EUSKO JAURLARITZA
GOBIERNO VASCO

Aurrera!

Nº 37
marzo de 2010

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

La verdad es que, hasta hace unos años, era muy extraño ver a alguien por la calle hablando con un móvil, y ahora, por el contrario, lo extraño es no ver a nadie con un móvil. Algo muy similar puede pasar en breve con los Libros Electrónicos (también llamados eBooks). Esos aparatos que aún no son muy populares pero que, poco a poco, se están dando a conocer y empiezan a ser aceptados. Por ello, y dado que algunos estudios afirman que éste puede ser su año, dedicamos nuestro primer tema a estos aparatos.

Como segundo tema, volvemos a tratar la Seguridad. En este caso, desde el punto de vista legal, tomando para ello como base el recientemente aprobado Esquema Nacional de Seguridad (ENS). Dada la importancia y repercusión que tendrá en las Administraciones Públicas la aplicación de esta nueva norma, creemos que se hace necesario el seguir muy de cerca, entre otros aspectos, su ámbito de actuación y las medidas técnicas a aplicar.

En el apartado *"Alboan"*, tratamos en esta ocasión un tema que puede convertir al Departamento de Educación, Universidades e Investigación en pionero en la gestión de los exámenes escritos. Se trata del proyecto para la digitalización de los exámenes de euskara EGA (Euskararen Gaitasun Agiria), el cual pretende mejorar la gestión de los exámenes que entregan los examinandos y, sobre todo, la gestión que de ellos hacen los distintos tribunales a la hora de corregirlos. Como veremos, se trata de un proyecto muy interesante que seguramente será aplicado también, en breve, por otros organismos, tanto locales como europeos.

Dentro de *"Breves"* os presentamos la herramienta que ha puesto en marcha la Dirección de Innovación y Administración Electrónica, la cual recibe el nombre de "Legesarea", y que pretende convertirse en el espacio colaborativo jurídico en red del Gobierno Vasco.

Por último, y continuando con los aspectos de seguridad pero, en este caso, centrándonos en red de redes, Internet, hacemos referencia a una encuesta realizada por Inteco donde se reflexiona sobre la llamada e-confianza.

Los libros electrónicos

Hasta hace poco, cuando hablábamos de libros y mencionamos la palabra "revolución" o "avance", lo primero que nos venía a la cabeza era la imprenta de Gutenberg[1]. Hoy en día, sin embargo, lo primero que nos viene a la cabeza son los libros electrónicos, ya que, según parece, estos aparatos son el presente (y futuro) de este sector.

DICCIONARIO

[1] **Gutenberg:** Johannes Gensfleisch zur Laden zum Gutenberg nació en Maguncia (Alemania) en 1398 y falleció el 3 de febrero de 1468.

Si bien las primeras imprentas fueron inventadas por los chinos varios siglos antes (las cuales usaban la técnica de impresión llamada xilografía), Gutenberg es considerado por los historiadores como el inventor de la imprenta moderna (o "imprenta de tipos móviles") hacia 1450 en Europa. Esta nueva técnica supuso una gran revolución gracias a la rapidez con la que se podían hacer las copias de un libro, ya que antes, ese mismo trabajo, podía durar varios años.

En 1971, Michael Hart lideró un proyecto llamado *"Gutenberg"* que buscaba digitalizar libros y ofrecerlos gratis.

Empecemos por el principio. ¿A qué llamamos *"libro electrónico"*? Un **libro electrónico** (*electronic book* o ***eBook***) puede ser, sin más, una versión electrónica o digital de un libro. De hecho, los libros que se cuelgan en Internet se pueden considerar libros electrónicos, al igual que cualquier obra literaria contenida en un disquete o CD. Sin embargo, últimamente, se usa esa expresión para identificar los aparatos o dispositivos físicos (*hardware*) creados específicamente para abrir y leer esos libros, los cuales, y según algunos expertos, deberían denominarse *"eBook readers"* o *"lectores de libros electrónicos"*.

Según las previsiones que manejan los fabricantes de estos dispositivos, este año puede ser el inicio de su consolidación en el mercado, y es por ello que vamos a dedicar este artículo a esos aparatos.

DEL PAPEL A LO DIGITAL

Todos sabemos que leer un documento de varias hojas en un ordenador durante mucho tiempo no es cómodo ni saludable, ya que cansa mucho la vista y terminamos con dolor de cabeza (tanto si el monitor es TFT, LCD o de tubo CRT). En el caso de las CRTs, esto se debe, principalmente, al refresco continuo que se produce de la imagen, lo que requiere forzar la vista continuamente.

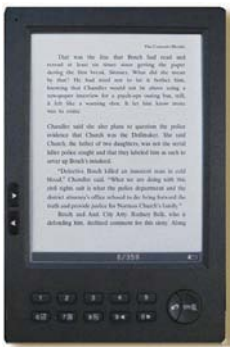
Sin embargo, los llamados *"libros electrónicos"* o *"eReaders"*, gracias a una tecnología conocida como *"tinta electrónica"*, no cansa la vista. La razón es que al no tener retroiluminación, no emiten luz, y, por lo tanto, es como si estuviésemos leyendo una hoja normal.

GUÍA DE REFERENCIA

A continuación os detallamos las principales características a las que debéis prestar especial atención si, finalmente, estáis pensando en comprar un eBook:

En primer lugar, y como siempre debemos hacer a la hora de comprar cualquier aparato, es importante reflexionar sobre nuestras necesidades reales y el uso que le vamos a dar (uso ocasional, diario...)

En este sentido, diremos que los libros electrónicos son ideales para aquellas personas que deben leer muchos documentos, viajeros que no quieren cargarse de libros, estudiantes que preparan una tesis y manejan cientos de volúmenes, profesionales que necesitan consultar documentación técnica, así como para aquellas personas a las que les resulte difícil leer las pequeñas tipografías que a veces utilizan las ediciones en papel.



