EUSKO JAURLARITZA
GOBIERNO VASCO

nº 47
Marzo de 2014

Aurrera!

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

Hoy en día, existen dispositivos (portátiles o teléfonos de última generación) que son capaces de identificar mediante sus huellas dactilares a sus dueños o dueñas. Las características biométricas de cada persona son únicas y, por ese motivo, muchos expertos creen que en breve se utilizarán como mecanismo para identificarnos y validar trámites que realizamos habitualmente. De todas formas, los sistemas que capturan y gestionan nuestras características biométricas (la huella dactilar, el olor corporal, la voz o la firma manuscrita) deben cumplir una serie de medidas de seguridad que garanticen en todo momento la privacidad de las personas. Todo ello lo analizamos en el artículo titulado *La firma biométrica*.

En el artículo titulado *eFactura en el Sector Público* os informamos de cuál es la situación de la Facturación electrónica, tanto desde el punto de vista normativo (estándares, normas...) como organizativo. Y, sobre todo, os adelantamos las fases que tiene previsto llevar a cabo el Gobierno Vasco (a través de EJIE) para adoptar la Factura electrónica.

Dentro del apartado *Alboan*, os presentamos en esta ocasión la llamada *EJGVbilduma* o *GaleríaEJGV*, la cual alberga una nueva serie de elementos gráficos (ilustraciones) que podremos usar en cualquier presentación corporativa que tengamos que realizar.

Gracias a los nuevos dispositivos tecnológicos (*smartphones*, *tablets*...) de los que disfrutamos hoy en día, el uso de las redes sociales se ha hecho tan habitual en cualquier ámbito que muchos usuarios suelen hacer caso omiso de las amenazas o peligros que puede conllevar compartir, por ejemplo, información personal en Internet, o bien no tener actualizado su dispositivo, hasta que es demasiado tarde. Por esa razón, la DIT ha elaborado una sencilla guía que resume las recomendaciones mínimas que cualquier persona debería tener en cuenta para no llevarse una sorpresa desagradable. Desde aquí os animamos a que le echéis un vistazo.

Asimismo, hemos incluido una referencia sobre la Agencia Vasca de Protección de Datos (AVPD), puesto que este año celebra su X aniversario.

La firma biométrica

Hasta ahora, muchos de los documentos que firmábamos estaban en formato papel. Sin embargo, y desde hace un tiempo, algunos establecimientos nos hacen firmar en unos dispositivos digitales que capturan nuestra firma y la incorporan al documento. A raíz de ello, muchos expertos han empezado a reflexionar sobre la validez o no de estos sistemas y sobre la seguridad jurídica que nos ofrecen.

Hoy en día muchos sistemas son capaces de identificar a una persona en base a alguna de sus **características físicas** (o biométricas[1]), siendo la más famosa la huella dactilar; aunque cada día surgen más dispositivos que son capaces de analizar nuevos rasgos biométricos diferentes a la huella.

Tanto es así que los elementos biométricos asociados a una persona se pueden clasificar en dos grandes grupos: los relacionados con sus características fisiológicas y los relacionados con su comportamiento.

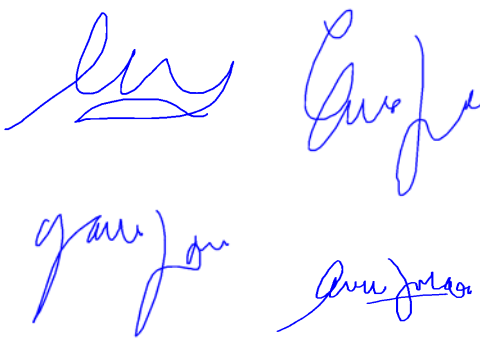
Características biométricas **fisiológicas**:

- Huella dactilar
- Reconocimiento del iris
- Morfología facial
- Geometría de la mano
- Olor corporal

Características biométricas de **comportamiento**:

- Reconocimiento de la voz
- Ritmo de las pulsaciones del teclado del PC
- Forma de caminar
- Reconocimiento de la firma manuscrita

Según algunos expertos, el primer antecedente de *firma biométrica* se podría situar en China, hace ahora más de mil años, cuando los alfareros empezaron a incluir sus huellas dactilares en los productos que realizaban como símbolo o firma del trabajo realizado.



FUNCIONAMIENTO

Los sistemas biométricos, en general, se componen básicamente de **tres elementos**:

1. **Sensor**: Es el dispositivo que captura los rasgos o las características biométricas de una persona.
2. **Repositorio**: Es la base de datos donde se almacenan los *patrones biométricos* que se usarán más tarde para determinar, por ejemplo, si una huella o una voz pertenece a una persona.
3. **Algoritmo**: Es el conjunto de cálculos matemáticos y estadísticos que se usa para comparar distintos patrones y decidir si pertenecen o no a la misma persona.

Pero ¿cómo funcionan exactamente estos sistemas? ¿qué datos capturan? y ¿cómo determinan si una firma es nuestra? El procedimiento consta de 4 pasos:

1. **Buscar coincidencias**: Se comparan las distintas muestras biométricas recogidas y se establece el grado de similitud entre ellas.
2. **Calcular el grado de afinidad**: Se obtiene un **valor numérico** que indica el **grado de afinidad** entre las muestras existentes. Los sistemas biométricos se basan en algoritmos de búsqueda de coincidencias que, al final, generan una **puntuación**. Ese valor representa el grado de coincidencia entre la muestra a validar y la que tenemos almacenada en el repositorio (base de datos). Por ejemplo, los métodos de verificación tradicionales (contraseñas, PINs, etc.) son binarios, es decir, ofrecen una respuesta de *verdadero* o *falso*.

