EUSKO JAURLARITZA
GOBIERNO VASCO

— Ejemplar en Castellano (*) —

Aurrera!

Nº 22

Junio de 2006

Boletín Divulgativo de Nuevas Tecnologías en Informática y Telecomunicaciones

Publicado por el Gabinete Tecnológico de la DIT

ÍNDICE

Parece mentira, pero es cierto. Los delitos que hoy en día hacen uso de las Nuevas Tecnologías (también llamados *"ciberdelitos"*), y que principalmente se basan en Internet, siguen teniendo un gran éxito a pesar de la cantidad de información que de forma continua nos avisa de sus peligros. Es por ello que, a modo de recordatorio, recogemos en el primero de los temas de este nuevo Boletín AURRERA!, algunas de las nuevas variantes del Phishing que se han puesto de moda durante los últimos meses.

Durante los días 7 y 8 del presente mes se ha celebrado en Bilbao la segunda edición del Congreso titulado *"Contratación Pública Electrónica Internacional"*, en el que han participado ponentes de distintos países compartiendo sus experiencias y/o reflexiones en este ámbito. Por ello, a lo largo del segundo tema del Boletín, se exponen las principales conclusiones que se han podido obtener de las distintas intervenciones. Pudiendo de esta forma, conocer los distintos proyectos de Contratación Electrónica que se vienen desarrollando en otras Administraciones.

Aprovechando la cercanía de las vacaciones veraniegas y todo lo que ello implica: desplazamiento de vehículos, atascos, incidentes de tráfico, ... hemos querido en esta ocasión dar a conocer (dentro del apartado ALBOAN), la gran movilización tanto de recursos humanos como materiales que realiza el Departamento de Interior y que son coordinados a través del llamado *"Centro de Gestión de Tráfico de Euskadi"*.

Por último, dentro de la sección "Breves" se informa de la participación que recientemente ha tenido el Gobierno Vasco dentro de las Jornadas organizadas por el Ministerio de Administraciones Públicas en Sevilla (conocidas como Tecnimap), a través de distintas ponencias presentadas y participación en mesas redondas donde se han dado a conocer sus proyectos de Administración Electrónica más significativos.

CIBERDELITOS

El usuario de Internet dispone hoy en día de mucha información sobre los riesgos existentes y las cautelas que debe adoptar, al visitar páginas desconocidas o a la hora de cumplimentar un formulario en una Web. Sin embargo, los delitos que se basan en las Nuevas Tecnologías (llamados "ciberdelitos") afectan cada día a más usuarios.

DICCIONARIO

(1) SPAM: Ver Boletín Nº 16 (diciembre de 2004).

(2) Spyware: Programa "espía" que recopila información sobre una persona sin su conocimiento.

Adware: Software que durante su funcionamiento despliega publicidad de distintos productos o servicios.

(3) Phishing: El término viene del ingles "fishing" (pesca) y hace alusión al acto de "pescar" usuarios mediante señuelos para obtener información secreta sobre ellos. También se dice que es la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas). La primera vez que se habló de phishing fue en 1996 y se hizo en el grupo de noticias de hackers "alt.2600".

(4) Phisher: Persona que "practica" el phishing.

Casi todos los usuarios saben lo que pasa si responden a un mensaje de alguien que dice ser su banco y les pide además la clave para acceder a su cuenta de banca electrónica. Sin embargo, y a pesar de todo, siguen existiendo muchos usuarios que por desconocimiento o simple dejadez, caen en este tipo de engaños. Debido a ello, el propio usuario facilita (entre otras cosas) el incremento del SPAM(1), las estafas electrónicas y las transferencias bancarias fraudulentas.

Hasta hace poco, la opción más común consistía en echar toda la culpa de todos estos peligros directamente a Internet. Sin embargo, actualmente, muchos expertos están empezando a responsabilizar directamente al usuario, ya que en muchas ocasiones son los propios usuarios los responsables finales de lo que les pasa en la Red. La razón es que nunca leemos las condiciones generales de una contratación vía web; el usuario facilita sus datos personales (su dirección de correo electrónico) a cambio de un tono polifónico para el móvil, una foto de un famoso, una canción MP3, etc. sin pensar en las consecuencias de ese acto (¿a quién se lo estoy dando?, ¿para qué lo usará?,...). El problema es que en algunos de esos casos, las cláusulas que se aceptan con un simple clic de ratón, incluyen

la aceptación de fórmulas de marketing muy intrusitas, que además, permiten la instalación de programas del tipo spyware/adware(2) en nuestros propios ordenadores. Asimismo, y como ejemplo de las consecuencias de esa dejadez, muchos usuarios de programas de intercambio de ficheros (llamados P2P) sin darse cuenta suelen dejar compartidos (abiertos) directorios de su PC, donde guardan datos personales. Para comprobarlo solo hay que buscar las palabras *currículum*, *contactos* o *contraseñas* en un programa como eMule y ver los resultados. Pero el exponente más grave de esa dejadez que muestran algunos usuarios en ciertos momentos, y que últimamente está teniendo más repercusión pública, se llama Phishing(3).

"En muchas ocasiones no es necesario ser un experto en Informática para evitar estos timos, solo hay que prestar un poco de atención."

EL PHISHING

El Phishing es de esos fenómenos que, al igual que ha pasado con el SPAM, no sólo se lee en los periódicos, sino que, seguramente, muchos de nuestros lectores han visto como evolucionaba en su propio buzón.

