador, el cual decide cuáles son esas páginas a bloquear, es decir, los contenidos de Internet que son inapropiados. A estas herramientas de filtrado de contenidos también se les conoce con los nombres de *copyrightware*<sup>5</sup>, *content control software* o *web filtering software*.

El filtrado de contenidos es una herramienta tecnológica de tipo software, que puede ser instalada de diferentes maneras, desde la instalación de un programa software en un ordenador personal, hasta la instalación de programas en los servidores que dan acceso a Internet; en todos los casos se activa y configura en función de una **política de seguridad determinada**.

Éticamente, el filtrado de contenidos puede interpretarse como un modo de censura, por lo que la formación de los usuarios es un elemento básico para comprender el porqué de este tipo de herramientas, así como saber cuáles son los contenidos a los que se debe acceder y a cuáles no.

### ANTECEDENTES

La Unión Europea, en octubre de 1996, aprobó dos documentos referentes a los contenidos en medios como Internet:

- ✓ Libro Verde sobre la Protección de los Menores y la Dignidad Humana en los Servicios Audiovisuales y de Información.
- ✓ Comunicación sobre Contenido Ilegal y Perjudicial en Internet.

El primer documento, el Libro Verde, proponía, por un lado, identificar o categorizar, para

cualquier persona, y al margen de las legislaciones nacionales, todo aquel material que violara la dignidad humana; y, por otro lado, evitar que los menores pudieran encontrar, accidentalmente o no, material que perjudicara su desarrollo físico y mental, estando éste solamente disponible para el público adulto. En cualquier caso se quería dejar claro lo que es prohibir el acceso a un contenido a todo el mundo, o sólo a los menores.

### NIVELES DE FILTRADO

Un filtrado de contenidos puede ser aplicado desde diferentes niveles, por ejemplo, el gobierno de un país puede prohibir el acceso a determinados contenidos (en determinados casos este tipo de actuaciones pueden ser consideradas como **censura**, como, por ejemplo,

**“El filtrado de contenidos lo que hace es bloquear el acceso a páginas Web inapropiadas en función de una política de seguridad determinada.”**

las que aplican países poco democráticos para con su ciudadanía), o un proveedor de acceso a Internet (ISP) puede bloquear contenidos a las personas usuarias, o un empleador a sus personas empleadas, o unos padres establecer a qué sitios pueden y no pueden acceder sus hijos.

De cualquier forma, se puede elegir un proveedor de acceso a Internet que bloquee contenidos inapropiados para niños, si bien la mayoría de las veces que se utiliza un filtrado de contenidos éste se realiza o bien por las organizaciones o por los propios padres, incluso existe la posibilidad de que personas adictas a algunos de los servicios o contenidos de Internet (juego,

pornografía...) puedan auto instalarse filtros de acceso a esos contenidos.



## OTRAS FUNCIONALIDADES

Las herramientas de filtrado actuales, además de bloquear el acceso a páginas Web, también incluyen otras funcionalidades, entre las que destacan:

- Monitorización de accesos de los usuarios
- Informes de uso
- Detección de intentos reiterados de acceso a páginas prohibidas

ámbito, de tal modo que para cambiar su configuración requieren de una palabra de paso (*password*), que también es requerida para realizar la desinstalación del producto; este tipo de filtro es lo que se conoce como **control parental**. Además de utilizarse en el ámbito doméstico, son una buena elección para ser utilizados en bibliotecas con acceso a Internet, a las cuales puedan acceder menores. Requieren administrar cada ordenador de manera individual, y debe ser actualizado en cada puesto que se instale.