DICCIONARIO

[1] **Biometría:** (del griego *bios* vida y *metron* medida) es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o rasgos físicos.

La «autentificación biométrica» es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de una persona, para verificar su identidad.

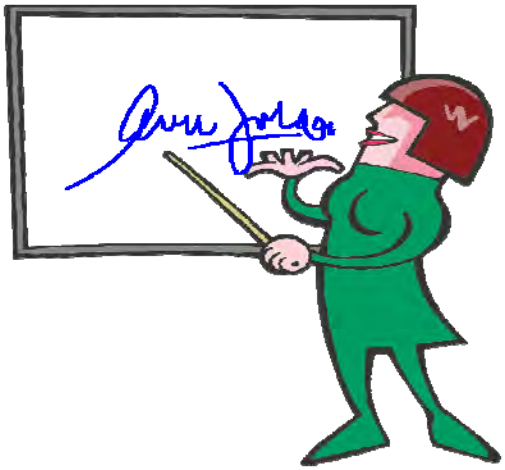
(Fuente: Wikipedia)

Para más información os recomendamos el documento elaborado en 2011 por **Inteco** (Instituto Nacional de Tecnologías de la Comunicación) titulado *Estudio sobre las tecnologías biométricas aplicadas a la seguridad* (edición de 2011)

http://www.inteco.es

http://observatorio.inteco.es

3. **Comparar con el *valor umbral***: El *umbral* es un número predefinido, normalmente por el Responsable del sistema, que establece el grado de correlación necesario para que una muestra se considere *similar* a otra. Si la puntuación resultante de la comparación de muestras supera ese *umbral*, las muestras se consideran coincidentes.
4. **Obtener una conclusión**: El resultado final de la comparación entre la puntuación y el umbral predefinido puede ser: *coincidencia*, *no coincidencia* e *inconcluyente* (el sistema no es capaz de determinar si la muestra recogida es coincidente o no)[2].



APLICACIONES

Los datos biométricos basados en las **características físicas estáticas** de una persona, según los expertos, presentan serios problemas a la hora de ser aplicados en la firma electrónica de documentos.

Por un lado, no constituyen por sí una muestra clara de voluntad, ya que alguien podría captar y usar los *datos* (huellas dactilares...) de una persona sin que ello signifique necesariamente que esa persona haya aceptado voluntariamente el contenido del documento que se va a firmar.

Y, por otro lado, no hay posibilidad de cambiar o repudiar esos *datos* (huella dactilar...), lo que limita la flexibilidad del sistema. La razón es que en caso de fallo o robo de los datos, por ejemplo, el sistema fallará siempre y se perderá la posibilidad de utilizar ese sistema para otras ocasiones futuras.

Por el contrario, la firma biométrica basada en los **rasgos identificativos de comportamiento** (como puede ser la firma manuscrita o rúbrica) implica una voluntad y ofrece la flexibilidad necesaria, ventajas todas ellas por las que es el sistema preferido desde hace varios siglos para la firma de documentos.

La firma escrita tiene la cualidad de ser *dinámica*, lo cual es una característica muy importante, ya que ésta constituye la forma perfecta de documentar un **acto voluntario**. Además, permite identificar al autor, es decir, permite unir una firma a una única persona.

Tanto es así que, hoy en día, en muchos bancos y centros comerciales, a la hora de otorgar nuestra autorización o conformidad a una compra, ya no firmamos un papel (tal y como hacíamos hasta hace no mucho tiempo), sino que firmamos sobre una tableta o dispositivo similar, el cual se encarga de capturar y almacenar nuestra firma en una base de datos. El problema en estos casos, según distintas opiniones, es que, normalmente, no vemos en pantalla el texto del documento que estamos firmando o autorizando, y, por lo tanto, no tenemos la certeza de estar firmando el documento adecuado; de la misma forma, tampoco sabemos exactamente dónde ni cómo se almacena nuestra firma; qué medidas de seguridad se aplican para evitar posteriormente un uso fraudulento de la misma, etc.

Por todo ello, existen distintos foros donde se están empezando a plantear preguntas de este tipo: ¿qué validez tiene esa firma? ¿es equiparable, por ejemplo, a la firma electrónica reconocida (p.ej. DNI electrónico)? ¿se puede utilizar dicha firma como prueba en un juicio?[3]

«Es fundamental que la generación y captura de la *firma biométrica* cumpla estrictamente las adecuadas medidas de seguridad»

En definitiva, muchos expertos consideran que la *firma biométrica* sólo será válida si el sistema que la gestiona cumple una serie de estrictos criterios que, en muchos casos, no se cumplen.

EL PROCESO DE CAPTURA

En referencia a la seguridad de los dispositivos o *tabletas* de firma, es necesario indicar que pueden ser de dos tipos:

DICCIONARIO

[2] **Funcionamiento:** la fiabilidad de los sistemas se pueden valorar mediante una serie de **tasas**:

- **Falso negativo** (*False Rejection Rate*): Porcentaje de ocasiones en las que el sistema no vincula a una persona con su propia plantilla biométrica existente en la base de datos.
- **Falso positivo** (*False Acceptance Rate*): Porcentaje de ocasiones en las que un sistema vincula erróneamente a una persona con la información biométrica guardada correspondiente a otra persona.

