— Ejemplar en Castellano (*) —

Aurrera !

Boletín Divulgativo de Nuevas Tecnologías en Informática y Telecomunicaciones

Publicado por el Gabinete Tecnológico de la DIT

Nº 20

Diciembre de 2005

Enviad vuestras sugerencias a: aurrera@ej-gv.es

ÍNDICE

¿Qué es la seguridad?, ¿se puede medir?, ¿cómo se establece?. Cuando los informáticos hablamos de la seguridad que nos reporta un Sistema o Producto Informático ¿a que nos estamos refiriendo exactamente?. Siempre hemos entendido la Seguridad relacionada con las Tecnologías de la Información como algo subjetivo y muy difícil de "calcular". Pues bien, resulta que desde hace más de 20 años, expertos de diferentes ámbitos están trabajando para hacer que esa subjetividad desaparezca e intentar convertirla (en la medida de lo posible) en una ciencia. Y es precisamente lo que se describe en el primero de los temas: la evolución y las distintas aproximaciones que se han desarrollado desde diferentes instancias y su posible convergencia bajo unas mismas siglas, las CC.

Como segundo gran tema, aparece el titulado "Videoconferencia", que tal y como refleja su subtítulo, pretende dar unas nociones básicas a través de una serie de Preguntas/Respuestas sobre el mundo de la Videoconferencia y todo lo que le rodea. Este artículo pretende ser por lo tanto, una breve introducción al seminario que el Gabinete Tecnológico tiene previsto organizar en breve para dar a conocer todas las posibilidades de esta Tecnología en nuestra Administración.

Por otro lado, el Departamento de Hacienda (a través del apartado Alboan) nos detalla en esta ocasión las características de un "viejo conocido" de la Administración Pública: el Boletín Oficial del País Vasco, el cual, tal y como veremos, tiene mucho que contarnos.

Por último, y como suele ser habitual, en el apartado "Breves" hemos incluido dos noticias de diferente índole: una de ellas referida al mundo del Software (y que detalla una nueva utilidad que acaba de poner en marcha Google para medir la audiencia de una web), y la otra referida al mundo del Hardware (donde se informa de las nuevas tendencias existentes en el mundo de las memorias).

(*) Los ejemplares en Castellano y Euskera están disponibles en la Intranet "Jakina".

COMMON CRITERIA

La evaluación y certificación de productos técnicos, siguiendo criterios estandarizados e internacionalmente aceptados, permite a las empresas demostrar objetivamente la seguridad de sus productos y a los usuarios estar más seguros de lo que compran.

DICCIONARIO

(1) **TCSEC**: Trusted Computer System Evaluation Criteria

(2) **ITSEC**: Information Technology Security Evaluation Criteria

(3) **CTCPEC**: Canadian Trusted Computer Product Evaluation Criteria

(4) **FCITS**: Federal Criteria for Information Technology Security

(5) **FIPS**: Federal Information Processing Standards

Las certificaciones de productos son una serie de procedimientos mediante los cuales una parte imparcial (llamada **Entidad Certificadora**) asegura que un producto, proceso o servicio cumple con unos requisitos concretos de acuerdo a unos criterios prefijados. Gracias a esta certificación, los **proveedores** pueden avalar la calidad de sus productos y los **usuarios** pueden tener la seguridad de que el producto elegido cumple con los requisitos prometidos. En definitiva, se trata de una especie de "control de calidad".

"Los Common Criteria son un método de evaluación para medir la Seguridad de los Sistemas de Información."