- **ISP's con acceso limitado a contenidos:** son proveedores de acceso a Internet que sólo permiten el acceso a una porción de Internet,



## DICCIONARIO

<sup>6</sup> **P2P:** del inglés "Peer to Peer", que significa entre iguales, es un servicio en el que se transmiten datos entre personas conectadas a una determinada red, en el cual cada parte realiza funciones de "cliente" y de "servidor". En la práctica existe una máquina que realiza las labores de mediador. Por ejemplo, Napster fue un servicio P2P de distribución e intercambio de archivos de música, que comenzó en el año 2000, y que originó las primeras protestas con respecto a los derechos de autor.

http://www.servicios.jakina/fitroweb/stop.asp?CAT=%5Bsearch\_engines-ig%7Cpornography-ig-au%7Credirectors-ig%5D&RULE=%5BDeny\_Porn%5D&DATETIME=%5B18/May/2011:12

**OPTENET**  
Get optimal internet

La página a la que desea acceder no puede ser visualizada, ya que pertenece a una categoría no permitida: [search\_engines-ig|pornography-ig-au|redirectors-ig]

Si cree que ha habido un error de categorización, por favor pulse el botón enviar y si nos indica su e-mail le daremos una respuesta una vez haya sido analizada.

**Ikusi nahi duzun orrialdea ezin da bistaratu, baimendu gabeko kategoria bati dagokiolako: [search\_engines-ig|pornography-ig-au|redirectors-ig].**

**Kategori hutsegitea dela uste baduzu, mesedez, sakatu BIDALI botoia eta adierazi zure helbide elektronikoa. Behin zure eskaera aztertuta, erantzungo dizugu.**

E-mail/Posta:

URL/URL:

Observaciones/Oharrak:

Enviar / Bidali

Borrar / Ezabatu

Powered by **OPTENET**

- Denegación del acceso a algunos servicios de Internet (por ejemplo, los servicios P2P<sup>6</sup>, chats o comercio electrónico)
- Limitación en el tiempo de conexión
- Bloqueo del acceso a Internet en función del número de intentos de accesos a páginas no permitidas

Otras funcionalidades están destinadas a ofrecer protección frente a las amenazas que existen en la web, almacenando las URL de sitios web que hospedan software malicioso y los que hospedan sitios que simulan ser páginas de sitios reales.



## TIPOS DE FILTROS

Los diferentes tipos de filtros los podemos clasificar de la siguiente manera:

- **Filtros cliente:** se instala como un software en el ordenador personal, o en cada equipo de una red. Estos filtros pueden ser configurados de tal forma que se adapten a las necesidades de su

estando especialmente diseñado para menores, ya que ofrecen acceso a páginas que han sido cuidadosamente revisadas múltiples veces y que han sido consideradas apropiadas y seguras.

- **Filtros en los servidores de acceso a Internet:** existe una política de acceso definida por la institución que es implementada en los servidores a través de estos programas de filtrado; estos servidores pueden ser los del proveedor de acceso a Internet o los servidores de la propia institución, en este último caso se suelen instalar en los equipos encargados de dar acceso a Internet o en una máquina dedicada exclusivamente a realizar este trabajo.
- **Filtros en el motor de búsqueda:** muchos buscadores (Google, Alta Vista, etc.) ofrecen la posibilidad de habilitar lo que se conoce como *safety filter* o filtros de seguridad, con lo cual, en las búsquedas realizadas se descartan los accesos que el filtro detecta como inapropiados, sin embargo, si se conoce la URL



concreta, se puede acceder a ella sin que los filtros del motor de búsqueda actúen. Para combatir esto muchos buscadores ofrecen versiones orientadas a menores.

## CLASES DE FILTRADOS

Básicamente existen cuatro tipos de filtrados, que son los siguientes:

- **Por contenido:** según qué tipo de contenido ofrezca el sitio Web se establecen dos listas, las “listas negras”, contenidos catalogados como inapropiados, los cuales no serán mostrados gracias al filtro; y “las listas blancas”, de páginas Web que se han catalogado como adecuadas, a las cuales el usuario tiene acceso.
- **Por análisis semántico:** se compara cada palabra del texto que se introduce en la URL con una lista de palabras vinculadas a contenidos inapropiados, y cuando se da una coincidencia el acceso se bloquea; esto puede conllevar a muchos errores de interpretación, ya que las palabras pueden tener diferentes

significados (polisemia) según el contexto en el que aparezcan.