En segundo lugar, una vez tomada la decisión, los principales **aspectos técnicos** a valorar son estos:

- ✓ **Diseño**: es muy importante valorar su ergonomía, el acabado de las formas, el criterio con el que están dispuesto los botones, su facilidad de uso, etc.
- ✓ **Pantalla**: respecto al tamaño de la pantalla (su parte visible). Además, algunos dispositivos tienen pantallas táctiles, lo cual facilita enormemente el manejo de los menús.

- ✓ **Imagen**: dadas las horas que, seguramente, pasaremos delante de la pantalla, es importante analizar la calidad y el contraste de esa pantalla, la cual se mide en escala de grises. Hoy en día, gracias a la *"tinta electrónica"* se generan páginas estáticas y, por tanto, no se cansa la vista. Además, son legibles incluso a plena luz del día.

"Un aspecto importante son los formatos de texto utilizados, ya que no todos los *eBooks* son capaces de abrir todos los formatos existentes."

- ✓ **Peso**: es recomendable que sea lo más ligero posible, sobre todo si nuestra intención es llevarlo de viaje. Lo normal es que estén entre los 200 y 300 gramos. De hecho, los eBooks han roto uno de los argumentos clásicos en contra de la expansión de la edición electrónica, aquel que dice que «*no te puedes llevar un ordenador a la cama, o a la playa*».
- ✓ **Conectividad**: que disponga de puertos USB o similar. Además, los usuarios valoran positivamente que tenga una buena conexión (WiFi o 3G) para descargar libros directamente de las tiendas on-line. En caso de no tener estas opciones se hará difícil el proceso de actualización de contenidos.
- ✓ **Batería**: dentro de este apartado hay que fijarse en su autonomía (duración). En casi todos los modelos, la batería suele durar más de una semana, debido, principalmente, al uso de la tecnología de "tinta electrónica", la cual consume muy pocos recursos. La razón es que esta tecnología sólo necesita alimentación cuando se pasa de página. Ello nos permite leer entre 8.000 y 9.000 páginas sin necesidad de recargarlo.
- ✓ **Formatos**: este apartado se refiere a los tipos de archivos que es capaz de abrir y leer el eBook. [ver el cuadro *"Los formatos de los archivos"*].

Los formatos de los archivos

Un aspecto importante, y muchas veces olvidado por los usuarios, son los formatos de texto utilizados, ya que todos los eBooks no son capaces de abrir todos los formatos existentes. Los más importantes, a día de hoy, son:

- ✓ **ePub:** formato de Publicación Electrónica. Es el más reciente (creado en 2007) y, junto con el PDF, tiene soporte internacional. Éste es un estándar de código abierto (promovido por el *International Digital Publishing Forum*) que establece los contenidos pero no delimita el formato desde el cual pueden ser leídos, lo que permite que éstos se adapten a distintas pantallas.
- ✓ **mobi, prc:** formatos mobipocket. Fue creado inicialmente para el programa Mobipocket Reader. Se diseñó tanto para libros electrónicos como para dispositivos móviles (PDA o teléfonos) y para el sistema operativo Windows.
- ✓ **pdf:** *(Portable Document Format)* su gran ventaja es su portabilidad y su estandarización ISO. Este formato es uno de los más populares, pero no es el más idóneo para un libro digital, ya que no es repaginable como, por ejemplo, mobipocket o ePub. El objetivo de un documento en PDF es conservar la estructura, disposición y apariencia del documento original, por lo que es mucho más complejo adaptar el texto a las distintas pantallas.
- ✓ **azw:** es el formato creado para el eBook Kindle de Amazon y, por lo tanto, es un formato propietario. El formato AZW está basado en el mobipocket.
- ✓ **lit:** es uno de los formatos más antiguos, creado en 2000, y se lee con Microsoft Reader, una aplicación gratuita de la empresa Microsoft, y que estaba pensado originalmente para su uso en PDAs.

Conversión de formatos: si bien, en general, los libros electrónicos vienen acompañados del software necesario para gestionar y/o convertir unos formatos en otros, es necesario destacar entre las alternativas de software libre para esta tarea el programa "*Calibre*".

Algunas webs de interés:

Illiad (www.irextechnologies.com)
Kindle (www.amazon.com)
Papyre 6.1 / Hanlin V3 (www.jinke.com.cn)
CyBook Gen3 (www.bookeen.com)
Sony Reader PRS-600 (www.sony.com/reader)
Apolo XXI (www.apoloxxi.com)
Grammata (www.grammata.es)
Pixmanía (www.pixmania.com)
Luarna (www.luarna.com)
TodoeBook (www.todoeBook.com)
Casa del Libro (http://casadellibro.publidisa.com)
El Corte Inglés (www.elcorteingles.es)
Elkar (www.elkar.com)
Alberdania (www.alberdania.net)
Google Books (http://books.google.com)
Biblioteca Cervantes (www.cervantesvirtual.es)
Proyecto Gutenberg (www.gutenberg.org)
Librodot.com (www.librodot.com)
Leer-e (http://tienda.leer-e.es)
Blog eBooks Gratis (www.ebooksgratis.eu)

- ✓ **Rendimiento**: la velocidad de interacción con el usuario es otro factor importante a la hora de valorar el uso de un lector. Por ejemplo: tiempo de arranque o puesta en marcha, tiempo necesario para abrir un libro o, más importante aún, tiempo de espera para pasar de una página a otra.
- ✓ **Almacenamiento**: suele ser importante que tenga ranuras para leer tarjetas tipo SD y Compact Flash.
- ✓ **Otras características**: que incorpore la posibilidad de añadir notas a los párrafos (bien como texto o bien como sonido), añadir marcadores, aumentar o disminuir el tipo de letra, que soporte el castellano/euskara y poder entender así los menús de usuario y, además, que éstos sean intuitivos. Se le podrían añadir nuevas funcionalidades actualizando su firmware[2]. Es importante recordar que la tecnología que utilizan los eBooks es aún nueva, y muchos de ellos no soportan características básicas de la imagen como son el movimiento (video) o el color. Por eso, todos los lectores ofertados a día de hoy son, de momento, monocromos.
- ✓ **Precio**: éste es un aspecto muy importante que no hay que olvidar y que debemos valorar en función de nuestras necesidades.