ANTECEDENTES HISTORICOS

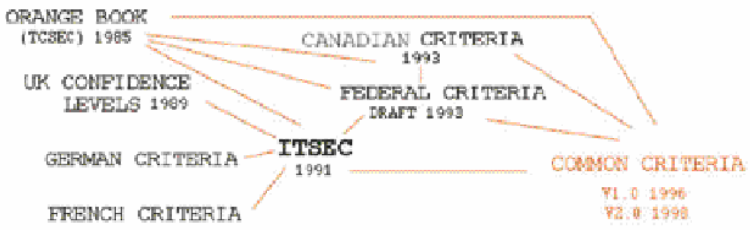
El mundo de las Tecnologías de la Información -TI- (al igual que cualquier otro sector) tampoco es ajeno a este tipo de certificaciones. En esta ocasión, y a lo largo de este artículo, mencionaremos las certificaciones de seguridad relacionadas con las TI y su evolución durante los últimos años.

La historia de estas certificaciones comienza a principios de los años 80, cuando en EEUU se desarrollaron los criterios de seguridad TCSEC(1) y que fueron editados en el llamado "libro naranja". Más adelante, en 1991, y partiendo de las TCSEC, la Comisión Europea publicó el ITSEC(2), desarrollado conjuntamente por Francia, Alemania, Holanda y Reino Unido, con la intención de conseguir unos criterios mucho más flexibles frente a la constante evolución de las Tecnologías de la Información.

Poco después, en 1993, Canadá desarrolló los criterios CTCPEC(3) uniendo los criterios americanos y europeos anteriormente comentados. Ese mismo año el Gobierno americano publicó los FCITS(4) como una segunda aproximación que combinaba las normas europeas y americanas.

LOS CRITERIOS COMUNES

Tal y como se puede comprobar, a lo largo de la historia se han ido definiendo diferentes criterios y/o métodos de evaluación para medir la seguridad de los Sistemas de Información, unos con mayor aceptación que otros, hasta llegar a un punto en que la disparidad de criterios hizo necesaria una unificación de todos ellos.



Con ese objetivo de crear un estándar común, a principios de los años 90 desde

la Organización ISO (International Organization for Standardization) se comenzó a trabajar en la homogeneización de unos criterios que fuesen reconocidos internacionalmente. Tras varios años de trabajo, se obtuvo como resultado la certificación "Common Criteria" (o ISO-IEC 15408).

Actualmente, los Common Criteria o Criterios Comunes (CC) son ya una certificación internacionalmente reconocida que es utilizada por gobiernos u organizaciones para evaluar la seguridad en productos de TI. Tanto es así, que en algunos casos los CC son usados como condición necesaria para concurrir a **concursos públicos**.

Con posterioridad al trabajo realizado por la ISO (y tras muchas negociaciones entre distintas Administraciones e industria), varios Gobiernos (entre ellos EEUU, Canadá, Francia, Alemania, Reino Unido, ...) firmaron un acuerdo (al que posteriormente se han ido adhiriendo otros países) por el que se comprometían a reconocer las certificaciones de seguridad sobre productos TI que siguiendo las directrices de los "Common Criteria" se hiciesen en cualquiera de esos países.

En estas negociaciones participaron hasta 14 países, entre los que figuraba España a través del Ministerio de Administraciones Publicas (MAP).

(http://www.map.es/csi/pg3432.htm)

Este tipo de acuerdos tienen como principal objetivo el aumentar la confianza

LOS NIVELES

Los CC han establecido una escala de seguridad (llamada Evaluation Assurance Levels o EAL) que va desde EAL1 hasta EAL7:

•**EAL1** (probado funcionalmente). Se trata del nivel básico. Es aplicable cuando no se consideran serias amenazas contra la seguridad. La evaluación puede realizarse sin ayuda del desarrollador y los costes, por lo tanto, son mínimos. La conclusión a este nivel es que el TOE[6] funciona como indica la documentación que lo acompaña y que ofrece una protección útil contra las amenazas identificadas.

•**EAL2** (probado estructuralmente). Nivel moderado de seguridad. Se necesita la cooperación del desarrollador para el suministro de informaciones relativas al diseño. En este caso se emplean pruebas de desarrollo de "caja negra" y búsqueda de vulnerabilidades obvias.