El phishing es simplemente **una modalidad de estafa** donde una persona (a través de un e-mail) se hace pasar por una empresa con el objeto de obtener de un usuario ciertos datos: número de tarjeta de crédito, clave secreta,... Este tipo de "robo de identidad" basa su éxito en la facilidad con que personas confiadas revelan información personal a los Phishers(4). El estafador en estos casos hace todo lo posible para suplantar la "imagen" de una empresa, y hacer creer al destinatario que los datos solicitados se los pide el sitio "oficial", cuando en realidad no es así.

Lo curioso de este delito es que, en realidad, no es una acción que requiera de sofisticadas herramientas y/o conocimientos. Es más, las técnicas que se utilizan, no son nuevas y son de sobra conocidas, sin embargo, hasta ahora no se habían utilizado en conjunto para realizar un ataque. Estas técnicas incluyen el **SPAM**, la **Ingeniería Social**[5], la Copia de páginas webs, aprovechar las vulnerabilidades de los

servidores, la instalación de Programas del tipo: troyanos, capturadores de contraseñas (keyloggers), etc. en los PCs de los usuarios. Los Phishers pueden usar varios canales para llegar al usuario (su víctima):

- **Correo electrónico**: es el método más utilizado. Aquí se envía un e-mail a muchos usuarios simulando ser una entidad oficial para obtener datos de algunos usuarios[6]. Los datos son solicitados alegando motivos de seguridad, mantenimiento del sistema, mejora del servicio, encuestas o cualquier otra excusa, para que el usuario facilite sus datos secretos. El correo puede contener formularios, enlaces falsos, textos originales, imágenes oficiales, etc., todo para que visualmente sea idéntica al original y no levante sospechas. La idea final es que el usuario facilite su información personal y (sin saberlo) lo envíe directamente al estafador, quien la usará de forma fraudulenta.
- **Página web o ventana emergente**: en este caso se simula visualmente la página web de una entidad oficial, normalmente un banco. El objetivo es que el usuario teclee sus datos privados en un formulario web.
- **Llamada telefónica**: El usuario recibe una llamada telefónica en la que el emisor suplanta a una entidad para que ese usuario le facilite datos privados. Un ejemplo claro es el que se produce en la época de la Declaración de la Renta, donde los ciberdelincuentes llaman a los contribuyentes para pedirles datos de su cuenta corriente haciéndose pasar por personal de Hacienda.
- **SMS**: El usuario recibe un mensaje en su teléfono móvil donde se le solicitan datos personales.

Normalmente, los servicios más suplantados son los relacionados con el dinero (Banca on-line, Servicios de subastas en línea y Tarjetas de crédito). La razón es que un atacante con la clave de un usuario podría manejar el dinero a su antojo, incluyendo la transferencia del dinero a otra cuenta bancaria. Para evitar en cierta medida este delito, muchos bancos limitan la capacidad de hacer transferencias internacionales.

Puesto que el procedimiento que utiliza el Phishing se basa por un lado en la suplantación de una identidad, por otro lado en el uso de la ingeniería social y por último en el robo de claves, se asemeja bastante a otros ataques que puede sufrir un usuario; por ejemplo, que los usuarios de una organización reciban una llamada de "su" Administrador de Sistemas o Centro de Atención a Usuarios (y mediante este engaño) pedirles directamente sus contraseñas.

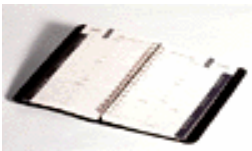
Algunos intentos de phishing dejan de lado el ya comentado envío de correo y basan su suerte "anunciando" su engaño (cebo) a través de banners (o incluso a través de los resultados de las búsquedas de un buscador como Google). Estos anuncios simulan proporcionar un servicio (por ejemplo, la recarga de un teléfono móvil) para lo cual se solicitan datos adicionales como el número de tarjeta de crédito y su fecha de caducidad.

EL SCAM

A raíz del éxito del Phishing ha surgido otro fenómeno llamado SCAM[7].

De forma periódica, los Phishers (haciéndose pasar por empresas ficticias) ofertan por e-mail o chat puestos de trabajo para trabajar desde casa cobrando una cantidad de dinero. Para que una persona pueda darse de alta con esta *empresa* debe rellenar un formulario en el cual se solicitan entre otros datos: nombre y apellidos, cuenta bancaria, etc. El usuario cree que es un trabajo real ya que incluso le envían a casa un contrato.

Todas aquellas personas que aceptan esta oferta se convierten automáticamente en *víctimas* que posteriormente (y sin saberlo) incurren en un delito de blanqueo de dinero. Ya que la finalidad de este proceso es que cada vez que el Phisher



DICCIONARIO

[5] Ingeniería social: Para más información consultar el Boletín N° 13 (marzo de 2004).

[6] Spear phishing: (literalmente *phishing con lanza*). Tipo de Phishing donde el envío de e-mails no es masivo, sino que es mucho más selectivo. Ya que los phishers son capaces de conocer previamente con exactitud con qué banco tiene relación una personal determinada, y de ese modo enviarle un e-mail totalmente personalizado.

[7] SCAM: Engaño con intención de estafa o fraude, que mezcla el correo no solicitado (SPAM) con un HOAX (bulo o broma). Dado el contenido y objeto del mensaje enviado, también reciben el nombre de "Ofertas de trabajo falsas".

"Phishing-Car" el último fraude

¿Quieres un BMW Z4 con 80.000 kilómetros por 1.600 euros?

El mecanismo utilizado es muy sencillo y además, es mas rápido que el phishing tradicional y mas económico para el estafador.

Los estafadores, haciendo uso de webs con direcciones muy similares a páginas de **venta de coches**, consiguen captar a las víctimas. Todas estas estafas suelen tener en común que el 90% de los vehículos suele estar fuera de España (Reino Unido), suelen pedir una entrada del 40% del precio total, las transferencias se realizan a través de agencias de envío de dinero (Western Union, Money Gram) y el vendedor oferta la entrega a domicilio.