Si tomamos como referencia el precio, podemos afirmar que el mercado de libros electrónicos actual se divide en dos categorías:

- **Modelos básicos**: dispositivos que rondan los 300 euros, tienen pantallas que no suelen superar las 6 pulgadas, no tienen conectividad a la red para descargar libros. (El Papyre 6.1, el Cool-ER o el Inves Book 600 son algunos ejemplos).
- **Modelos de gama alta**: ofrecen pantallas superiores a las 6 pulgadas (a veces táctiles), tienen un diseño más ergonómico, y disponen de conectividad a Internet. (Algunos dispositivos de ejemplo son el iLiad de iRex o el Nook de Barnes & Noble).

De todas formas, un lector de libros electrónicos

TINTA ELECTRÓNICA

Las pantallas de los eBooks están formadas por **tres capas**: una formada por microtransmisores eléctricos, otra formada por una matriz que tiene varios millones de pequeñas cápsulas (que representarán los textos) y, por último, una lámina protectora exterior.

Gyricon, técnica desarrollada por Xerox, es el nombre comercial del primer *ePaper* de la historia, y tenía poca resolución.

E-Ink, desarrollada posteriormente por el Media Lab del Massachussets Institute of Technology, tomando como base las investigaciones realizadas por Xerox, es la que tiene actualmente una mayor resolución. El funcionamiento básico de ambas tecnologías se basa en unas pequeñas cápsulas (esferas) con dos partes, una mitad negra y otra blanca, la primera cargada positivamente y la blanca negativamente, y que se encuentran sumergidas en un gel. Una vez que cada cápsula es estimulada adecuadamente (se le aplica una carga positiva o negativa), se puede conseguir que asciendan (suban) todas las partículas negras, todas las blancas o mitad y mitad, representando en la pantalla un texto o un gráfico. El gel de silicona que les permite girar hace que conserven su posición, incluso, cuando deja de pasar electricidad.

Esto permite a las pantallas que usan tinta electrónica E-Ink mostrar muchos más matices de grises. Gracias a ello, se supera ampliamente la resolución de las TFT o LCD y se consigue un ahorro de energía importante, ya que no emiten iluminación propia (retroiluminación) y no es necesario tampoco ningún voltaje para mantener en pantalla el texto generado.

De todas formas, a día de hoy esta tecnología presenta dos grandes inconvenientes: se ha conseguido desarrollar pantallas a color, pero éstas son muy caras; y, la velocidad de refresco no es todavía muy elevada.

DICCIONARIO

[2] **Firmware**: es el conjunto de instrucciones de un programa informático que se encuentra grabado en una memoria (ROM, flash, EEPROM o similar) y establecen la lógica de bajo nivel que controla los circuitos del eBook.

El firmware forma parte del hardware, ya que se encuentra integrado en la electrónica, pero también está considerado como parte del software, al estar desarrollado bajo un lenguaje de programación. El firmware, por tanto, actúa como mediador entre las órdenes externas que recibe el eBook y los componentes electrónicos.

En definitiva, controla el funcionamiento de los eBooks y, por tanto, lo que son o no son capaces de hacer. Mediante una actualización de este software un fabricante puede añadir nuevas funciones, modificar las ya existentes, restringirlas o, directamente, eliminarlas.

Por lo tanto, el firmware es la forma más rápida y fácil que tenemos para actualizar el eBook.

también tiene **inconvenientes**. El principal, y más importante, es que sus dimensiones son todavía limitadas, lo que dificulta su uso para otras actividades, como puede ser la lectura de periódicos. En este sentido, la gran esperanza de cara al futuro es el "papel electrónico flexible" que también hace uso de la tinta electrónica.

RECURSOS

Una vez vistas sus características técnicas, la pregunta que nos podemos hacer es la siguiente: ¿dónde puedo comprar un eReader y los libros electrónicos[3]?

La respuesta es que, si bien a medida que pasa el tiempo es posible encontrar estos aparatos en más sitios, la tienda más popular para comprarlos es Apolo XXI (www.apoloxxi.com), que distribuye en España casi todos los modelos del mercado. El Papyre (alias Hanlin) también se encuentra en Grammata (www.grammata.es), el Cybook en Pixmanía (www.pixmania.com) y el Sony Reader se puede conseguir en TodoUmpc (www.todoumpc.com). Quien desee un Kindle deberá encargarlo en EEUU, pero siendo consciente de sus limitaciones fuera de ese país. Asus, por su parte, ha desvelado que prepara una serie de lectores que, siguiendo su costumbre, se llamarán Asus eee Book, el cual se pondrá a la venta en breve.

En cuanto a los libros en sí, y a falta de que los grandes editores se decidan a entrar en este mercado, algunas editoriales como Luarna (www.luarna.com) y librerías como TodoeBook (www.todoeBook.com) o Casa del Libro (http://casadellibro.publidisa.com) cuentan con una sección especializada en la venta de libros electrónicos en castellano, mientras que editoriales como Elkar (www.elkar.com) y Alberdania (www.alberdania.net) también empiezan a ofertar libros en euskara. Para contenidos gratuitos puedes recurrir a Grammata, Wikilibros (http://es.wikibooks.org), Google Books (http://books.google.com), la Biblioteca Cervantes (www.cervantesvirtual.es) y, por supuesto, las obras en castellano incluidas en el Proyecto Gutenberg (www.gutenberg.org). El Corte Inglés (www.elcorteingles.es) dispone también en su página web de una sección para adquirir algunas obras. Otras webs de interés son Librodot.com (www.librodot.com), Blog eBooks Gratis (www.ebooksgratis.eu) y Leer-e (http://tienda.leer-e.es).

Según algunas estadísticas, se calcula que, actualmente, hay más de 300.000 libros en castellano libres de derechos que circulan por Internet.

> "Los llamados *«libros electrónicos»* o *«eReaders»*, gracias a una tecnología conocida como *«tinta electrónica»*, no cansan la vista."