[3] **Presentaciones:** Podéis consultar la documentación presentada durante la jornada organizada por **Pribatua** (Asociación vasca de privacidad y seguridad de la información) el 26 de septiembre de 2013 en Getxo (Bizkaia) titulada *La firma biométrica* en: http://pribatua.org

a) Sencillos: únicamente capturan la firma manuscrita *estática*, es decir, la **imagen** final de la firma.

b) Avanzados: son capaces de registrar gran cantidad de datos o **parámetros** relativos al proceso que sigue la persona cuando escribe su firma o rúbrica, como pueden ser los siguientes:

- ✓ Calidad de la línea
- ✓ Proporciones de la firma
- ✓ Presión ejercida durante el proceso de la firma
- ✓ Angulosidad de las letras
- ✓ Inclinación del texto
- ✓ Puntos de detención o levantamiento del puntero (bolígrafo)
- ✓ Orden que siguen los trazos
- ✓ Forma de los trazos iniciales y finales
- ✓ Posición y forma de signos de puntuación (tildes…)
- ✓ Forma y construcción de las letras
- ✓ Forma de enlazar las letras
- ✓ Puntos de ataque y puntos de escape
- ✓ Velocidad de la firma

En el caso de las firmas manuscritas, si bien cabe la posibilidad de que existan ligeras variaciones en la firma de una misma persona, la consistencia creada por el movimiento natural y la práctica a lo largo del tiempo crea un patrón reconocible que hace que pueda usarse para identificar a una persona.

«Los datos biométricos capturados mediante la tableta deberían transmitirse al PC de forma encriptada.»

Por lo tanto, en función de los datos recogidos, existen dos variantes a la hora de verificar si una firma es de una persona o no:

• **Comparación simple**: únicamente se considera el grado de parecido entre las dos firmas, la original y la que está siendo verificada.

• **Verificación dinámica**: en este caso, se realiza un análisis de la forma, la velocidad, la presión del bolígrafo y la duración del proceso de firma. No se considera significativa la forma o el aspecto final de la firma, sino los cambios en la velocidad y la presión que ocurren durante el proceso, ya que sólo el firmante original puede reproducir esas características.

SEGURIDAD JURÍDICA

La *firma electrónica reconocida* (FER) que todos conocemos requiere que a la persona firmante se le haya asignado previamente una clave de firma

Software de firma biométrica

Un aspecto muy importante que debe cumplir cualquier sistema que capture una firma (o los datos asociados a ella) es custodiar adecuadamente todos los parámetros recogidos para evitar su Reutilización, Falsificación o Alteración.

Algunos elementos que pueden darnos confianza en la entidad que recoge y almacena nuestra firma son disponer, entre otros, de un **dispositivo certificado**, un **software adecuado** y el servicio de un **tercero confiable**.

Normalmente, las *tabletas de firmas* disponibles en el mercado[4] incluyen tanto el *software* como las APIs (*Application Programming Interface*, Interfaz de programación de aplicaciones) necesarias para capturar y guardar la imagen de la firma y controlar la pantalla del dispositivo.

Sin embargo, si se requiere una mayor seguridad (y poder demostrar la validez de la firma en un juicio, por ejemplo), se recomienda utilizar un software que firme y selle el documento correspondiente. Este software inserta los datos biométricos y la imagen de la firma, por ejemplo, en un PDF y los une al documento protegiéndolo mediante algoritmos *hash* y *sellado asimétrico* (como puede ser RSA 2048 bits).

DICCIONARIO

[4] **Principales fabricantes de *tabletas de firma*:**

EpadLink: Tabletas de firma y software. Productos: Epad Ink...

Signotec: Empresa alemana creada en 2000. Tabletas de firma y software. Productos: Signotec LCD Signature Pad Sigma...

StepOver: Fundada en 2001 en Stuttgart (Alemania). Sus tabletas de firma son un referente en el sector, especialmente por su seguridad (ostenta el 80% del sector asegurador alemán). Productos: NaturaSign Pad Colour...

Topaz: Fundada en 1995 en EE.UU. es proveedor de soluciones de firma electrónica de documentos (tabletas de firma, software…) Productos: SigGem Colour 5.7, etc.

Wacom: Compañía japonesa fundada en 1983. Se ha establecido como líder en el mercado mundial de tabletas con lápiz. Productos: Wacom STU-520, etc.

(clave privada), la cual se la ha facilitado una tercera parte fiable (un proveedor de servicios de certificación, como, por ejemplo, **Izenpe**). Este tipo de firma electrónica no es la más apropiada para ser implantada en puestos de ventanilla ni en negocio de contacto directo (cara a cara con el cliente), ya que, normalmente, el firmante no dispondrá del certificado reconocido correspondiente. Por ello, la *firma electrónica escrita*, al no requerir ningún certificado reconocido, se ha impuesto en muchos sectores del mercado.

Según los expertos, tal y como sucede con la *firma electrónica reconocida* (por ejemplo, el DNI electrónico o los ofrecidos por **Izenpe**), la *firma biométrica* también debería tener como finalidad demostrar que el autor de la firma es quien dice haberla hecho (*identificación*), y que sirva también como forma de mostrar la aprobación sobre lo firmado (*no repudio*).

De no ser así, nos podríamos encontrar con situaciones donde la persona afectada diga «Esa no es mi firma» o «Yo firmé un documento, pero no ese documento».

Por ello, las entidades que gestionan este tipo de servicios deben ser capaces de asociar una determinada firma a un determinado documento sin ningún tipo de duda.

Para ello, es fundamental que la **generación y captura** de la Firma biométrica cumpla estrictamente las adecuadas medidas de seguridad.

Tal es así que si se requiere la máxima seguridad, los datos biométricos capturados mediante la tableta deberían transmitirse al PC de forma **encriptada**. Esto impediría que en algún momento los datos biométricos pudiesen ser capturados en un entorno inseguro como es el ordenador. De esta forma se conseguiría una vinculación entre la firma y el documento firmado. [ver cuadro *Software de firma biométrica*]

A través de un sistema de firma electrónica escrita adecuado, por tanto, se puede conseguir un documento firmado igual o más seguro que un equivalente firmado en papel.