•**EAL3** (Probado y verificado metódicamente). Nivel medio de seguridad. Se aplica cuando los usuarios exigen un nivel de seguridad moderado. EAL3 exige un análisis apoyado en pruebas de "caja gris" (de nivel alto) y la prueba de que el desarrollador ha investigado el descubrimiento de las vulnerabilidades evidentes.

•**EAL4** (Diseñado, probado y verificado metódicamente). Nivel alto de seguridad. Exige un análisis sustentado en el diseño global (de bajo nivel) de los módulos del TOE, así como la correcta implantación de un subconjunto de elementos.

•**EAL5** (Diseñado y probado semi-formalmente). La investigación de vulnerabilidades ha de asegurar la resistencia a las tentativas de penetración con un potencial de ataque moderado. También se imponen una arquitectura modular y el análisis de los canales ocultos.

•**EAL6** (Diseñado, probado y verificado semi-formalmente). Se aplica al desarrollo de TOE especializados dedicados a la seguridad que vayan a utilizarse en situaciones dónde existen riesgos elevados y el valor de los bienes justifica costes más importantes. La investigación de las vulnerabilidades tiene que asegurar la resistencia a las tentativas de penetración con un potencial de ataque elevado. También se exige unos controles profundos del entorno de desarrollo

•**EAL7** (Diseñado, probado y verificado formalmente). Se aplica al desarrollo de TOEs dedicados a la seguridad que deban utilizarse en situaciones dónde existen riesgos extremadamente elevados o el valor de los bienes justifica costes de desarrollo más importantes. Se requiere probar que el desarrollador ha efectuado pruebas de "caja blanca", así como una confirmación independiente y completa de los resultados de las pruebas realizadas por el desarrollador.

DICCIONARIO

[6] Siglas a tener en cuenta:

- TOE: los "Target Of Evaluation" (Objetivos de Evaluación) son **la parte** del producto que se va a evaluar.
- Requisitos Funcionales ("functionality requirements"): Definen el **comportamiento** de seguridad deseado frente a las amenazas que están presentes.
- Requisitos para el aseguramiento ("assurance requirements"): Son las **propiedades** del Target Of Evaluation (TOE) que garantizan que la seguridad que el TOE dice proporcionar es efectiva y está implementada correctamente.
- Protection Profile (PP): El PP especifica **el entorno** donde se utilizará el TOE (amenazas a las que se esta expuesto), los objetivos de seguridad y los requisitos de seguridad que el TOE debe satisfacer para alcanzar los objetivos de seguridad.

un país en marcha

EUSKO JAURLARITZA GOBIERNO VASCO

de los usuarios en los productos de TI que éstos contratan. Para ello, se le facilita información y criterios objetivos que le ayudarán a tomar sus decisiones dejando a un lado valoraciones que pueden ser más subjetivas. En este sentido, los CC, como estándar internacional que son, aportan las siguientes ventajas:

"Los CC son ya una Certificación internacionalmente reconocida."

- Permiten al usuario comparar sus requerimientos específicos frente a los niveles establecidos por los CC para decidir el nivel de seguridad que necesita [Ver cuadro "Los Niveles"].
- Permiten al usuario saber cuándo un producto cumple una serie de requisitos.
- Exigen a los fabricantes de los productos una exhaustiva documentación sobre los productos evaluados.
- Proporcionan al usuario plena confianza en las evaluaciones, ya que estas son realizadas por laboratorios independientes (y no por los propios fabricantes).

Si bien el objetivo de todos certificados es el mismo (analizar y puntuar un producto) la diferencia entre ellos es que los CC son más útiles para evaluar un producto como

puede ser un Sistema Operativo -SO- (el cual es amplio y difícil de ajustar a estándares determinados) mientras que, por ejemplo los estándares ITSEC y FIPS[5] son más útiles para evaluar productos más específicos, como puede ser un microcircuito que realiza un determinado cifrado (el cual debe cumplir un estándar muy concreto).