Una vez realizada la transferencia del dinero, el comprador se queda sin dinero y sin coche.

realiza un acto fraudulento de *phishing,* la víctima recibe en su cuenta bancaria el dinero procedente de la estafa. Una vez recibido el ingreso, el *trabajador* se queda con un % del total (a modo de comisión) y el resto lo reenvia a través de Internet (por medio de empresas como Western Union o Money Gram) a cuentas de otros países que previamente le ha indicado la *seudo-empresa*.

Como vemos, una vez que el usuario ha sido *contratado*, éste se convierte automáticamente en lo que se conoce como "*mulero*".

En definitiva, el usuario acaba involucrado en un acto de estafa, pudiéndose ver requerido por la justicia.

Ejemplo real de e-mail para captar "muleros":

Asunto: Ofrecemos trabajo bien pagado.
Nuestra compania se llama Magnat Trading Group.
Nuestra especializacion es ayudar a empresarios a vender o comprar el articulo en la subasta mundial Ebay. Como un resultado del trabajo intenso la compania en 4 anos pudo lograr el nivel mundial y segun los expertos ser una de las 20 mas influyentes companias, que proponen los servicios de comercio.
En Espana empezamos a trabajar recientemente y en relacion con eso tenemos una vacancia de manager financiero supernumerariom, quien va a ser representante de nuestra compania en Espana.
Los requerimientos basicos son los siguientes:
- conocimiento de los sistemas electronicos de pago (por ejemplo - Western Union) - computador, internet, e-mail, telefono
- la cuenta bancaria en Espana
Por buen cumplimiento del deber prometemos alto nivel de beneficio, tiempo de trabajo flexible.
El pago se comete sin retraso. Le pagamos a Usted 150-500 euro por cada operacion.
Si esta Usted interesado en nuestra proposicion, puede recibir mas detalles por e-mail:
magnat_group@km.ru

FORMAS DE PROTEGERSE

Algunos estudios afirman que cerca de un 82% de los clientes de banca electrónica no sabe distinguir entre un mensaje de correo legítimo y uno fraudulento. De todas formas, en muchas ocasiones no es necesario ser un experto en Informática para evitar estos timos, solo hay que prestar un poco de atención. A modo de ejemplo, a continuación mencionaremos algunas medidas que (desde tres puntos de vista) se pueden aplicar para frenar estos delitos, así como algunas pistas en las que fijarnos y que nos pueden ayudar a detectarlos:

1.- EL USUARIO:

La forma más segura para que un usuario no sea estafado, es que NUNCA responda a NINGUNA solicitud de información personal a través de estos medios. Las entidades NUNCA le solicitarán claves, números de tarjeta de crédito o cualquier información personal por correo, por teléfono o SMS. Recuerde que éstas NUNCA se lo van a solicitar porque ya los tienen.

"El phishing es simplemente una modalidad de estafa."

Por otro lado, a la hora de visitar sitios Web, el usuario debería teclear siempre la dirección URL directamente en la barra de direcciones. NUNCA acceder pinchando sobre enlaces procedentes de cualquier otro sitio. Pocos usuarios serían capaces, por ejemplo, de detectar que la web www.bankofthevest.com no es www.bankofthewest.com (donde ha sido sustituida la w de la web verdadera por la v del falso). Asimismo, algunos usuarios seguirán creyendo que la dirección de correo *informatica@soporte_empresa.com* es lo mismo que *informatica@empresa.com*.

En este mismo sentido, el uso de subdominios (*www.nombrebanco.com.ejemplo.com*) son también trucos usados por los phishers. Otro ejemplo para disfrazar enlaces es el de utilizar direcciones que contengan *@*. En el caso del enlace *www.google.com@members.tripod.com* puede engañar a un usuario al creer que el enlace va a abrir la página de www.google.com, cuando realmente el enlace envía al usuario a la página members.tripod.com

Otros intentos de phishing usan comandos en JavaScripts para alterar la barra de direcciones. Esto lo hacen colocando una imagen de la dirección web de la entidad legítima encima de la barra de direcciones del Navegador y ocultando la barra de direcciones original para que no se detecte el cambio de dirección.

Por otra parte, muchas compañías (eBay,...) a la

hora de dirigirse a sus usuarios incluyen su nombre y apellidos en los correos que le remiten, de manera que si un correo electrónico se dirige al usuario de una manera genérica (*"Querido miembro de eBay"*) es probable que sea un intento de phishing. Otras organizaciones utilizan la técnica denominada "pregunta-desafío", en la que se pregunta información que sólo es conocida por el usuario y la organización.

Ya por último, ciertos usuarios han recibido correos electrónicos que por gramática (incluían errores ortográficos) y aspecto visual resultaban ya sospechosos.

2.- LA TECNOLOGÍA:

Algunos expertos consideran que la mejor solución frente a este tipo de timos es hacer uso de un sistema de autenticación robusta (mediante tarjetas), ya que éstas no permiten extraer las claves necesarias para responder a la autenticación.

De todas formas, a día de hoy, la autenticación robusta no es una opción para servicios universales, es decir, los que tengan como objetivo cualquier usuario que utilice Internet. Por ejemplo, eBay o Amazon, no podrían hacer llegar una tarjeta a todos sus usuarios, no ya sólo por cuestiones económicas o logísticas, sino porque también supone introducir un retraso en la compra que puede llevar a perder usuarios potenciales.