- **Por análisis de la imagen:** se analiza la estructura de la imagen en función de unos patrones establecidos (técnicas de aprendizaje automático), por ejemplo, utilizando la herramienta **imgSeek**<sup>7</sup>; este tipo de filtrado es utilizado, sobre todo, para bloquear páginas de carácter pornográfico.
- **Por la calificación moral de los contenidos:** es el más utilizado hoy en día y es el que recomienda la Unión Europea; cabe destacar el mecanismo de filtrado PICS (*Platform for Internet Content Selection* - Plataforma para la Selección de Contenidos de Internet) desarrollado por el consorcio W3C (*World Wide Web Consortium*), organismo encargado de establecer los estándares de la red (ver tabla «Especificaciones PICS» a pie de página). El problema es que el etiquetado es realizado por los propios generadores del contenido, lo cual es un claro caso de autorregulación, esto es, el propio generador de los contenidos es el que decide cómo clasificar este contenido.

Es de destacar que los filtros de contenidos no



### DICCIONARIO

<sup>7</sup> **imgSeek:** es un producto basado en software libre que está disponible en versiones para varias plataformas; su potencia viene dada por su capacidad para buscar una imagen por su similitud con otra. Para convertirlo en un detector de imágenes pornográficas basta con confeccionar dos colecciones, una de imágenes pornográficas y otra de no pornográficas e indexar ambas.

### Especificaciones PICS

Las especificaciones PICS (Plataforma para la Selección de Contenido en Internet) permiten incluir etiquetas que se asocian con los contenidos de Internet, a través de metadatos (datos sobre los datos), etiquetas electrónicas no visibles por el lector.

Originalmente estas especificaciones fueron diseñadas para controlar, por parte de padres y profesores, el acceso que hacían los menores sobre los contenidos web.

No se corresponden con ningún software, no son sino un conjunto técnico de especificaciones que posibilita clasificar los contenidos web utilizando metadatos, tampoco establece criterios de clasificación de la información.

Es el proveedor de contenidos el que, en base a una clasificación previa (conjunto de categorías y niveles para clasificar contenidos), debe establecer el nivel asociado al contenido que puede mostrar a sus clientes.

Para que tenga efecto, el software de filtrado de contenidos debe saber

interpretar las especificaciones PICS.

A día de hoy existen tres sistemas de clasificación PICS:

- **RSACi** (*Recreational Software Advisory Council on the Internet*). Es el más extendido y clasifica los materiales en función del grado de sexo, violencia, desnudos y lenguaje soez.
- **SafeSurf.** Este sistema incluye categorías como edad, palabrotas, temas heterosexuales, temas homosexuales, desnudos, violencia, *sexo-violencia-y-palabrotas*, intolerancia, apología del uso de drogas, otros temas para adultos y juego, con nueve subcategorías para cada una de ellas.
- **Net Shepherd.** Clasifica los sitios en base a criterios de madurez (general, niños, adolescentes, jóvenes, adultos y objetable) y niveles de calidad (de una a cinco estrellas).

(Clasificación PICS extraída de la publicación realizada por Javier Villate en la página Web de Fronteras Electrónicas, con el título «Libertad de expresión en Internet, retos y amenazas»)

<http://www.w3.org/PICS/>

siempre actúan sobre toda la página, puede que todos los contenidos sean “normales” excepto, por ejemplo, una imagen o un enlace (*link*) dentro de la página visualizada, entonces el filtro de contenidos actuará sobre esa imagen o ese enlace.