VALIDEZ DE LOS CERTIFICADOS

Además de los CC, tal y como hemos mencionado en la introducción, existen otros estándares de certificación de seguridad como pueden ser los ITSEC, TCSEC, los FIPS, etc.

De todas formas, independientemente del tipo de certificado elegido, hay ciertas características que todos ellos tienen que cumplir. Por ejemplo, es necesario que ese Certificado tenga un **periodo de validez** bien definido, tras el cual se debe proceder a su revisión para renovar su vigencia. Además, se debe asegurar que la Entidad Certificadora es **imparcial** y sigue unos criterios universales y **estandarizados**.

Es importante saber que los Certificados se encargan de evaluar un producto bajo unas condiciones muy concretas en un momento determinado.

Por esa razón, es muy probable que, si el producto que nosotros como usuarios hemos comprado no se encuentra bajo las condiciones definidas en el certificado, la seguridad del producto se vea comprometida. Esto puede ocurrir, por ejemplo, en el caso de un SO certificado, al cual se le instalan a posteriori ciertas aplicaciones que pueden "debilitar" su seguridad.

Debido a ello, si queremos evaluar la validez de un certificado, es imprescindible conocer en detalle el proceso que ha seguido desde la petición del certificación hasta la emisión del certificado por parte del Laboratorio certificador. [Ver "¿Garantía de Seguridad vs. Marketing?"]

LOS LABORATORIOS

En España la certificación de productos de seguridad corre a cargo un organismo como es el Centro Criptológico Nacional (CCN), quien ha adoptado los estándares CC y el ITSEC.

Sin embargo, cabe recordar que España ha firmado un acuerdo de equivalencia (o Reconocimiento Mutuo)

¿Garantía de Seguridad o Marketing?

Algunos expertos estiman que una Certificación no asegura que los requisitos evaluados cubran las necesidades del usuario, ni que las circunstancias especiales bajo las que se ha testeado el producto se den en el entorno real del usuario, ni pueden garantizar que el producto en su próxima versión siga cumpliendo esos mismos requisitos, y mucho menos puede asegurar que dentro de unas semanas no se descubra una vulnerabilidad crítica que ponga en entredicho el producto analizado.
De todas formas, estos mismos expertos, consideran que la obtención de estos certificados por parte de un producto es un indicador positivo, si bien no garantizan su seguridad global ni la adecuación total a nuestras necesidades reales.

de los productos certificados por otros laboratorios.

- Relación de documentos del Acuerdo de reconocimiento mutuo de certificados de la evaluación de la seguridad de las TI:

http://www.csi.map.es/csi/pg3410.htm

- Arreglo sobre el reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de la TI

www.csi.map.es/csi/pdf/acuerdo.pdf

En el mundo existe un número limitado de laboratorios que están oficialmente acreditados para realizar evaluaciones basadas en Common Criteria.

- Listado de Laboratorios:

www.commoncriteriaportal.org/public/consumer/index.php?menu=7

- Listado de Productos Certificados:

www.commoncriteriaportal.org/public/consumer/index.php?menu=4

CONCLUSIONES

Dada la diversidad de métodos y las distintas interpretaciones existentes sobre los mismos, la adopción en su momento de un estándar como puede ser el Common Criteria se consideró como un paso muy importante para el mundo de la seguridad de las TI. En cualquier caso, no hay que olvidar que cuando se certifica un producto, su validez está condicionada a las condiciones exactas del test realizado. Por tanto, a la hora de valorar un producto no es fácil asegurar que éste es más seguro que otro simplemente porque alguna de sus versiones este certificada.

"Toda evaluación debe implicar **Imparcialidad**, **Repetibilidad**, **Reproducibilidad** por otros evaluadores, **Completitud** en los resultados y equilibrio coste-eficacia."