3.- EL SOFTWARE:

Actualmente, ya existen programas de software (llamados anti-phishing) que se integran como una barra de herramientas más en los navegadores web y muestran la dirección real del sitio al que estamos accediendo.

CASOS REALES

A pesar de todas las medidas técnicas que hoy en día implementa la banca on-line y las advertencias que estas entidades realizan habitualmente sobre el riesgo de facilitar claves secretas a través de Internet, siguen produciéndose engaños de este tipo entre sus usuarios. Según el Observatorio Español de Internet, alrededor de 10.000 personas han sido víctimas de este tipo de ataques en los últimos tiempos. En estos momentos, lo que más preocupa al sector financiero, más que el daño económico que ocasiona realmente este tipo de delitos, es el daño a la credibilidad y a la confianza que sus clientes puedan tener en los servicios on-line.

Entre los últimos objetivos conocidos, han estado Caja Madrid, Banesto o BBVA, aunque en meses anteriores también se conocieron los ataques al Santander o al Banco Popular.

Ejemplo real de phishing sobre Caja Madrid:

"Estimado cliente de Banco CAJA MADRID! Por favor, lea atentamente este aviso de seguridad. Estamos trabajando para proteger a nuestros usuarios contra fraude. Su cuenta ha sido seleccionada para verificación, necesitamos confirmar que Ud. es el verdadero dueño de esta cuenta. Por favor, tenga en cuenta que si no confirma sus datos en 24 horas, nos veremos obligados a bloquear su cuenta para su protección".

En este caso, los datos se tecleaban en el cuerpo del e-mail para posteriormente ser enviados a un servidor ubicado en Taiwán, y a la vez, el usuario era redireccionado a la web oficial de Caja Madrid por lo que no sospechaba nada.

CONCLUSIONES

Gran parte del esfuerzo actual para evitar el phishing debe ir dirigido hacia la correcta formación del usuario final.

De todas formas, muchos expertos coinciden en afirmar que, mientras se confíe únicamente en el usuario para discernir si un correo es legítimo o no (y evitar así los ciberdelitos), siempre habrá alguno que se "equivoque".

Anti-Phishing Working Group APWG

LINKS:

- Anti-Phishing Working Group www.antiphishing.org
- Ejemplos de Phishing: www.antiphishing.org/phishing_archive.html
- Ejemplos de Phishing por correo: banksafeonline.org.uk/phishing_examples.html
- Ejemplos de SCAM: worldwidespam.info/phishing/

eCONTRATACIÓN: otras referencias

El Gobierno Vasco considera que la implantación del Modelo de Contratación Pública Electrónica constituye para las empresas vascas una *"oportunidad para la experimentación y la familiarización"* con respecto a un mecanismo que el conjunto de las Administraciones (Gobiernos, Diputaciones y Ayuntamientos) deberán adoptar en el futuro.

DICCIONARIO

(8) **Organizadores:**

- Dirección de Patrimonio y Contratación del Gobierno Vasco
  euskadi.net/kontratazioa
  euskadi.net/contratacion
- IVAP (Instituto Vasco de Administración Pública)
  www.ivap.org
- EIPA-CER (Instituto Europeo de Administración Pública - Centro Europeo de Regiones)
  www.eipa.nl

(9) **El Seminario en cifras:** El evento ha reunido a 14 expertos de distintos países ante un total de 200 asistentes. Para más detalle indicar que 13 de las 17 Comunidades Autónomas del estado español estaban representadas y 22 de los 25 países miembros de la Unión Europea.

La Dirección de Patrimonio y Contratación del Gobierno Vasco, el Instituto Vasco de Administración Pública (IVAP) y el Instituto Europeo de Administración Pública - Centro Europeo de Regiones(8) organizaron durante los días 7 y 8 de junio el 2º Seminario Internacional sobre Contratación Pública Electrónica que se desarrolló en Bilbao(9).

El Seminario reunió a numerosos expertos que desempeñan un papel fundamental en el proceso de Contratación Electrónica en sus países, con lo que se cubrieron los aspectos prácticos más relevantes de las diversas experiencias, y proporcionaron ejemplos de prácticas internacionales de países como: Noruega, Dinamarca, Austria, Canadá, Italia y Francia.

A lo largo de las dos jornadas se discutieron proyectos, dificultades encontradas en la implantación de la oferta electrónica, experiencias en la adopción de medidas para promocionar el uso de la Contratación Electrónica entre los proveedores, el uso de plataformas de Contratación Electrónica compartidas por los distintos órganos gubernamentales, y las disposiciones legales que regulan estas actuaciones.

El seminario estuvo dirigido a expertos de la contratación, abogados, empresas públicas y privadas, así como a miembros de las comunidades técnicas y académicas interesados en las innovaciones que están surgiendo en el campo de la Contratación Electrónica.

A continuación, y de forma resumida, se exponen algunas de las reflexiones expuestas.

ANTECEDENTES INTERNACIONALES

A finales de los años 90, la aparición de las modalidades de Comercio Electrónico activó el interés de las Administraciones Públicas por las posibilidades que Internet ofrecía en el ámbito de la Contratación Electrónica. Además, factores como el efecto-moda, los resultados reales obtenidos por las empresas multinacionales de distintos sectores (automóvil, electrónica, química,...), así como la aparición de proveedores de software y plataformas electrónicas de elevado eco mediático (Ariba, VerticalNet, Covisint,...) actuaron como detonantes de tal interés.