De cara al futuro, y según los expertos, el principal problema que plantean estos nuevos dispositivos, a parte del precio actual, es si acabarán siendo **plataformas abiertas** o no, es decir: si cualquier usuario podrá editar un libro para ser leído en uno de estos dispositivos (igual que cualquiera puede hacer un juego para un PC), o si, por el contrario, sólo lo podrán hacer los que tengan una licencia del propietario (como ocurre actualmente con los juegos de las consolas, por ejemplo).

Asimismo, al ser los eBooks nuevos en el mercado deben hacer frente también a ciertos "enemigos" que les van a acechar por el camino, como puede ser el nuevo **tablet** de Apple, presentado recientemente y que recibe el nombre de iPad, ya que éste aporta más funcionalidades (permite navegar por internet, enviar emails, ver fotos/vídeos, escuchar música) y podría usarse como eReader. En este sentido, Apple abrirá una tienda de libros electrónicos llamada iBookStore. ❑

DICCIONARIO

[3] **Libro electrónico:** la Agencia Internacional del **ISBN**, a través del Manual de Usuario (www.isbn-international.org), en su actualización del 5 de febrero de 2002, reconoce los libros electrónicos como sujetos de código ISBN.

El ISSN (*International Standard Serial Number* / Número Internacional Normalizado de Publicaciones Seriadas) y el ISBN (*International Standard Book Number* / Número Internacional Normalizado de Libros) son códigos numéricos de identificación.

El ISSN, un número de 8 cifras, identifica las publicaciones seriadas y el ISBN, de 10 cifras, identifica los libros. Mientras que el ISSN es opcional, el ISBN sí es obligatorio.

El ISSN y el ISBN no son incompatibles: hay publicaciones que pueden llevar ambos, por ejemplo los anuarios, las series de monografías, etc. El ISSN identificará la serie mientras que el ISBN identificará la entrega o volumen.

Esquema Nacional de Seguridad y Manual de Seguridad PLATEA

Después de que el año pasado, 2009, pudimos leer varios borradores del Esquema Nacional de Seguridad, por fin, a principios de 2010, ha visto la luz el Real Decreto que regula dicho Esquema; a la par, también está a punto de aprobarse nuestro Manual de Seguridad PLATEA[4]. De todo ello se va a hablar en las próximas líneas.

DICCIONARIO

[4] **PLATEA:** acrónimo de **PLA**taforma **TE**cnológica para la e-**A**dministración, que no es sino la infraestructura tecnológica de base para el desarrollo de la e-Administración del Gobierno Vasco, y que es de obligado uso en los desarrollos de aplicaciones relacionadas con la e-Administración.

Comprende diferentes componentes elementales que, juntos, constituyen una Plataforma Tecnológica de base para ofrecer los servicios de Administración Electrónica, como son:

- La infraestructura de integración (pasarela de pagos, framework GEREMUA, libro de registro telemático, etc.)
- Las herramientas de gestión de contenidos, portales y ejes de catalogación.
- Los sistemas de infraestructura de tramitación telemática.
- Los sistemas de infraestructura de gestión documental.

El pasado 29 de enero se publicó en el Boletín Oficial del Estado el Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** (en adelante, **ENS**) en el ámbito de la Administración Electrónica, asimismo, en breve se publicará la Orden por la que se aprueba el **Manual de Seguridad** (en adelante, **MSPlatea**) para el mantenimiento de la seguridad de la información de la Administración general de la CAPV y sus Organismos Autónomos en el entorno de las aplicaciones informáticas que sirven de soporte a la tramitación telemática (e-Administración).

LA LEY 11/2007 Y EL ENS

El ENS se crea en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP). En su artículo 42, punto 2, dice textualmente: "*el Esquema Nacional de Seguridad* ***tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos*** *en el ámbito de la presente Ley, y* ***está constituido por los principios básicos*** *(fundamentos que deben regir toda acción orientada a asegurar la información y los servicios)* ***y requisitos mínimos*** *(exigencias necesarias para asegurar la información y los servicios)* ***que permiten una protección adecuada de la información***", asimismo, se ha elaborado, como dicta la Ley, con la participación de todas las administraciones, siendo aprobado por Real Decreto, teniendo en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas y los servicios electrónicos ya existentes. También se debe tener en consideración el uso de estándares abiertos y, de forma complementaria, aquellos que sean de uso generalizado por la población (estándares de facto). A destacar que este ENS se regula en dicha Ley junto con el Esquema Nacional de Interoperabilidad (ENI).

Cabe destacar el objetivo de esta Ley 11/2007, que se puede resumir, básicamente, en la existencia de, por un lado, un derecho (entre muchos otros), y por otro lado, de una obligación (entre muchas otras); **el derecho de la ciudadanía y de las empresas a comunicarse con las Administraciones Públicas a través de medios electrónicos, informáticos y telemáticos, y del deber u obligación de estas últimas, las Administraciones, a que ésto realmente sea así**.

> "El ENS tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información."

Es por todo ello por lo que con la única finalidad, dentro del ámbito de esta Ley, de **crear las condiciones de confianza necesarias en el uso de estos medios electrónicos**, se presenta este ENS.

DECRETO 232/2007 Y MSPlatea

En cuanto al MSPlatea, se puede decir que sigue un camino paralelo al ENS, esto es, se crea por orden del Decreto 232/2007, de 18 de diciembre, por el que se regula la utilización de medios electrónicos, informáticos y telemáticos en los procedimientos administrativos, también conocido como Decreto de Medios EIT. Este Decreto, en su Capítulo VII, que está dedicado en parte al Manual de Seguridad, dictamina que éste «***sirve para dotar al sistema de la adecuada homogeneidad, al establecer las medidas de seguridad de carácter general, de índole técnica y organizativa, dirigidas a asegurar el cumplimiento de una serie de garantías***

(autenticidad, integridad, confidencialidad, disponibilidad y conservación de la información).» Una vez publicado el Decreto de Medios EIT, desde la Dirección de Informática y Telecomunicaciones (DIT) se decidió empezar a trabajar en la elaboración, tal y como especifica dicho decreto, de un borrador con el objetivo de construir el Manual de Seguridad en el ámbito de los servicios y sistemas que utilizan la plataforma tecnológica de la e-Administración.