CRITERIOS DE CERTIFICACION DE PRODUCTOS DE SEGURIDAD	
TCSEC ("orange book - libro naranja")	**ITSEC ("white book - libro blanco")**
✓ 1985 (Trusted Computer Security Evaluation Criteria) ✓ Criterios Norteamericanos ✓ Recomendaciones del Dpto. de Defensa ✓ Se detallan criterios de seguridad de HW y SW básico, así como metodologías de evaluación de la seguridad en los SI ✓ Permiten examinar el sistema comprobando si las funciones de seguridad están presentes y si funcionan correctamente. ✓ Una Agencia Gubernamental es la que evalúa los productos. ✓ Los productos se clasifican en: • Nivel D (menor nivel de seguridad) • Nivel C1, C2 • Nivel B1, B2, B3 • Nivel A1 (mayor nivel) ✓ La mayoría de los sistemas operativos están en el nivel C2 ✓ Inconvenientes: • Excesivo coste y duración (1 a 3 años) • Excesiva orientación a Sist. Operativos • Demasiado énfasis en confidencialidad (origen militar).	✓ 1991 ✓ Criterios Europeos (Alemania, Francia, Reino Unido y Holanda). ✓ Se analiza la confidencialidad, integridad y disponibilidad ✓ Se evalúan productos y/o sistemas para entornos específicos ✓ Los productos dispondrán de funciones como: controles de acceso, auditoria, recuperación de errores, etc. ✓ Se evalúa la corrección con la que están desarrollados, la operatividad funcional de las medidas y su efectividad frente a las amenazas. ✓ Define 10 clases de funcionalidades, de las cuales 5 equivalen a niveles de TCSEC: • ITESEC: F-C1, F-C2, F-B1, F-B2, F-B3 • TCSEC: C1, C2, B1, B2, B3/A1 ✓ Inconvenientes: • Evaluación larga (9 meses) • Falta de reconocimiento entre países • Falta de interés del sector privado
Common Criteria	**FIPS 140-1**
✓ 1996 v1.0 - 1998 v2.0 ✓ USA + Europa ✓ Iniciativa conjunta para armonizar TCSEC e ITSEC ✓ www.commoncriteria.org ✓ Niveles de seguridad: • De EAL1 (nivel básico) al EAL7 (nivel alto) ✓ Ventajas: • Reconocimiento mutuo de la certificación • Mayor interés del sector privado	✓ FIPS (Federal Information Processing Standard) y 140-1 (Security Requirements for Crypto Modules) ✓ Se verifican estos parámetros: • Diseño y documentación del módulo cripto • Interfaces, roles-servicios, modelo utilizado • Seguridad del SO • Gestión de claves • Algoritmos criptográficos • Emisiones Electrómagnéticas (EMI/EMC) • Autotests ✓ 4 Niveles

VIDEOCONFERENCIA (CONCEPTOS BÁSICOS)

Cada vez más organizaciones adoptan la tecnología de videoconferencia beneficiándose de sus numerosas ventajas.

DICCIONARIO

(7) El **Codec**: Las señales de audio y video que se desean transmitir suelen estar en formato analógico, por lo que para poder transmitir esta información a través de una red digital, ésta debe de ser transformada mediante algún método a una señal digital, una vez realizado esto se debe de comprimir y multiplexar estas señales para su transmisión. El dispositivo que se encarga de este trabajo es el CODEC (Codificador/ Decodificador) que en el otro extremo de la red realiza el trabajo inverso para poder desplegar y reproducir los datos provenientes desde el punto remoto.

Gracias a los avances tecnológicos, la integración de la voz, los desarrollos en la infraestructura de red, el vídeo, los datos y los precios cada vez más asequibles, la videoconferencia se está convirtiendo en una herramienta indispensable en el día a día de las organizaciones. A continuación veremos algunos conceptos básicos que nos ayudarán a visualizar el escenario completo de la comunicación visual y que servirá de introducción al seminario que sobre la videoconferencia se tiene previsto organizar a principios de 2006 por parte del Gabinete Tecnológico de la Dirección de Informática y Telecomunicaciones.