Para la **demostración de autenticidad** de un documento firmado de forma electrónica hay que tener en cuenta los siguientes puntos:

1. **Calidad** de la firma capturada (rasgos identificativos del firmante)
2. **Seguridad** de la transferencia de la firma y de su custodia (la firma no debe poder copiarse ni usarse para una finalidad distinta para la que fue otorgada)
3. El contenido del documento y la firma deben ser **inseparables** (cualquier modificación ulterior del documento debe invalidar la firma)
4. La empresa no debe tener la posibilidad de **descifrar** los datos biométricos de la firma, ni de extraerlos del documento de modo que los pueda introducir en otro.
5. Desde el punto de vista del archivo se deben utilizar formatos de documentos **estándar** (p.ej. PDFs) para asegurar que el documento electrónico podrá seguir leyéndose en el futuro.
6. Debe tenerse en cuenta la posibilidad de **revisar los rasgos identificativos** (en nuestro caso, la firma) con independencia del fabricante y la tecnología empleada. Esto es necesario, por un lado, para la demostración lógica y verosímil ante los tribunales y, por otro, para asegurarse de que podrá seguir usando a largo plazo los archivos que hoy ha firmado digitalmente.

Si la entidad es capaz de asegurar todo lo anterior, desde el punto de vista del usuario final, son muchas las ventajas que nos ofrece la firma biométrica: es cómoda, poco intrusiva, no hace falta recordar contraseñas o tener tarjetas, etc.

CONCLUSIÓN

La firma es y ha sido durante muchos años una de las técnicas más habituales de identificación de las personas, razón por la cual hoy en día goza de una gran aceptación por parte de la ciudadanía.

Sin embargo, tal y como sucede con cualquier nueva tecnología, muchos usuarios pueden mostrar cierto **rechazo** a usar la firma biométrica al percibir que se invade su privacidad[5].

Por ello, dependiendo del servicio que se quiera prestar y del perfil de las personas afectadas, la entidad será quien deberá valorar si el uso de la firma biométrica es la solución más adecuada. ❑

DICCIONARIO

[5] **Privacidad y marco regulatorio:** La recogida de una firma biométrica manuscrita estará sujeto a lo expuesto en la Ley Orgánica de Protección de Datos (**LOPD**), ya que se considera que es un dato de carácter personal.

Tal es así que, desde el punto de vista de la LOPD debe tenerse en cuenta lo siguiente:

- ✓ El tratamiento de datos debe ser legítimo.
- ✓ Es necesario informar al interesado/a.
- ✓ Es necesario obtener el consentimiento de la persona.
- ✓ Es necesario tener inscrito el fichero ante la Agencia de Protección de Datos.

Según los expertos, existen suficientes normativas relacionadas con la protección de datos personales; sin embargo, sería recomendable profundizar en aquellos aspectos relacionados con la biometría.

eFactura en el Sector Público

Los términos sinónimos *factura electrónica*, *factura telemática*, *factura digital* o *eFactura* están adquiriendo cada vez más fuerza en el ámbito de las tecnologías de la información y las comunicaciones, sobre todo si nos centramos en el campo de la contratación pública, donde se los asocia con eficacia y con ahorro de costes. Vamos a intentar enmarcar la *eFactura* dentro del Sector Público.

La Comisión Europea ha identificado la facturación electrónica como un factor clave para la reactivación económica, así como un elemento significativo para la creación de un mercado digital único europeo, que sirve para favorecer el comercio transfronterizo entre sus estados miembros; de hecho, el Parlamento Europeo aprobó la Resolución de 20 de abril de 2012, sobre un mercado único digital competitivo, dicha Resolución apunta que la facturación electrónica sea obligatoria para todos los procesos de contratación pública antes del año 2016.

«La factura electrónica es el equivalente funcional a la factura en soporte papel, equiparándose tanto en sus efectos como en sus consecuencias»

En el ámbito del Estado la Comisión para la Reforma de las Administraciones Públicas (CORA) recogía dentro de sus medidas de carácter general el anteproyecto de Ley de impulso de la Factura Electrónica y creación del Registro Contable, que culmina con la publicación el pasado mes de diciembre de la **Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas del Sector Público**.

QUÉ ES LA FACTURA ELECTRÓNICA

Una factura básicamente es un documento que refleja una operación de compraventa, esto es, da validez a la entrega de un bien o a la realización de un servicio, va asociada a una fecha de devengo, e indica la cantidad que se debe pagar por ese bien o por ese servicio; además, es el único justificante fiscal válido que da al receptor el derecho a la deducción del impuesto.

La factura electrónica es un documento electrónico equivalente funcional de la factura en formato papel, esto es, se equipara con esta factura tanto en sus efectos como en sus consecuencias, y al ser electrónica se transmite a través de medios informáticos y telemáticos, estando avalada por una firma electrónica reconocida[6], necesitándose el reconocimiento de ambas partes, emisor y receptor, para que ésta tenga validez, a la vez que respeta las garantías de **autenticidad** de su origen (garantizar en todo momento quien es el proveedor del bien o del servicio prestado), de **integridad** de su contenido (que éste no ha sido modificado) y de **legibilidad** de la misma (las garantías de autenticidad e integridad se resuelven gracias a la firma electrónica de la que hemos hablado antes).