Australia, tanto a nivel de su gobierno federal, como de los gobiernos regionales de Victoria y Queensland, dieron los primeros pasos a nivel internacional en este terreno (convirtiéndose así en modelo para otras Administraciones). Ya en su momento, definieron tendencias tan representativas e innovadoras como son:

- Ofertar información de concursos y licitaciones a través de Internet.
- Desarrollar portales de compra y catálogos electrónicos para la adquisición de productos recurrentes.
- Desarrollar aplicaciones de licitación electrónica seguras para la remisión de ofertas por parte de las Empresas.

Posteriormente, otras Administraciones, como **Canadá** y diversos **Estados de América del Norte** (California, Virginia, Carolina del Sur) emprendieron el desarrollo de acciones semejantes a las ya iniciadas por Australia.

Por otra parte, si nos fijamos en ámbitos más cercanos al nuestro, por ejemplo a nivel europeo, hay que destacar las experiencias de **Gran**

Bretaña y de **Italia**, líderes, respectivamente, en la implantación de sistemas de licitación electrónica y de portales de compra de productos recurrentes y estándares.

De todas formas, a día de hoy, Australia sigue encabezando el pelotón de la Contratación

"La CAV fue la primera Comunidad que puso en marcha la Contratación Electrónica (octubre de 2005)."

Electrónica a nivel mundial, habiendo generado un conjunto de buenas prácticas, las cuales siguen siendo ineludibles (y por tanto, un ejemplo a seguir) en la expansión de la Contratación Electrónica en cualquier organismo público. Entre ellas podemos destacar:

- ✓ El desarrollo de labores de sensibilización y formación para impulsar la adopción de la Contratación Electrónica por parte de las empresas proveedoras.
- ✓ La disposición de la plataforma del Gobierno Australiano para su uso voluntario por otras administraciones locales y regionales.

Si nos fijamos en la Unión Europea (UE) como un conjunto, hay que decir que ésta también se ha interesado por la Contratación Electrónica. Así, ya a finales de 2001, y a propuesta de **Suecia**,

la Contratación Electrónica se integró en la lista de los *"servicios digitales básicos de los ciudadanos y de las empresas"*.

Es más, la UE estima, que el desarrollo del Plan de Contratación Electrónica constituye un paso lógico y natural en la digitalización de los servicios de cualquier Administración. Así, la directiva 18/2004/CE de contratación administrativa, de fecha 31 de Marzo de 2004, indica la obligatoriedad de transponer la normativa comunitaria a partir del 1 de Febrero de 2006 y recomienda que la Contratación Electrónica sea efectivamente implantada por los Estados miembros, a lo más tardar, a la conclusión del **año 2007**.

EN ESPAÑA

El lanzamiento de Planes de Acción en materia de Sociedad de la Información y de Administración Digital por parte de buena parte de los Gobiernos Autonómicos propició en su momento la aparición de los primeros intentos de incorporación de la Contratación Electrónica por parte de las Administraciones Públicas españolas. La **Generalitat de Cataluña**, la **Generalitat Valenciana** y la **Xunta de Galicia** fueron las que iniciaron los primeros movimientos en esta materia. De todas formas, dada la amplitud y complejidad de la tarea que pretendían abarcar desde el principio, tales iniciativas no condujeron a la implantación efectiva y real de los sistemas de Contratación Electrónica que pretendían. (10)

De forma paralela a todas las iniciativas tecnológicas desarrolladas, los órganos legales responsables de regular estos procedimientos administrativos, han ido aprobando todos los sustentos legales imprescindibles para implantar la Contratación Electrónica en la Administración con todo el valor jurídico y legal necesario; entre las que podemos señalar:

- ✓ El marco jurídico de la contratación electrónica de la Unión Europea.
- ✓ El marco jurídico europeo y estatal de la firma electrónica.
- ✓ El marco jurídico estatal de los registros y las notificaciones telemáticas.

GOBIERNO VASCO

En cuanto a la actividad del Gobierno Vasco se

DICCIONARIO

(10) Si hablamos de Sistemas de Presentación Electrónica de Documentos a través del cual se comunican y transmiten documentos relativos por ejemplo a poderes, hay que mencionar el proyecto estatal **SILICE** (Sistema de Información para la Licitación y Contratación Electrónica. Guías Técnicas Aplicables a la Adquisición de Bienes y Servicios Informáticos), transformado posteriormente en el aplicativo **PLYCA** (**P**royecto de **L**icitación **y** **C**ontratación **A**dministrativa) implantado por el Gobierno de Canarias, que vienen a demostrar que puede considerarse cumplido el objetivo inicial de Mejorar la eficiencia en la licitación y contratación en las Administraciones Públicas a través del uso de medios electrónicos, informáticos y Telemáticos.

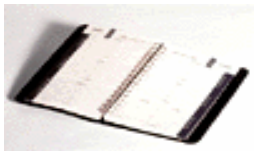
refiere, en el año 2002, el **Plan Euskadi en la Sociedad de la Información** (PESI) abría el camino de la Contratación Electrónica en la Administración vasca, cuando, con el objetivo de *"agilizar los procesos de aprovisionamiento del Gobierno y facilitar la accesibilidad a los expedientes de contratación"* iniciaba prácticas propias de la Contratación Electrónica. En una fase ulterior, con fecha 7 de abril de 2004, la Comisión Delegada para Asuntos Económicos (CDAE) del Gobierno Vasco aprobó las líneas básicas del proyecto de Contratación Electrónica.

Gracias al trabajo desarrollado en los últimos **4 años**, la Comunidad Autónoma Vasca fue la primera Comunidad que puso en marcha la Contratación Electrónica (realizándose la **primera apertura de plicas en octubre de 2005**), siendo el objeto de esa primera licitación electrónica, precisamente, la *"Asistencia para la Implantación de la Contratación Electrónica"*.