## PROBLEMAS EN EL USO DE FILTROS

Existen dos problemas principales cuando utilizamos un programa de filtrado de contenidos, por un lado, que se bloqueen contenidos que no son inapropiados, pero que, al contener, por ejemplo, alguna palabra que puede considerarse inapropiada, no permita el acceso a los mismos; esto se denomina *overblocking* (**sobrebloqueo**), ocurre en los filtros que son altamente efectivos; y, por otro lado, que se bloqueen de una forma ineficaz los contenidos, dejando acceder a contenidos inapropiados, lo que se conoce como *underblocking* (**infrabloqueo**).

## FILTROS COMERCIALES Y EL FILTRO UTILIZADO EN LA RED CORPORATIVA DEL GOBIERNO VASCO

En el mercado existen numerosos programas de filtrado de contenidos, como pueden ser, entre otros muchos, *Net Nanny*, *CyberPatrol*, *Surfcontrol* u *Optenet*.

En el caso de la **red PREMIA** del Departamento de Educación, Universidades e Investigación se utiliza el producto *McAfee Web Gateway*, mientras que el programa que se utiliza en la **Red Corporativa Administrativa del Gobierno Vasco (RCAGV<sup>8</sup>)** para filtrar los contenidos es el *WebFilter de Optenet*, entre sus principales características destacan:

- Más del 99% de eficacia en los procesos de filtrado
- Porcentaje de error inferior al 0,1%
- Los filtros no afectan a las comunicaciones, tardando menos de 1 milisegundo en analizar una página de Internet
- Informes de todos los procesos de filtrado
- Utilización de tecnología avanzada: motor de análisis semántico de contenido on-line, análisis heurístico de ejecutables, listas predefinidas, etc.
- Servicio de desbloqueo de páginas por error, el

usuario puede mandar automáticamente un correo electrónico exponiendo el motivo del error para su corrección

- Permite el bloqueo de programas de intercambio y descarga de archivos P2P (*peer to peer*)
- Permite bloquear los programas de mensajería instantánea
- Permite el filtrado de protocolos, tomando diferentes acciones en base a la política establecida

Posee unas **políticas de filtrado** que pueden eliminarse, editarse y crearse. Para realizar estas dos últimas acciones, editar o crear políticas, se pueden seleccionar **cinco parámetros diferentes**:

- Estado (si la política va a estar activa o no)
- Origen y destino (conjunto de usuarios, grupos de IP, etc., a los cuáles les va a afectar la política)
- Perfiles (grupo de condiciones que deben cumplirse para aplicar la política)
- Acción (varían en función del perfil seleccionado)
- Horario (período temporal en el que se aplicará la política)

Si la política se asocia a un evento, cada vez que la política sea ejecutada un evento será lanzado, como, por ejemplo, una alarma.

¿Qué son los perfiles? Es una combinación flexible de condiciones basadas en categorías de sitios web (páginas web relacionadas con un contenido específico), tipos de archivos y tamaños de los mismos (puede afectar a todas las URLs o sólo a categorías concretas), excepciones (URLs a incluir y a excluir), tiempo límite de navegación, verificación de solicitudes reiteradas a páginas prohibidas y verificación de certificados digitales (permite establecer políticas si un certificado digital no es válido).

Existen, por defecto, dos políticas de filtrado web:

- **WebWl**: permite el acceso a todas las URLs incluidas en la Lista Blanca
- **WebBl**: bloquea el acceso a todas las URLs incluidas en la Lista Negra

El incluir una URL determinada en estas listas no implica que siempre será accesible o que siempre estará bloqueada, ya que, aunque estas listas están asociadas con dos perfiles, su aplicación dependerá de la estrategia usada por las políticas de filtrado. □



### DICCIONARIO

<sup>8</sup> **RCAGV**: Red Corporativa Administrativa del Gobierno Vasco: “se corresponde con la gestión centralizada de los servicios de telecomunicaciones; la Red Corporativa Administrativa, referida a órganos, inmuebles y servicios de telecomunicaciones en sentido amplio, ha de entenderse como una definición dinámica que, respetando los parámetros básicos, evolucionará al ritmo de las alteraciones orgánicas y físicas, sin solución de continuidad. Se integrarán en ella los Departamentos y Organismos Autónomos, ubicados en los edificios de gestión centralizada o en otros inmuebles.”