Este trabajo no se realizó de espaldas al ENS, todo lo contrario, en su elaboración se han tenido en cuenta los diferentes borradores del ENS que han sido publicados durante el pasado año 2009.

GARANTÍAS/DIMENSIONES A SALVAGUARDAR

El MSPlatea habla de **garantías**, mientras que el ENS se refiere a **dimensiones de seguridad.**

- **Garantías de Seguridad**

Por un lado, en lo que respecta al **MSPlatea** para la elaboración de las aplicaciones informáticas que sirvan de soporte a la tramitación telemática, éste **contiene medidas de carácter general, de índole técnica y organizativa** (estas últimas no son sino una declaración concisa de directrices de la alta gerencia), **que aseguren el cumplimiento de una serie de garantías**, que son las siguientes:

- ✓ ***Autenticidad****: característica por la que se garantiza la identidad del usuario que origina una información, permite conocer con certeza quién envía o genera una información específica.*
- ✓ ***Integridad****: característica que asegura que la información no se ha transformado ni modificado de forma no autorizada durante su procesamiento, transporte o almacenamiento, detectando fácilmente posibles modificaciones que pudieran haberse producido.*
- ✓ ***Confidencialidad****: característica que previene contra la puesta a disposición, comunicación y divulgación de información a individuos, entidades o procesos no autorizados.*
- ✓ ***Disponibilidad****: característica que asegura que los usuarios autorizados tienen acceso a la información cuando se requiera y previene contra intentos de denegar el uso autorizado a la misma.*
- ✓ ***Conservación de la información****: en un sentido amplio, es el conjunto de procesos y operaciones que se conjugan para estabilizar y proteger los documentos del deterioro. A la hora de hablar de la gestión de recursos digitales, sea cual sea su forma o función, se debe tener en cuenta todas las etapas que componen el ciclo de vida de los documentos para aplicar las medidas de preservación lo antes posible. Por lo tanto, más que a una característica intrínseca de la información se hace referencia a la gestión del ciclo de vida de la información.*

Si bien el Decreto de Medios EIT sólo menciona estas cinco garantías, en el MSPlatea se ha añadido otra más:

- ✓ ***Trazabilidad****: característica de la información que asegura el conocimiento de aspectos clave de las operaciones de creación, modificación y consulta, tales como: ¿quién realizó la operación?, ¿cuándo se realizó la operación?, ¿qué resultados tuvo la operación?*

(Definiciones de las garantías extraídas del MSPlatea).

- **Dimensiones de seguridad**

Por otro lado, el **ENS** indica las siguientes dimensiones de seguridad: **Disponibilidad, Autenticidad, Integridad, Confidencialidad y Trazabilidad**.

El hecho es que una información o servicio puede verse afectada en una o más dimensiones de seguridad, por lo que el ENS categoriza las dimensiones afectadas con uno de los siguientes niveles:

- ✓ **Bajo** (**perjuicio limitado** sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados).

PRINCIPIOS BÁSICOS DEL ENS:

- Seguridad integral
- Gestión de riesgos
- Prevención, reacción y recuperación
- Líneas de defensa
- Reevaluación periódica
- Función diferenciada

REQUISITOS MÍNIMOS DEL ENS:

- Organización e implantación del proceso de seguridad
- Análisis y gestión de los riesgos
- Gestión de personal
- Profesionalidad
- Autorización y control de los accesos
- Protección de las instalaciones
- Adquisición de productos
- Seguridad por defecto
- Integridad y actualización de sistemas
- Protección de la información almacenada y en tránsito
- Prevención ante otros sistemas de información interconectados
- Registro de actividad
- Incidentes de seguridad
- Continuidad de la actividad
- Mejora continua del proceso de seguridad

- **Medio** (**perjuicio grave** sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados).
- **Alto** (**perjuicio muy grave** sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados).

"La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema."

El propio ENS describe qué es un perjuicio limitado, grave y muy grave. Los perjuicios son causado por **incidentes de seguridad**[5] .

ENS Y LAS GUÍAS DE SEGURIDAD

El CCN fue creado el año 2004, a través del Real Decreto 421/2004, adscrito al Centro Nacional de Inteligencia (CNI). Dicho Centro se encarga de elaborar y difundir las guías de seguridad (CCN-STIC) de las tecnologías de la información y las comunicaciones (en adelante, TIC), además, ante incidencias de seguridad el CNN-CERT (ver "¿Qué es un CERT?") es el equipo técnico de apoyo y coordinación para las Administraciones Públicas en lo referente a estas incidencias. El ENS no hace sino remarcar esta labor del CNN en su artículo 29.

ENS, ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y LAS AUDITORÍAS

En cuanto a la Adquisición de productos de seguridad, el ENS dedica un artículo (artículo 18) en el que explica que cuando se adquieran productos de seguridad de las TIC para las Administraciones públicas se valorarán positivamente aquellos que tengan asociada alguna certificación de seguridad relacionada con el objeto de su adquisición (certificación de acuerdo con las normas y estándares de mayor reconocimiento internacional), es más, en el anexo V del propio ENS propone un modelo de cláusula administrativa particular para poder ejercitar este hecho.

Por lo que respecta a las Auditorías de Seguridad, el ENS define dos niveles de

¿QUÉ ES UN CERT?

Un **CERT** es el acrónimo de *Computer Emergency Response Team;* definen un grupo o conjunto de personas que se dedican a implantar y gestionar medidas tecnológicas para mitigar el riesgo de ataques contra los sistemas de la comunidad a la que se proporciona el servicio, es decir, ofrece servicios de respuestas ante incidentes y gestión de seguridad, también se le conoce por las siglas CSIRT (*Computer Security and Incidente Response Team*). Existen distintos foros y organizaciones que coordinan a los diferentes CSIRT, siendo su objetivo el divulgar medidas tecnológicas que mitiguen el riesgo de ataques y compartir información sobre vulnerabilidades y ataques.