➢ **La formación y apoyo al usuario**

Como es por todos sabido, los mecanismos digitales previstos en la Contratación Pública Electrónica son novedosos para todos los participantes. Es por ello que los Responsables del Proyecto en el Gobierno Vasco (entre otras muchas medidas), han puesto especial cuidado en la formación y apoyo al usuario final (tanto empresas licitadoras como personal de la propia Administración), creando para ello un **Centro de Soporte a Usuarios** cuyas características son las siguientes:

- Consta de 41 personas en 3 niveles



DICCIONARIO

(11) El Gobierno Vasco ha establecido un detallado Plan de Implantación que tiene por objeto la adopción de la Contratación Electrónica por parte de las potenciales empresas proveedoras. Para ello, la Administración vasca está desarrollando un conjunto de actividades informativas y formativas tanto para las 3.136 empresas que constan en el registro público como para las que no lo están. A estas acciones se suma ahora un **"Servicio de Alerta Temprana"** sobre expedientes susceptibles de ser objeto de licitación electrónica, que advertirá con 30 días de antelación a las empresas sobre el lanzamiento de un expediente de contratación, permitiendo así que las que estén interesadas puedan prepararse y formarse con tiempo para afrontar con garantías y suficiencia una licitación electrónica.

GOBIERNO VASCO

Empresas proveedoras

Según las distintas experiencias internacionales de implantación (dadas a conocer durante las sesiones celebradas en Bilbao), éstas demuestran que la Contratación Electrónica requiere de *"algo más"* que una aplicación de Licitación Electrónica.

Así, ejemplos de países próximos demuestran que es preciso desarrollar acciones específicas de **sensibilización** y **formación** de las empresas proveedoras. De no ser así, se estima que las ofertas recibidas por procedimientos digitales solo alcanzarán niveles de 1 oferta digital por cada 1.000 ofertas en papel.

Conscientes de ello, los Responsables del Gobierno Vasco tienen previsto realizar acciones específicas de formación y sensibilización para las 3.136 empresas que, a día de hoy, se encuentran registradas en el Registro Oficial de Contratistas.(11)

Los Departamentos

El Plan de Contratación Electrónica del Gobierno Vasco se define como un **proyecto progresivo**, pues pretende ir incorporando al sistema a todos los órganos que contratan, empezando por la Comisión Central de Contratación (CCC), los diversos Departamentos, sus Organismos Autónomos y sus Entes Públicos de Derecho Privado, así como otras Administraciones que lo deseen.

Complejidad

Para hacernos una idea de la complejidad del proyecto, indicar que sólo en el ámbito del Gobierno Vasco estamos hablando de cientos de funcionarios y cargos implicados, con 100 Mesas de contratación, 150 Órganos de Contratación e innumerables órganos de gestión, prácticamente tantos como Direcciones y servicios existan, pues todas ellas contratan y además han de contratar con el mismo procedimiento.

- Ofrece un punto central de contacto directo con las empresas.
- Ofrece asesoramiento en el manejo de las aplicaciones.

"Australia sigue encabezando el pelotón de la Contratación Electrónica a nivel mundial."

➢ **Nuevas modalidades de contratación**

El Gobierno Vasco desea imprimir una actitud proactiva a este proyecto en el cumplimiento de la directiva comunitaria 18/2004/CE. Es por ello que desea avanzar aún más en la adopción de las nuevas modalidades de contratación electrónica que no han sido incluidas en esta primera fase, y que son entre otras, los Sistemas de adquisición dinámicos y las Subastas electrónicas.

CONCLUSIÓN

Las ventajas del correcto diseño de estos procedimientos son evidentes: se agiliza el procedimiento de adjudicación de los contratos; supone una minimización de errores en la mecanización de las ofertas recibidas al hacerse el vuelco de las mismas de forma automatizada; e implica una disminución de las cargas del personal público.

Información

Para más información sobre aspectos relacionados con este tema se pueden consultar los siguientes documentos:

- Artículo "Proyecto eContratación" (Boletín Nº 15, sección Alboan, septiembre 2004)
- Artículo "Premios Tecnimap" (Boletín Nº 15, sección Breves, septiembre 2004)
- Artículo "Servicios de Licitación y Notificación Electrónica (SLNE)" (Boletín Nº 11, sección Alboan, julio 2003)
- Artículo "eGovernment" (Boletín Nº 8, junio 2002)

PROYECTOS INTERNACIONALES DE REFERENCIA

Australia

- AusTender (Australian Government Tender System); Sistema de contratación electrónica del Gobierno Federal. (https://www.tenders.gov.au).
- Smartbuy del Gobierno de Nueva Gales del Sur (www.smartbuy.nsw.gov.au)
- Queensland Government Marketplace eTender System, del Gobierno de Queensland. (www.projectservices.qld.gov.au/etenderqgm).
- Victorian Government Purchasing Board. Autoridad de Contratación del Gobierno de la Región de Victoria (www.vgpb.vic.gov.au)

USA

- Estado de Carolina del Norte. (www.ncgov.com/eprocurement/asp/section/ep_index.asp).
- Eva. Portal de compras del Estado de Virginia. (http://eva.state.va.us).
- Portal de compras del Estado de California. (www.pd.dgs.ca.gov).

Canadá

- MERX: Web Informativa a Licitadores. (www.merx.com)
- Contracts Canada: Acción de promoción, marketing y difusión de la contratación pública entre las empresas. (http://contractscanada.gc.ca).
- SourceCAN: Market Place Electrónico, promocionado por la Administración Federal Canadiense para la sensibilización de las Empresas (www.sourcecan.com).