(Extraído de la “Propuesta de Acuerdo de Consejo de Gobierno relativa a la definición de la RCA de Telecomunicaciones”, de 28 de julio de 1998)



ALBOAN:



## Utilidades de Desarrollo de Aplicaciones

Gobierno Vasco - EJIE

"UDA basa su funcionamiento, principalmente, en el uso de patrones o plantillas."

**D**urante los últimos meses, la sociedad informática del Gobierno Vasco, EJIE, ha estado trabajando en un proyecto que tiene como objetivo **augmentar la productividad de los desarrolladores** que realizan su trabajo para el Gobierno Vasco. A través de ese proyecto, denominado UDA (*"Utilidades de Desarrollo de Aplicaciones"*), EJIE quiere facilitar a sus proveedores un conjunto de utilidades, herramientas, librerías, *plugins*, guías y normativas funcionales y técnicas que les permitan acelerar el proceso de desarrollo/construcción de cualquier sistema software basado en tecnología **Java**.

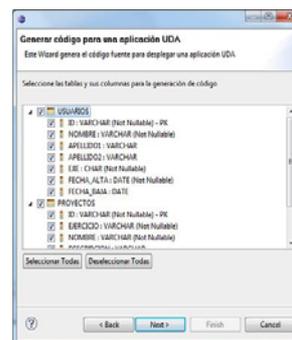
### CARACTERÍSTICAS DE UDA

A la hora de definir UDA EJIE identificó las tecnologías que mejor soportaban cada una de las **capas** que componen la arquitectura técnica de cualquier aplicación informática, especificando en cada caso el modelo de uso y su inter-relación. Alguna de las tecnologías definidas en UDA son las siguientes:

- Capa de presentación: Tiles, jQuery, Spring MVC y JSTL
- Capa core: Spring Framework, Spring AOP, Weblogic y Java Development Kit
- Capa de persistencia: Spring JDBC y EclipseLink
- Capa de servicio: Spring Framework
- Capa de plataforma: Eclipse, Subversion, Maven y Ant
- Capa de asistentes: Hibernate Tools y Freemaker

Una de las principales características del proyecto UDA es que todo el trabajo realizado por los técnicos de EJIE y los productos seleccionados pueden servir para cualquier otra

entidad que no sea Gobierno Vasco-EJIE (sea administración pública o no). Es por ello que, entre otras cosas, se podría decir que UDA es una especie de *"proyecto de software libre"*, y que, por lo tanto, permitiría a cualquier tercero interesado aportar los desarrollos realizados, pedir modificaciones, notificar fallos (*bugs*), etc. y, por supuesto, reutilizar lo que los propios responsables de EJIE construyan. Esto es posible porque todo lo que se ha desarrollado está basado en herramientas, librerías y *frameworks* de software libre.



EJIE

Para ello UDA proporciona a los desarrolladores (programadores informáticos) una serie de "piezas" básicas, es decir, una serie de *plugins*, que les van a permitir **generar código de forma automática** en las tareas repetitivas y de poco (o nulo) valor añadido, pero que, sin embargo, son imprescindibles para construir una aplicación informática. En este sentido, cabe indicar que UDA:

- Propone elementos de usabilidad web, que aprovechan las mejoras proporcionadas por las tecnologías RIA - AJAX y cubre los escenarios de uso más habituales para aplicaciones web.
- Genera interfaces de usuario. Crea automáticamente las interfaces de datos y otras de uso común (combos enlazados, fechas -horas, *feedback*, etc.)
- Genera código. Crea el código imprescindible en toda aplicación con arquitectura en capas.