VENTAJAS DE LA FACTURA ELECTRÓNICA

Las ventajas de la utilización de la *eFactura* son numerosas, yendo desde el ahorro de costes, tanto desde el punto de vista del emisor de la factura como del receptor de la misma, hasta la eficiencia en la gestión: se elimina el papel, y se elimina

DICCIONARIO

[6] **Firma electrónica reconocida:** es una firma electrónica avanzada (esto es, permite identificar al firmante y cualquier cambio ulterior de los datos firmados, está vinculada al firmante de manera única y a los datos a que se refiere y ha sido creada por medios que el firmante puede mantener bajo su exclusivo control) basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma (por ejemplo, la Firma Electrónica Reconocida -FER- ofrecida por la empresa de certificación IZENPE, a través, entre otros, del **certificado corporativo privado reconocido**; o el eDNI).

www.izenpe.com

también la gestión tradicional de envío y recepción (franqueo postal y ensobrado), además, a día de hoy los costes de envío y recepción a través de medios informáticos y telemáticos son muy bajos, y a esto hay que añadir la inmediatez de estas acciones; también, al automatizarse el proceso de emisión de facturas (ya que se puede integrar con el ERP[7] de la empresa), se minimizan los posibles fallos e incidencias, mejorándose la imagen de la empresa o corporación emisora de cara a los clientes, y en lo que respecta al receptor, la integración automática de los datos en los sistemas contables de la empresa implica una menor participación de las personas, mejorando la eficacia y eficiencia de las operaciones contables, y, además, posibilita una reducción en los plazos de cobro de las facturas.

LEY DE IMPULSO DE LA FACTURA ELECTRÓNICA

La **Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas del Sector Público** tiene por objeto:

- **Impulsar el uso de la factura electrónica**
- **Crear un registro contable de facturas**, para,

Despliegue plataforma *eFactura* en el País Vasco

Actualmente, en EJIE (la Sociedad Informática del Gobierno Vasco) se dispone de una plataforma de facturación electrónica, la cual puede ser utilizada, en el ámbito de la administración pública de la Comunidad Autónoma del País Vasco, para poner en funcionamiento un servicio de facturación electrónica sin tener que realizar desarrollos propios.

Desde EJIE se va a lanzar un plan de despliegue para capacitar y dar a conocer este servicio hacia todos sus clientes.

Tanto desde el Gobierno Vasco como desde otros entes se ha mostrado interés en la utilización de esta plataforma de servicios de factura electrónica. Este interés también está condicionado por la Ley 25/2013, de 27 de diciembre, de impulso de la facturación electrónica y la creación del registro contable de facturas del sector Público.

Este proyecto de despliegue de la plataforma de *eFactura* tiene varias fases:

- **Fase I**: Servicio *eFactura* del Gobierno Vasco

Comprende las fases de análisis, diseño, construcción e implantación, junto con la comunicación, formación y soporte en el propio Gobierno Vasco, lo cual implica una integración con los sistemas internos (sobre todo con la aplicación de gestión contable y con la aplicación de contratación pública) y con el nuevo registro contable de facturas (con una arquitectura normalizada de recepción de facturas electrónicas).

También contemplará la interoperabilidad con otras plataformas (por ejemplo, con el punto general de entrada de la Administración General del Estado).

El alcance es la gestión con los proveedores (recepción de facturas electrónicas).

- **Fase II**: Servicio *eFactura* de Osakidetza y Ayuntamientos

Definirá el modelo de despliegue y uso para el ente público de derecho privado Osakidetza y para las entidades locales (ayuntamientos).

Al exponer la plataforma toda su funcionalidad a través de servicios web proporcionando interfaces *marca blanca* que cada promotor puede hacer suyos, y entendiendo que los servicios que expongan, tanto Osakidetza como los Ayuntamientos, serán servicios propios, los frontales destinados a sus clientes y proveedores se supone que también residirán en sus entornos y serán proyectos propios, desarrollados por ellos.

- **Fase III**: Otros servicios de *eFactura*

Dar a conocer y promover el uso de la plataforma en el resto de sectores de la administración pública de la Comunidad Autónoma del País vasco.

- **Fase IV**: Mantenimiento de la plataforma

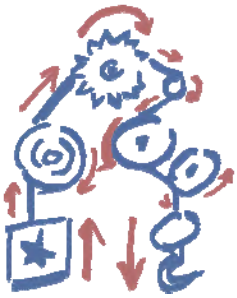
Actividad de mantenimiento de la plataforma en sí misma.

http://www.ejie.euskadi.net

DICCIONARIO

[7] **ERP:** (*Enterprise Resource Planning*, Sistemas de planificación de recursos empresariales) Son sistemas que manejan la producción, logística, distribución, inventario, envíos, facturas y contabilidad de una empresa de una forma integrada.

Para más información podéis leer el artículo titulado *ERP/CRM* publicado en el Boletín Aurrera Nº 6, de diciembre de 2001.



de este modo, agilizar los procedimientos de pago al proveedor y dar certeza de las facturas pendientes de pago existentes (para mejorar la competitividad se quiere reducir la morosidad de las Administraciones Públicas)

- **Regular el procedimiento para su tramitación**
- **Regular las actuaciones de seguimiento** por los órganos competentes

El ámbito de esta Ley se refiere a las facturas emitidas en el marco de las relaciones jurídicas entre proveedores de bienes y servicios y las Administraciones Públicas.

Los proveedores tienen la obligación de presentar en un registro administrativo las facturas expedidas por los servicios que presten o por los bienes que entreguen (plazo de treinta días desde la entrega efectiva de las mercancías o la prestación de servicios); se pueden excluir reglamentariamente de esta obligación las facturas cuyo importe sea hasta 5.000 €.

Esta factura tendrá los mismos efectos tributarios que la factura en soporte papel.

Respecto al formato, la Ley dice que tendrá un formato estructurado, y que mientras no se apruebe la Orden ministerial las facturas electrónicas se ajustarán al formato de la factura electrónica ***Facturae*, versión 3.2**, y estarán firmadas con una firma electrónica avanzada basada en un certificado reconocido, conforme a la especificación *XML Advanced Electronic Signatures* (ver recuadro titulado *XAdES*).