Gran Bretaña

- OGC (Office of Government Commerce). Central de Compras del Gobierno Británico. (www.ogc.gov.uk).
- Ciudad de Leeds: proyecto de eProcurement líder europeo en el ámbito municipal. (www.leeds.gov.uk)

Bélgica

- Portal de compras federal. (www.jepp.be).

Italia

- Consip: Portal de compras de la administración pública italiana. Está considerado el más avanzado de Europa. (www.consip.it).

Irlanda

- Basis. Canal Empresa del Gobierno Irlandés. (www.basis.ie).

Dinamarca

- Portal de Compras de Dinamarca. (www.gatetrade.net)

ALBOAN:

Trafikoa Euskadiko Trafikoa Kudeatzeko Zentroa
Tráfico Centro de Gestión de Tráfico de Euskadi

Departamento de Interior

Hasta hace poco tiempo la ordenación, regulación, vigilancia y control del tráfico y la circulación viaria, así como la asistencia a los usuarios de las vías públicas, se ha venido ejerciendo mediante el despliegue de patrullas policiales en las carreteras. Sin embargo, este modelo de gestión del tráfico se muestra en muchas ocasiones poco eficaz a la hora de afrontar y dar una **rápida solución** a los problemas que se presentan en nuestras carreteras (el cual tiene su origen en el crecimiento exponencial del tráfico que hemos sufrido en los últimos años).

Dada la magnitud que ha adquirido este problema, se hace necesario adoptar un enfoque global de la situación, basándose para ello en el conocimiento en tiempo real del estado de toda la red de carreteras en cada momento, lo cual facilita la planificación de las actuaciones y la adopción de medidas de ordenación y regulación del tráfico.

Con ese claro objetivo, y siendo conscientes de las ventajas que proporcionaban las Nuevas Tecnologías, desde la Dirección de Tráfico del Departamento de Interior se decidió dar los pasos necesarios (partiendo del Decreto 87/2001) para poner en marcha el 8 de junio de 2005 el denominado *"Centro de Gestión de Tráfico de Euskadi"* (CGTE).

PROYECTO ARTS

El desarrollo del CGTE está estrechamente ligado a las iniciativas impulsadas desde la Unión Europea (UE) y, en concreto, al **Proyecto ARTS** (*Advanced Road Telematics in South West*).

La UE pretende impulsar la realización de proyectos internacionales para el desarrollo y aplicación de sistemas de control de tráfico en la Red de Carreteras Transeuropeas, lo cual afectará a más de 70.000 Kms de carreteras y autopistas. En este sentido, la participación del País Vasco en este contexto es importante debido a la situación geográfica estratégica que ocupa dentro de la red transeuropea de carreteras.

EL CGTE

A la hora de implantar un Centro de estas características, los Responsables del mismo, constataron que el antiguo centro desde el que se dirigía el tráfico en el País Vasco resultaba totalmente insuficiente para dar respuesta a las nuevas necesidades; es por ello que se decidió centralizar todos los servicios en un único sitio físico, ubicando su nueva sede en el barrio bilbaíno de Txurdinaga.

Este nuevo Centro, que alberga el Sistema de Gestión de Tráfico interurbano, esta integrado dentro de la red transeuropea, y permite monitorizar las 24 horas del día y los 365 días del año la red de carreteras en tiempo real. De esta forma se facilita la adopción de decisiones y medidas para regular, controlar u orientar el estado de la circulación por las vías interurbanas en cada momento, evitando así eventuales congestiones como consecuencia de incidentes de tráfico, etc. Todo ello permite utilizar los efectivos policiales de un modo mucho más eficaz a la hora de garantizar la seguridad y protección tanto de viajeros como de mercancías.

Una vez *"ubicado"* el centro, el siguiente paso fue potenciar la infraestructura tecnológica que daría soporte al CGTE.

Dada la importancia del servicio que se pretendía soportar, las directrices emanadas del proyecto para esta fase, (el cual posibilitaba el paso de un entorno Host a otro de servidores estándares), daban máxima prioridad a la **integración** de todos los elementos tecnológicos y a la **fiabilidad** y **escalabilidad** de los mismos, todo ello con el objetivo de evitar posibles *"caídas"* en el servicio.

En relación a los servidores albergados en el CPD, indicar que se encuentran configurados en cluster, contemplan balanceos de carga e incluyen redundancia para sus elementos. La mayor parte de esta plataforma de hardware está basada en servidores HP ProLiant (modelos DL580 y DL380).

Por otra parte, el Sistema Operativo sobre el que corren las aplicaciones es Microsoft Windows2003 Server. Microsoft también proporciona el software en el ámbito de la mensajería (con Exchange) y la base de datos (SQL Server). La gestión de uno de los elementos más espectaculares del Centro, el *videowall* (que se encuentra dentro de la *"Sala de Operaciones"*), se basa en una solución Open-Source.

La Infraestructura de **Comunicaciones** esta formada por la red de Fibra Óptica, que es uno de los elementos clave de toda la parte tecnológica. Ello queda reflejado en la atención que requirió en su momento para definir su tipología, el plan de instalación y estudiar su futura evolución. La tecnología escogida fue Gigabit-Ethernet, la cual interconecta actualmente alrededor de 100 cámaras repartidas por toda la red viaria vasca, permitiendo obtener información en tiempo real.

A la hora de hablar de la Infraestructura de **Conectividad**, podemos decir que el Centro cuenta con 3 líneas de acceso soportadas por dispositivos de Cisco Systems (con software IPSec) gracias a los cuales se integran voz y datos y se proporcionan capacidades de acceso seguro tanto a Internet como Extranet o Intranet vía VPN. Los **operadores** encargados de proporcionar el acceso redundante y duplicado de Internet son Euskaltel y Sarenet.