CCN-CERT: es un CERT gubernamental español creado a principios del 2007, no es sino la capacidad de respuesta a incidentes de seguridad de la información del Centro Criptológico Nacional (CCN) dependiente del Centro Nacional de Inteligencia (CNI).

CCN-STIC: son un conjunto de normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las Tecnologías de la Información y de las Comunicaciones (TIC) en la Administración, elaboradas por CCN-CERT.

Durante el pasado año 2009 se han actualizado-publicado 20 nuevas guías, como, por ejemplo, la guía de Dispositivos Biométricos de Iris (CCN-STIC 491), la guía RFID[6] (CCN-STIC 443) o la guía de Seguridad en Bluetooth[7] (CCN-STIC 418).

Las guías actualizadas se dividen en los siguientes campos: políticas (Serie 000), procedimientos (Serie 100), normas (Serie 200), instrucciones técnicas (Serie 300), guías generales (Serie 400), guías entornos Windows (Serie 500), guías otros entornos (Serie 600) e informes técnicos (Serie 900). Los responsables de seguridad TIC de las administraciones pueden acceder a ellas y a otros servicios a través del portal del CCN-CERT en Internet **www.ccn-cert.cni.es**.

DICCIONARIO

[5] **Incidentes de seguridad:** sucesos inesperados o no deseados con consecuencias en detrimento de la seguridad del sistema de información.

[6] **RFID:** acrónimo de ***R**adio **F**requency **ID**entification*, identificación por radiofrecuencia; la idea fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

[7] **Bluetooth:** especificación industrial para redes inalámbricas de área personal que posibilita el intercambio de datos entre dispositivos mediante un enlace por radiofrecuencia.

auditoría, uno para los sistemas de categoría Básica, y otro para los sistemas de categoría Media y Alta.

Estos primeros (categoría Básica) no necesitarán realizar una auditoria, bastando con una autoevaluación realizada por el propio personal, siendo los informes resultantes analizados por el responsable de seguridad competente; para los segundos (categoría Media y Alta) se exige un informe de auditoría que determine sobre el grado de cumplimiento del R.D. que regula el ENS, identificando deficiencias y sugiriendo medidas correctoras, debiendo incluir los criterios metodológicos de auditoría utilizados.

MANUAL DE SEGURIDAD PLATEA

Como ha quedado claro, el ámbito de este Manual de Seguridad son las aplicaciones informáticas que sirven de soporte a la tramitación telemática (e-Administración), tratando la seguridad desde un punto de vista general (hardware, software, redes, datos, personas…). Asimismo, este Manual se divide en dos apartados:

- ✓**Política de seguridad**: *declaración de alto nivel de objetivos, directrices y compromiso de la Administración general de la Comunidad Autónoma del País Vasco y sus Organismos Autónomos para acometer la gestión de seguridad de la información en los medios electrónicos, informáticos y telemáticos utilizados en la prestación de servicios públicos.*
- ✓**Normativa de seguridad**: *medidas de seguridad de obligado cumplimiento. Es un compendio del conjunto de normas que soportan los objetivos recogidos en la política de seguridad de la información. En este nivel se describen los objetivos de seguridad y se anticipan las reglas generales de obligada adopción. Este apartado es el objetivo final perseguido por el Manual.*

Las directrices de la política de seguridad del Manual han sido definidas de acuerdo con el estándar **ISO/IEC 27001:2005**[8], basado en **dominios** (equiparables con los requisitos de seguridad del ENS), **objetivos de control** y **controles** (criterios o medidas de seguridad).

Dentro de la Gestión de la Seguridad el Manual dicta establecer un "Sistema de gestión de la Seguridad de la Información" (SGSI) con el objetivo de establecer un proceso de mejora continua de la seguridad.

DESARROLLO NORMATIVO DEL MSPLATEA

Las medidas de seguridad (36 están recogidas en el Manual) viene implantadas en fichas, que se agrupan en 12 objetivos:

- *Política de seguridad (M1)*
- *Aspectos organizativos de la seguridad de la información (M2)*
- *Gestión de activos (M3)*
- *Seguridad ligada a los recursos humanos (M4)*
- *Seguridad física y ambiental (M5)*
- *Gestión de comunicaciones y operaciones (M6)*
- *Control de acceso (M7)*
- *Adquisición, desarrollo y mantenimiento de los sistemas de información (M8)*
- *Gestión de incidentes de seguridad de la información (M9)*
- *Gestión de la continuidad del servicio (M10)*
- *Cumplimiento (M11)*
- *Gestión de la seguridad (M12)*

Asimismo, cada ficha, a la vez que especifica el objetivo al que se corresponde, tiene un código (referencia unívoca), un nombre de la medida, un alcance (categorización) que en la ficha se especifica en función de colores (bajo-color verde, medio-color amarillo y alto-color rojo), un campo garantías, que indica las garantías de seguridad que están cubiertas por esa medida y una parte explicativa, dividida en tres campos:

- Propósito: define el objetivo de la medida de seguridad
- Exposición: desarrolla la medida de seguridad en sí
- Actividad: si la medida lo requiere, tarea o tareas a realizar.

Este Manual de Seguridad es un documento vivo, es decir, se debe evaluar, actualizar, modificar y adaptar en la medida en que los riesgos a los que se ven expuestos los Sistemas de Información de tramitación telemática y los sistemas de protección evolucionan. ❑

DICCIONARIO

[8] **ISO 27001:2005:** estándar internacional certificable para implementar, dentro de un alcance determinado y definido, un Sistema de Gestión de Seguridad de la Información (SGSI -ver definición en el boletín AURRERA! nº 24-); está centrado en mitigar el riesgo al que están sujetos los activos de información, previa realización de un análisis y evaluación del riesgo.

El objetivo es asegurar la continuidad de las operaciones de la organización y minimizar la posibilidad de que una amenaza haga daño a los activos de dicha organización.