- Es flexible y configurable. Permite adaptar el código generado por los asistentes a las necesidades de cada organización (libro de estilo, estándares de codificación, etc.)
- Es adaptable y ampliable. Su arquitectura modular y desacoplada permite ampliar y/o sustituir las tecnologías utilizadas en cada una de las capas que la componen.
- Crea aplicaciones accesibles. Hasta donde sea posible, se cumplen con las recomendaciones WCAG2.0 y WAI-ARIA.

Sin teclear ni una sola línea de código el Departamento dispondría de una aplicación plenamente operativa en muy pocos minutos.



### FUNCIONAMIENTO DE UDA

UDA basa su funcionamiento, principalmente, en el uso de **patrones o plantillas**.

En ese sentido, EJIE, en colaboración con un equipo de expertos, identificó y normalizó en su momento el conjunto de patrones de usabilidad web para aplicaciones con **tecnología RIA-AJAX**, así como los principios de diseño y de usabilidad que pueden ser aplicados en las aplicaciones de gestión. En dichos trabajos se catalogaron y estudiaron los distintos tipos de aplicaciones existentes:

- Según el contexto: de internet, de intranet, de extranet, o combinaciones de varios de ellos.
- Según la experiencia de sus usuarios: expertos de negocio, noveles, sin conocimientos, etc.
- Según su frecuencia de uso: diario, casual, en fechas concretas, etc.

Algunos de los asistentes que ya se encuentran disponibles permiten, por ejemplo:

- generar código de negocio y control
- generar interfaces de usuario
- generar nuevos módulos Web
- generar nuevos módulos EJB
- generar código para EJB cliente
- generar EJB servidor

El espíritu de este proyecto, y por tanto su principal objetivo, es **aumentar la productividad** de los programadores informáticos, sin coartar por ello su imaginación ni su libertad para crear software.

“UDA tiene como objetivo aumentar la productividad de los desarrolladores que realizan su trabajo para el Gobierno Vasco.”

### PRÓXIMOS PASOS

Actualmente, los responsables del área de consultoría de EJIE, área encargada del desarrollo y mantenimiento de UDA, están valorando la posibilidad de preparar un “kit de desarrollo” que incluya todos los elementos de UDA para, posteriormente, ponerlo en Internet a disposición de todos los proveedores. Este kit incluiría un paquete descomprimible con el IDE Eclipse totalmente configurado, una imagen virtual (sistema operativo virtualizado) con el entorno de desarrollo ya operativo, vídeos explicativos de cómo generar un nuevo sistema software, y, por supuesto, toda la documentación necesaria sobre UDA.

UDA, en definitiva, pretende convertirse en el nuevo generador de código del Gobierno Vasco-EJIE y, al mismo tiempo, gracias a sus módulos, que los Departamentos y Organismos Autónomos del Gobierno puedan desarrollar sus aplicaciones en un plazo mucho más corto. □

ID Pedido	Lugar de envío	Estado	Ult. Actua	Descuento
<input type="checkbox"/> 11	Madrid	S	19/03/2011	25
<input type="checkbox"/> 22	Bilbao	S	02/05/2011	22
<input type="checkbox"/> 454	Murcia	N	15/04/2011	45
<input type="checkbox"/> 666	12	N		0
<input type="checkbox"/> 666	12	N		0

Se establecieron entonces los modelos básicos de navegación, los estilos visuales, el catálogo de componentes de presentación y sus comportamientos, la disposición preferente de los elementos que componen las páginas Web, modelos de refresco, etc.

De entre todos los elementos disponibles en UDA uno los más interesantes es el uso de los “asistentes”. Estos permiten generar automáticamente los componentes básicos necesarios para construir un sistema software.