La Ley también obliga a cada Comunidad Autónoma a la **creación de un punto general de entrada de facturas electrónicas**, que no es sino una solución de intermediación entre el ente que presenta la factura y la oficina contable a la que le compete su registro, proporcionando un acuse de recibo electrónico que acredita la **fecha** y **hora** de registro, permitiéndose la consulta del estado de la tramitación de la factura. Las entidades locales podrán adherirse al punto general que proporcione su Diputación, Comunidad Autónoma o el Estado, y las Comunidades Autónomas podrán adherirse al que proporcione el Estado. A estos puntos generales de entrada, según esta Ley, se les deberá dar publicidad.

Asimismo, la Ley obliga a la **creación de un Registro Contable de facturas** (vigente a partir del 1 de enero de 2014) y la regulación de un **nuevo procedimiento de tramitación de facturas**, a este Registro Contable deberá dársele publicidad, y pertenecerá al órgano que tenga atribuida la función contable.

La disposición adicional cuarta de esta Ley indica que se intercambiará la información (interoperabilidad) sobre deudores de las Administraciones y los pagos a los mismos con el objeto de realizar las actuaciones de embargo o compensación que procedan.

La **entrada en vigor de esta Ley** respecto a las obligaciones de presentación de la factura electrónica es el 15 de enero de 2015.

FORMATO DE LA FACTURA ELECTRÓNICA

El formato de factura electrónica más empleado en el Estado es el ***XML Facturae***, formato al que se ajustan las facturas electrónicas admitidas por la Ley 25/2013, de 27 de diciembre, **de impulso de la factura electrónica y creación del registro contable de facturas del Sector Público,** y que es compatible con UBL[8] y CII (*Cross Industry Invoice*), que son los dos principales formatos internacionales, si bien existe otro formato que es utilizado en el sector de la distribución, el formato denominado EDIFACT, que no está basado en XML[9], sino en formatos del tipo EDI (*Electronic*

«Desde febrero de 2005, la factura UBL se ha impuesto por ley para todo el sector público en Dinamarca. Cada mes se intercambian en Dinamarca 1,2 millones de facturas UBL. El ministerio danés de finanzas estima unos ahorros para el estado de 100 millones de euros anuales por el uso de este tipo de documento.»

DICCIONARIO

[8] **UBL:** *Universal Business Language*, norma que nace de una propuesta realizada por Charles Hoffman, experto contable y auditor, con el objeto de automatizar el intercambio de información financiera mediante el uso del lenguaje XML, propuesta realizada allá por el año 1988. Al estar basado en XML asegura su estandarización y la posibilidad de ser utilizada con numerosas herramientas. La versión actual es la 2.0, y se puede conseguir aquí: http://www.docs.oasis-open.org/ubl/cs-UBL-2.0.zip/

[9] **XML:** *eXtensible Markup Language*, lenguaje de marcas extensible, que es el lenguaje utilizado en Internet para el intercambio de información.

Data Interchange, Intercambio Electrónico de Datos), y que, al contrario que *Facturae*, es de pago.

FORMATO FACTURAE: BLOQUES

El formato *Facturae*, en su versión 3.2, recoge cinco bloques de información principales:

- ✓**Cabecera**: bloque obligatorio y único (*versión* [3.2], *modalidad*, *tipo emisor*, *tercero*, *lote* y *datos cesión factura*)
- ✓**Sujetos:** con datos del emisor y receptor de la factura. **Emisor**: bloque obligatorio y único referente a la persona que emite la factura. **Receptor**: bloque obligatorio y único con la información de la persona a la que va referida la factura. Ambos bloques tienen la siguiente información: *identificación fiscal*, *identificación de la entidad*, *centros* y *otros datos*.
- ✓**Factura**: conjunto de facturas que contiene el fichero, y para cada factura incluye *cabecera de factura* [número de factura, número de serie, tipo documento, clase de factura, rectificativa], *datos factura* [fecha expedición, fecha operación, lugar expedición, período facturación, moneda facturación, tipo de cambio, moneda de impuesto, lengua], *impuestos repercutidos*, *impuestos retenidos*, *totales factura* [total importe bruto, descuentos generales, cargos generales, total descuentos, total cargos, total importe, total impuestos repercutidos, total impuestos retenidos, total factura, subvenciones, anticipos, suplidos, total gastos financieros, total a pagar, total anticipos, retenciones, total a ejecutar, total suplidos], *líneas de detalle* -por cada concepto facturado-, *datos de pago* (incluye la fecha en la que se deben atender los pagos), *literales legales* y *datos adicionales*.
- ✓**Extensiones:** permite incorporar nuevas definiciones estructuradas cuando sean de interés.
- ✓**Firma Electrónica:** conjunto de datos asociados a la factura que garantizarán la autoría y la integridad del mensaje. Se define como opcional para facilitar la verificación y el tránsito del fichero. No obstante, debe cumplimentarse este bloque de firma electrónica para que se considere una factura electrónica válida legalmente frente a terceros.

La siguiente dirección web http://www.facturae.es/es-ES/Descargas/Paginas/Utilidades.aspx proporciona utilidades de validación, visualización y conversión entre versiones de facturas generadas siguiendo el formato *Facturae*. ❑

XAdES (firma electrónica avanzada)

XAdES son las siglas de *XML Advanced Electronic Signatures*. Recoge un conjunto de extensiones a la recomendación XMLDSig propuesta por el W3C[10]. Proporciona autenticación básica, protección de integridad y satisface requerimientos adicionales para firma electrónica avanzada. Una característica es que los documentos firmados pueden seguir siendo válidos durante largos períodos de tiempo, incluso cuando los algoritmos utilizados para realizar la firma hayan sido rotos.