Está basado en la gestión de riesgos de los activos de la organización, los cuales se pueden tratar de cuatro modos:

✓Reducir el riesgo

✓Aceptar el riesgo

✓Transferir el riesgo

✓Evitar el riesgo

ALBOAN:

Digitalización de los exámenes EGA

Departamento de Educación, Universidades e Investigación

"Una vez se ponga en marcha el proyecto, el Departamento de Educación, Universidades e Investigación será pionero en la gestión digital de los exámenes escritos."

dokusi
Dokumentu kudeaketa sistema integrala
Sistema integral de gestión documental

ALTE, acrónimo de *Association of Language Testers in Europe*, es una organización no gubernamental que ha colaborado con el Consejo de Europa en el establecimiento del sistema común europeo de niveles para los conocimientos de idiomas, el cual conocemos y utilizamos hoy en día.

Esta organización, fundada en 1990, está compuesta por distintas instituciones que administran exámenes de idiomas, es más, actualmente muchos de los más importantes entes certificadores de la competencia lingüística están representados en ALTE. De hecho, en estos momentos, cuenta con 31 miembros que administran exámenes de 26 lenguas, pudiendo destacar, entre todos ellos, los siguientes: la University of Cambridge ESOL Examinations del Reino Unido, el Goethe-Institut de Alemania; la Generalitat de Catalunya, la Xunta de Galicia y el Instituto Cervantes. En este mismo sentido, indicar que el euskara también está representado es este foro desde el año 2000, en este caso, a través del certificado EGA del Departamento de Educación, Universidades e Investigación del Gobierno Vasco.

TENDENCIAS EUROPEAS

La Dirección de Innovación Educativa del Departamento de Educación, Universidades e Investigación, y, en concreto, el Servicio de Euskara es el órgano encargado de gestionar los exámenes relativos al euskara, más conocidos como EGA *(Euskararen Gaitasun Agiria),* desde el año 1982.

Este Departamento, como miembro de pleno derecho de ALTE, asiste periódicamente a las distintas reuniones que se organizan. Gracias a ello, los responsables del departamento, viendo cuáles son las ideas y/o tendencias de futuro que se van planteando en estos foros europeos, y teniendo en cuenta, además, las grandes posibilidades que ofrecen actualmente las nuevas tecnologías, han tomado la decisión de digitalizar los exámenes de todas aquellas personas que se presenten al examen EGA.

EL EXAMEN EGA

Como bien conocen muchos de nuestros lectores, el examen EGA en su modalidad escrita consta de dos subapartados:

- ✓ Una primera parte de corrección objetiva, se aplica mediante un lector óptico;
- ✓ En una segunda parte el examinando debe escribir una serie de textos (*idazlanak* y *berridazketak*) y, por lo tanto, de corrección personal, no mecánica, por parte del Tribunal.

Como dato de referencia, y tomando en su conjunto las 2 convocatorias que el Departamento organiza cada año, indicar que en la prueba escrita se gestionan alrededor de 7.500 exámenes y cada examen entregado, de media, contiene 6 hojas.

Haciendo un poco de historia, el procedimiento que se ha venido usando para la gestión y corrección de los exámenes ha sido el siguiente:

Hasta el **año 2009**, cada examen entregado era corregido por un único evaluador del Tribunal, y, adicionalmente, un porcentaje de todos ellos era corregido una segunda vez por otro evaluador,

proceso que recibe el nombre de "doble corrección".

Esta forma de trabajar, por tanto, obligaba a manejar el examen o documento original y distintas fotocopias del mismo, lo cual hacía que la gestión del documento escrito fuese compleja. Además, no se puede olvidar el coste que suponía realizar todas las copias, repartirlas (transporte) y gestionar su confidencialidad.

En la segunda convocatoria del **año 2009** se realizó, por primera vez, la doble corrección para el 100% de los exámenes presentados, es decir, cada examen entregado fue revisado y corregido por dos evaluadores del Tribunal de forma independiente.

Posteriormente, continuando con la decisión de mejorar el procedimiento empleado, este mismo **año 2010**, y, en concreto, en la primera convocatoria que ya se está desarrollando, se ha decidido realizar la primera prueba masiva usando el nuevo procedimiento de digitalización para el 100% de los exámenes que se entreguen. La decisión de digitalizar los exámenes evitará al Departamento de Educación, Universidades e Investigación y a los distintos tribunales la gestión de una extensa documentación en formato papel.

DOKUSI

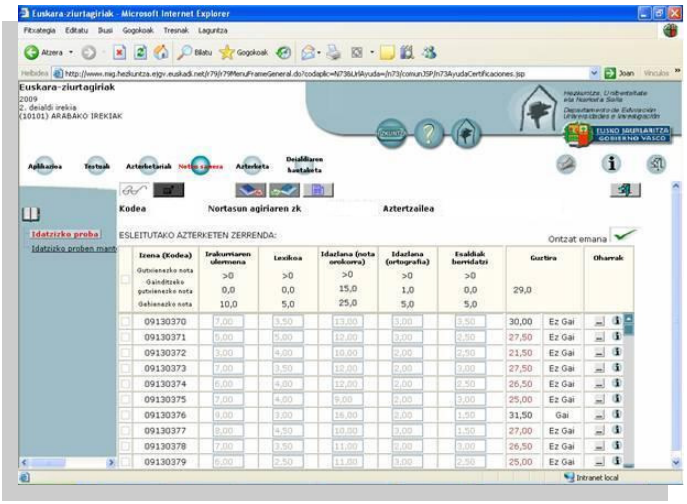
Desde un punto de vista técnico, cabe indicar que a la hora de realizar el escaneo de los exámenes (proceso de digitalización) se utilizará un **código de barras** para identificar cada uno de los exámenes. Con ello se podrá indicar dónde empieza y dónde termina un examen. Esto, además, garantizará la seguridad de que no se extravía o mezcla ninguna de sus hojas y, sobre todo, el anonimato del examinando. Aspecto éste último muy importante para garantizar la confidencialidad durante el proceso de corrección.