ELEMENTOS DEL SISTEMA

1- **Sistemas telemáticos para la administración del tráfico** (los cuales incluyen: sensores, circuito cerrado de televisión, postes de auxilio, estaciones meteorológicas, paneles de mensaje variable,...)

2- **Instalaciones, medios y recursos desplegados en la red de carreteras**. (elementos periféricos, red de telecomunicaciones, centro de gestión de tráfico, servicios de tráficos de la Ertzaintza,...)

3- **Mecanismos de planificación estratégica y táctica** (gestión semafórica en tiempo real, control lineal de la velocidad, control de accesos, gestión de carriles, información al usuario,...)

EL PORTAL WEB

Otro punto a destacar es el **Portal Web** www.trafikoa.net, el cual se puede considerar como la *"guinda"* de toda esta infraestructura, ya que alberga y difunde toda la información del tráfico que llega al Centro.

A través de esta página web, el ciudadano puede conocer el estado real del tráfico en cada momento, ya que en él se recogen las últimas incidencias acaecidas (planificadas o no), el estado del acceso a las tres capitales vascas, y un completo mapa donde quedan registradas las obras y/o los accidentes. Otro área muy consultado en invierno es el estado de los puertos de montaña, cuya información se muestra al usuario clasificada por provincias y carreteras.

En otro de los apartados que conforman el portal, también es posible encontrar información sobre los planes estratégicos, múltiples trámites de interés para los conductores, educación vial, escuelas particulares de conductores o, incluso, estadísticas de accidentes.

Por último, indicar que con el objetivo de mejorar el servicio que se presta al Ciudadano, la Dirección de Tráfico pretende impulsar distintos acuerdos de colaboración en materia de gestión del tráfico (y seguridad vial) tanto con los municipios vascos, como con otras administraciones del Estado, así como con otros organismos enmarcados en la Red Transeuropea de Carreteras.

"El desarrollo del CGTE está estrechamente ligado a las iniciativas impulsadas desde la Unión Europea y, en concreto, al Proyecto ARTS."

- Página Web: www.trafikoa.net
- Decreto 87/2001, de 22 de mayo, por el que se Regula el Sistema de Gestión del Tráfico Interurbano en la Comunidad Autónoma de Euskadi, y se crea el Centro de Gestión de Tráfico de Euskadi. BOPV Nº 115, (18 de junio de 2001)

902 112 088 TRAFIKOA

Nº 22

Junio de 2006

¡¡BREVES!!

TECNIMAP 2006

Más de 9.000 asistentes se han dado cita en las IX Jornadas sobre TIC para las Administraciones Públicas, también llamadas TECNIMAP, celebradas en esta ocasión en la ciudad de Sevilla del 30 de mayo al 2 de junio.

Este evento bienal que se viene realizando desde 1989, y que es organizado por el Ministerio de Administraciones Públicas (MAP), tiene como objetivo principal el compartir ideas y experiencias sobre modernización y aplicación de las Tecnologías de la Información en el sector público, y sobre todo, qué planes y herramientas están poniendo en marcha éstas en sus respectivas Comunidades para conseguir la incorporación de sus ciudadanos a la Sociedad de la Información.

Begoña Gutiérrez (Directora de Informática y Telecomunicaciones)

El formato de la presente edición, como viene siendo habitual, habilitó un área de exposiciones donde las distintas Comunidades Autónomas (y las empresas privadas participantes) pudieron ubicar sus Stands. De forma paralela, se celebraron una serie de mesas redondas donde participaron destacados representantes públicos y privados. En la segunda de estas mesas, titulada *"Convergencia Digital y posibilidades para el desarrollo de servicios electrónicos"*, intervino Begoña Gutiérrez, Directora de Informática y Telecomunicaciones.

Nuestra participación

Otro apartado donde el Gobierno Vasco tuvo la oportunidad de dar a conocer los proyectos más innovadores que está desarrollando actualmente, fueron las distintas sesiones de trabajo que se organizaron durante el Congreso, las cuales incluían la Ponencia del tema elegido. A continuación se lista el titulo de los temas expuestos y sus ponentes:

-DOMA: *"Portal Corporativo euskadi.net"*, ponente: Javier Arrese.

-Departamento de Hacienda y Administración Pública: *"Contratación Pública Electrónica"*, ponente: Ángel Cancelo.

-Departamento de Medio Ambiente y Ordenación del Territorio: *"GIS Corporativo geoEuskadi"*, ponente: Pedro Isasi.

-DIT/EJIE: *"PLATEA: Plataforma de Administración Electrónica"*, ponente: Juan Pedro Álvarez.

De izquierda a derecha: Carmelo Arcelus (Viceconsejero de Administración y Servicios), Agustín Elizegi (Director de EJIE) y Begoña Gutiérrez (Directora de Informática y Telecomunicaciones)

-Departamento de Industria, Comercio y Turismo: *"Tramitaciones telemáticas"*, ponente: Ricardo Pereda.

-DIT: *"Centros KZgunea como soporte a la eAdministración"*, ponente: Txomin Alkorta.

-Departamento de Interior: *"Voto Electrónico"*, ponente: Itziar Lizeaga.

Vista del Stand del Gobierno Vasco en el Tecnimap

Por último, indicar que el Gobierno Vasco dispuso durante los cuatro días que duró el Congreso de un Stand donde se informó y facilitó todo tipo de información sobre los proyectos más actuales: Servicios de Firma Electrónica de Izenpe, Sistemas de Información estadística del Eustat, así como de todos los temas expuestos en las Ponencias antes señaladas.

Web oficial del Congreso: www.tecnimap.es