Define diferentes perfiles según el nivel de protección ofrecido:

- XAdES-BES (*Basic Electronic Signature*): Se construirá sobre un XMLDSig incorporando una serie de propiedades
- XAdES-EPES (*Explicit Policy based Electronic Signature*): Se construirá sobre un XMLDSig o un XAdES-BES incorporando una propiedad en la que se define la política particular de firma utilizada.
- XAdES-T (*Timestamp*): Se construye sobre una firma XAdES-BES o XAdES-EPES incorporando una propiedad que contiene un sello o marca de tiempo proporcionada por una *TSA (Autoridad de Sellados de Tiempo)* que certifica que la firma existe a partir de ese punto en el tiempo, protegiéndola contra el repudio.
- XAdES-C (*Complete*): Se construye sobre una firma XAdES-T añadiendo referencias a certificados y listas de revocación utilizados durante la verificación y que serán útiles para poder seguir validando la firma en el futuro.

Fuente: Documento de Guía de implementación de la firma de documentos CODICE (Ministerio de Economía y Hacienda).

https://contrataciondelestado.es/codice/2.0/doc/CODICE_2_GuiaImplementacion_Firma_v1.1bis.pdf

DICCIONARIO

[10] **W3C:** *World Wide Web Consortium,* comunidad internacional que desarrolla estándares que aseguran el crecimiento de la web a largo plazo.

ALBOAN:

Elementos gráficos para presentaciones corporativas del Gobierno Vasco

«El banco de imágenes consta de más de 500 ilustraciones»

Probablemente muchos de nuestros lectores y lectoras han tenido que realizar en algún momento de su vida profesional una presentación para un seminario o congreso. Y, seguramente, han usado imágenes copiadas directamente de Internet para complementar las diapositivas de su presentación. Sin embargo, serán muy pocos los que han tenido en cuenta o se han fijado en si esa imagen tenía algún tipo de *copyright* o derechos de autor. Por lo que, en muchas ocasiones, podríamos estar incurriendo en una falta al incumplir alguna clausula referida a la Propiedad Intelectual de esas imágenes.

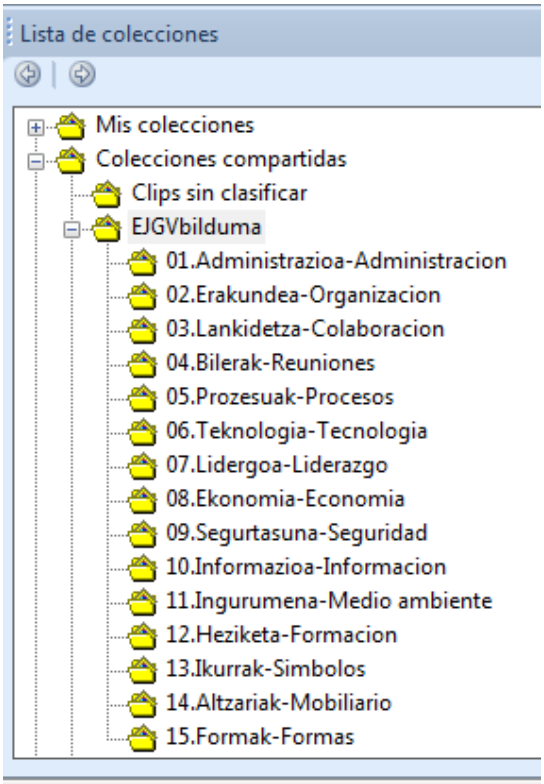
EL PROYECTO

Siendo conscientes de esta problemática, la Dirección de Informática y Telecomunicaciones (DIT) del Gobierno Vasco puso en marcha (a finales del año pasado) un proyecto cuyo objetivo era **crear una serie de elementos gráficos** que pudiesen ser utilizados en presentaciones corporativas, es decir, disponer de una colección de imágenes propias para ser usadas en *power-point*, *impress*, *prezi* o cualquier otra aplicación similar, sin ningún tipo de limitaciones.

La primera tarea que se llevó a cabo fue definir, junto con el ilustrador encargado de diseñar las imágenes, las líneas maestras de los elementos gráficos: tipo de elementos gráficos solicitados, estilo general de los mismos, gama de colores a utilizar, formato en el que se iban a guardar las imágenes, etc.

Pues bien, una vez establecidos todos los aspectos técnicos y organizativos necesarios, durante varias semanas se fueron diseñando los distintos elementos solicitados (flechas, cuadrados, círculos, iconos, imágenes, símbolos, etc.)

El banco de imágenes, denominado *EJGVbilduma* o *GaleríaEJGV,* consta de más de **500 ilustraciones**, todas las cuales han sido agrupadas en 15 **categorías** en función de su temática: Administración; Organización; Colaboración; Reuniones; Procesos; Tecnología; Liderazgo; Economía; Seguridad; Información; Medio ambiente; Formación; Símbolos; Mobiliario; y, por último, Formas.



El formato finalmente elegido para las ilustraciones ha sido el .PNG (*Portable Network Graphics*), debido, entre otros aspectos, a las ventajas de escalabilidad que ofrece.

Una vez finalizada esa parte del trabajo, se abordó la tarea de diseñar una **plantilla corporativa** para

power-point e *impress*. En este caso, también fue necesario establecer el diseño general de las diapositivas, la línea gráfica a utilizar, los elementos que se iban a incluir en el patrón, la tipografía, etc.

Teniendo como referencia el trabajo realizado en su momento por Lehendakaritza, finalmente se han creado dos versiones de la plantilla corporativa: una en escala de grises y otra en color.

La **ventaja** que nos ofrecen estas dos plantillas es que podemos crear de una manera fácil y rápida cualquier presentación que necesitemos, sin necesidad de perder tiempo pensando en temas como puede ser, entre otros, el diseño; pudiendo, de esta forma, centrarnos desde un principio en el contenido de la presentación. Además, gracias a este tipo de plantillas se dispone ya de un **diseño institucional** y fácilmente identificable con el Gobierno Vasco, independientemente del foro o encuentro en el que se utilice.