Todos los exámenes entregados, una vez digitalizados (escaneados), serán almacenados dentro del sistema de gestión documental del Gobierno Vasco, más conocido como **dokusi**, donde serán albergados por un periodo determinado, quedando de esta forma a disposición de los miembros del Tribunal en un plazo no superior a 48 horas. Cabe señalar que alrededor de 150 profesores en total forman parte de los tribunales en cada convocatoria.

Dentro de la nomenclatura de **dokusi**, la serie documental (fondo.sección.serie) que va a identificar a estos documentos será KL.HZ.EGA

Cada miembro del Tribunal podrá acceder al sistema **dokusi**, y por lo tanto a los exámenes, a través de la aplicación departamental N73 *"Publicación de certificaciones de euskara"*, para lo cual cada uno de ellos tendrá que hacer uso de una clave personal. Una vez identificado, entre otras cosas, el evaluador podrá ver cuántos exámenes le han correspondido para corregir, proceder a su revisión, imprimirlos, y, lo más importante para los examinandos, reflejar la nota final de cada examen.

Debido al procedimiento que se empleaba hasta ahora, los exámenes que entregaban los examinandos debían ser gestionados por distintas personas para guardarlos en un lugar seguro, transportarlos y hacer las distintas fotocopias que posteriormente se entregaban al Tribunal, el examen original podía desgastarse y sufrir algún desperfecto. Por ese motivo, los responsables del Departamento de Educación, Universidades e Investigación, gracias a esta nueva iniciativa, pretenden, en primer lugar, simplificar la gestión de los exámenes en formato papel, evitar su desgaste y su traslado; y, en segundo lugar, facilitar la doble-corrección por parte del Tribunal. Tarea ésta que a partir de ahora se quiere aplicar al 100% de los exámenes en todas las convocatorias.



Esta nueva iniciativa, por tanto, tiene el objetivo de seguir mejorando la gestión interna de los propios exámenes, e intentar ser un referente dentro de este ámbito. Una vez se ponga en marcha el proyecto, el Departamento de Educación, Universidades e Investigación será pionero en la gestión digital de los exámenes escritos. ❑

"Cada miembro del Tribunal podrá acceder al sistema dokusi, y por lo tanto a los exámenes, a través de la aplicación departamental N73 (Publicación de certificaciones de euskara)."

[+info]:

ALTE

(Association of Language Testers in Europe):

www.alte.org

¡¡BREVES!!

Nº 37

marzo de 2010

Legesarea

La Dirección de Innovación y Administración Electrónica ha habilitado recientemente un espacio colaborativo en red (basado en la herramienta corporativa SharePoint de Microsoft) para todo el personal jurídico del Gobierno Vasco, el cual ha sido bautizado como "Legesarea".

El objetivo de esta nueva iniciativa es establecer un espacio colaborativo de conocimiento compartido destinado a los operadores jurídicos con responsabilidad en el procedimiento de elaboración de disposiciones de carácter general, no obstante, el espacio colaborativo nace con voluntad de extenderse a otros ámbitos y materias jurídicas.

Todos los participantes o miembros con acceso a este SharePoint tendrán como principales tareas las siguientes: en el caso del Departamento promotor de una iniciativa legal deberá hacer público en el portal Legesarea la **Orden de Iniciación** correspondiente. El resto de los Departamentos, por su parte, deberán realizar todas aquellas consideraciones jurídicas que estimen oportunas en relación a sus ámbitos de actuación antes de la **Orden de Aprobación Previa**.

Este entorno de trabajo dispone de varios apartados, entre los cuales podemos destacar los siguientes:

- ✓ Tablón y Foros: lugar donde hacer públicas las ideas y/o sugerencias.
- ✓ Calendario: agenda donde registras las reuniones y/o eventos que se celebren.
- ✓ Anuncios: notificación de las novedades más significativas para los participantes en legesarea.
- ✓ Biblioteca: repositorio donde se guardarán todos los documentos.

legesarea
Espacio Colaborativo Jurídico en Red
Lankidetza Juridikorako Sareko Gunea

En definitiva, mediante esta nueva herramienta se pretende agilizar la elaboración y desarrollo de todas aquellas iniciativas legales que se llevan a cabo en los Departamentos del Gobierno Vasco.

Web del portal: http://elkarlan.jakina/webguneak/legesarea

Nivel de e-confianza

El Instituto Nacional de Tecnologías de la Información (INTECO) publicó el pasado diciembre un ***"Estudio sobre el fraude en Internet"***, visto este fraude como una amenaza que impide la consolidación de la confianza (e-confianza) por parte del usuario en la utilización de estos medios electrónicos, informáticos y telemáticos.

El resultado a destacar es que **la confianza del usuario en el medio Internet para realizar operaciones económicas es de un nivel alto**, por ejemplo, seis de cada diez usuarios muestran mucha o bastante confianza en la utilización de la banca electrónica, si bien, los usuarios que han sufrió un fraude con un perjuicio económico asociado suelen cambiar las prácticas de uso e incluso abandonar el servicio.

El informe apunta que se ha detectado un **repunte del *phishing*** (se intenta adquirir información confidencial de forma fraudulenta), si bien al principio el fraude se basaba en ingeniería social (engañar al usuario para conseguir información confidencial, por ejemplo, a través de una llamada de teléfono o mediante el envío de un simple correo electrónico), al día de hoy se introducen otros componentes, como **personalizar las herramientas** en función de la persona objeto del fraude (por ejemplo, se utiliza el ***whaling***, que no es sino una evolución del *phishing* en la que el ciberdelincuente recaba información de contacto de personas de influencia y alto poder adquisitivo, como empresarios, autoridades y gerentes, habitualmente a través de la información contenida en redes sociales, para, posteriormente, remitir un correo electrónico personalizado en el que se le trata de engañar para robar credenciales de cuentas bancarias personales o de la propia compañía), **aumentar la complejidad** (utilización de herramientas sofisticadas) y **profesionalizar el fraude** (mediante bandas organizadas).

Para más información: www.inteco.es