EJIE

EJIE

[+info]:

Repositorio del proyecto UDA

<http://code.google.com/p/uda/>



Nº 42

junio de 2011



## Modificación LOPD

La Disposición final quincuagésima sexta de la Ley de Economía Sostenible, que el pasado 6 de marzo entró en vigor, ha modificado los artículos 43, 44, 45, 46 y 49 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter (LOPD). Dichos artículos hacen referencia al régimen sancionador.



BOLETÍN OFICIAL DEL ESTADO



Núm. 55

Sábado 5 de marzo de 2011

Sec. I. Pág. 25033

### I. DISPOSICIONES GENERALES

#### JEFATURA DEL ESTADO

4117 Ley 2/2011, de 4 de marzo, de Economía Sostenible.

La Ley recoge una nueva figura, la del **apercibimiento** (medida preventiva), una medida excepcional y limitada, que permite advertir de la irregularidad cometida y requerir la adopción de las medidas adecuadas para corregir la irregularidad, si bien, no se podrá aplicar cuando las infracciones sean consideradas **muy graves**, ni cuando el responsable **haya sido apercibido o sancionado anteriormente**. La ley dice: «*excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos... no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras...*»

También **se mejora la tipificación de las infracciones** (nueva redacción) y **se modifica el rango de la cuantía de las multas**, así como **se mejora la tipificación de las cesiones ilícitas**; tomando en consideración el volumen de negocio y el tipo de actividad desarrollada por el infractor, valorándose la diligencia profesional que se le debe exigir (no es lo mismo una gran multinacional que una PYME); en definitiva, la consideración del volumen de negocio y el tipo de actividad permitirá aplicar de una forma más proporcional el régimen sancionador. Cuando las infracciones fuesen cometidas en ficheros de titularidad pública, esta Ley dice que se actuará conforme al régimen disciplinario de las Administraciones Públicas.

## KZgunea cumple 10 años

En 2001, bajo el “*Plan Euskadi en la Sociedad de la Información*”, y como una de las muchas iniciativas dirigidas a la integración de la ciudadanía vasca en la Sociedad de la Información, nació la Red Pública Vasca de Telecentros, más conocida como KZgunea. Por lo que este año celebra su décimo aniversario.

El proyecto KZgunea ha tenido y tiene como finalidad ofrecer un servicio público, gratuito y asistido de acceso a Internet, potenciando la alfabetización de la sociedad vasca en entornos digitales y en Internet. En 2010, KZgunea alcanzó los **357.438 usuarios** registrados.

Desde 2008 KZgunea forma parte de la “*Asociación Comunidad de Redes de Telecentros*”, lo que le ha llevado a realizar numerosas colaboraciones con telecentros de otras comunidades autónomas, así como a conocer nuevas experiencias y nuevos proyectos.

En esta nueva etapa que comienza ahora, KZ hace una apuesta firme por la **Administración Electrónica**, participando, por ejemplo, mediante cursos de formación y planes de difusión, con el proyecto “*Metaposta*” y los certificados digitales de Izenpe. Asimismo, en su labor de capacitación a microempresas en herramientas digitales para la gestión y administración, se considera que las aplicaciones de software libre son una vía imprescindible; por ello, otra de sus grandes apuestas es el **Software Libre**.

De cara al futuro, KZgunea seguirá con su compromiso de apoyar la formación de las personas, a las cuales se les ofrece ya más de 100 cursos interactivos, siendo el de Internet y eAdministración los más solicitados. En cuanto a los certificados en informática e Internet, las **IT-txartelas** siguen teniendo un papel muy destacado. Desde 2002 se han realizado más de 338.600 exámenes. A su vez, las colaboraciones con entidades profesionales y colectivos sociales seguirán siendo una labor prioritaria para KZ, que pondrá a su disposición toda su red de centros (277) para realizar diferentes cursos. Sólo el año pasado fueron más de 5.300 personas las formadas por esta vía.



<http://www.kzgunea.net>  
<http://kzgunea.blog.euskadi.net>