¿CÓMO LOS UTILIZO?

Una vez diseñados todos los elementos gráficos anteriormente comentados, EJIE ha realizado las tareas necesarias para que, tanto las imágenes como las plantillas, estén accesibles para cualquier persona cuyo ordenador esté conectado a la Red Corporativa del Gobierno Vasco; tanto es así, que están *integrados* en el paquete ofimático estándar instalado en los equipos informáticos del Gobierno Vasco: *Microsoft Office2010* (*Power-point*…) y *LibreOffice3.5* (*Impress*…)

Gracias a ello, si queremos usar cualquiera de las imágenes diseñadas sólo tenemos que seguir estos pasos: abrir la aplicación *Power-point2010*, por ejemplo; pinchar sobre la pestaña *Insertar*; y, a continuación, elegir *Imágenes prediseñadas/ ClipArt*.

A continuación, en la casilla *Buscar* indicaremos el tema o palabra clave sobre la cual queremos una imagen.

Cabe destacar que, gracias a los **metadatos** o **etiquetas** (palabras claves) asignadas a cada una de las imágenes, el usuario final puede buscar de una manera fácil y cómoda las ilustraciones que mejor se ajusten al concepto que quiera representar: «mujer», «interoperabilidad», «teletrabajo», etc.

En el caso de las Plantillas, éstas están accesibles dando estos pasos: abrir la aplicación *Power-point2010*; pinchar sobre la pestaña *Archivo*; y, a continuación, elegir *Nuevo*, y, después, *Mis Plantillas*. Donde tendremos la opción de elegir la plantilla *EJGV* o *EJGV_color* (cada una de las cuales incluye el diseño de varias diapositivas).

Antes de acabar, desde la DIT os invitamos a que visitéis la galería de imágenes y hagáis uso de las plantillas diseñadas, y nos hagáis llegar cualquier idea o sugerencia que estiméis oportuna. ❑

«La ventaja que ofrecen las dos plantillas diseñadas es que podemos crear de una manera fácil y rápida cualquier presentación que necesitemos»

[+info]:

Sugerencias a:

aurrera@euskadi.net

ALBOAN

¡¡BREVES!!

nº 47

Marzo de 2014

Guía de recomendaciones para un uso SEGURO de los dispositivos y de las Redes Sociales en el GV

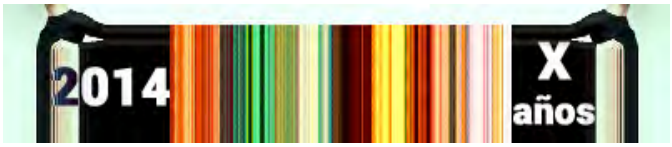
Las personas usuarias de las Redes Sociales no prestan excesiva atención a las amenazas a las que se exponen, y, en consecuencia, a través de estas redes, se puede propagar código dañino y se puede obtener información de una forma ilícita, por ello, la Dirección de Informática y Telecomunicaciones (DIT) ha elaborado una sencilla ***guía de recomendaciones para un uso SEGURO de los dispositivos y de las redes sociales en el Gobierno Vasco***, en la misma se abordan los siguientes temas:

- ✓ Contraseñas (cómo conseguir una contraseña segura)
- ✓ Seguridad y privacidad en las redes sociales (con enlaces a guías elaboradas por **Irekia** y videoguías elaboradas por la **Agencia Vasca de Protección de Datos (AVPD),** y enlaces para configurar la privacidad y seguridad en las redes sociales)
- ✓ Consejos para proteger dispositivos móviles
- ✓ *WhatsApp* y la información sensible
- ✓ Dispositivos móviles y el ocio
- ✓ Riesgos de la geolocalización
- ✓ Pasos a dar cuando se pierde o nos roban el dispositivo móvil
- ✓ Diez consejos básicos de seguridad

Dicha guía, que fue presentada el pasado 30 de enero en el Salón de Actos de Lakua, está accesible (en formato *pdf* y *epub*) en la siguiente dirección:

www.euskadi.net/informatica (apartado *Seguridad*)

X aniversario de la Agencia Vasca de Protección de Datos



El 25 de febrero de 2004 se aprobó en el Parlamento Vasco la Ley 2/2004, a través de la cual se creaba la Agencia Vasca de Protección de Datos (AVPD). Este año, por tanto, se celebra el décimo aniversario de la aprobación de la ley y de la creación de la Agencia.

Tal y como establece esa Ley, la AVPD es la entidad encargada de velar por la protección de los datos personales en manos de las administraciones públicas vascas.

Es por ello que desde entonces esta institución ha desarrollado sus tareas con un único objetivo: conseguir que las Administraciones Públicas de nuestra comunidad autónoma (en el ámbito local, de los territorios históricos y a nivel autonómico) cumplan estrictamente la Ley en ese ámbito.

Con motivo del X aniversario, el pasado día 24 de febrero tuvo lugar en el Parlamento Vasco una Jornada titulada «Pasado, presente y futuro de la Agencia Vasca de Protección de Datos», a la cual acudieron distintas personalidades relacionadas con la Agencia.

Durante ese acto, clausurado por el Consejero de Administración Pública y Justicia del Gobierno Vasco, Josu Erkoreka, tuvieron lugar dos mesas redondas así como la entrega de varios premios a distintas personalidades y entidades que han destacado significativamente en el ámbito de la protección de datos.

Por nuestra parte, ¡Zorionak a la Agencia (y a todo su personal)!

Web a la AVPD: http://www.avpd.euskadi.net