PREGUNTAS MÁS FRECUENTES

A continuación daremos respuesta a aquellas cuestiones que nos suelen plantear cuando participamos en una conversación sobre la Videoconferencia.

➢ **¿En que consiste la comunicación visual o videoconferencia?**

La videoconferencia permite una comunicación, colaboración y toma de decisión eficientes entre interlocutores que no están presentes en un mismo lugar. Se beneficia de muchas de las mismas ventajas de la comunicación cara a cara como la posibilidad de ver las expresiones faciales y el lenguaje corporal de sus interlocutores. De igual manera, permite a los participantes compartir informes, datos e información, facilitando así mismo la posibilidad de realizar presentaciones, revisar conjuntamente documentos y tomar decisiones con mayor rapidez.

➢ **¿Cuáles son los componentes necesarios para realizar una videoconferencia?**

Existen cinco componentes principales que constituyen el sistema de videoconferencia: una cámara, un micrófono, un monitor, un altavoz y un codec(7). La cámara y el micrófono captan la imagen y el sonido en un sitio. El codec, cerebro del equipo, convierte el vídeo y el

audio en una señal digital y la comprime enviándola por la red. En el otro extremo, otro codec descomprime la señal, proyecta la imagen en un monitor y el sonido en un altavoz. Puede parecer complicado pero el

proceso es transparente al usuario, ya que éste, desde el mando a distancia con el que se maneja el equipo, lo único que tiene que hacer es marcar el número del equipo remoto con el que se quiere poner en contacto y presionar el botón "Conectar"; es tan fácil como realizar una llamada telefónica.

➢ **¿Con quien puedo comunicar por videoconferencia?**

Puede utilizar su equipo de vídeo para colaborar con cualquier persona que tenga un equipo de videoconferencia o un teléfono basado en estándares, incluyendo compañeros de trabajo, empleados, clientes (o en el caso de la Administración los Ciudadanos) o proveedores.

"Los estándares garantizan la compatibilidad entre equipos de distintos fabricantes."

➢ **¿Cuanto tiempo se requiere para aprender a manejar un equipo de videoconferencia?**

Depende del equipo. Hoy día, los proveedores de este tipo de productos, intentan centrar gran parte de sus esfuerzos en conseguir que la facilidad de uso sea esencial, y por ello el mando a distancia de los equipos y los menús en pantalla pretenden ser muy intuitivos o "amigables".

➢ **¿Qué tipo de red necesito para realizar una videoconferencia?**

Se puede realizar una videoconferencia en casi cualquier red digital. Actualmente, la

RDSI es la red más utilizada, aunque las llamadas de vídeo sobre IP se están extendiendo cada vez más.

➢ **¿Qué tipo de calidad de vídeo y audio obtendré?**

Como regla general, cuanto mayor es el ancho de banda utilizado para conectar los equipos, mayor será la calidad de vídeo y audio. Como los equipos de videoconferencia priorizan el audio sobre el vídeo, el ancho de banda afecta sobre todo a este último. Como la calidad mínima aceptable es subjetiva, no se puede hablar de un ancho de banda mínimo para una videoconferencia, y además este ancho de banda mínimo también depende de la aplicación para la que se vaya a utilizar la videoconferencia (no es lo mismo una reunión de trabajo que una sesión de telemedicina, donde la señal no puede sufrir ningún tipo de interferencia y/o corte bajo ningún concepto). Por otra parte, no todos los equipos del mercado incorporan los últimos estándares en audio y vídeo, que mejoran considerablemente su calidad. Este es un aspecto importante a tener en cuenta a la hora de valorar un equipo u otro, ya que algunos equipos pueden incorporar nuevas funcionalidades y estándares con una simple actualización de software, lo que contribuye en gran medida a proteger la inversión realizada.

➢ **¿Por qué resulta importante elegir un equipo de vídeo basado en estándares?**

Los estándares garantizan la compatibilidad entre los equipos de distintos fabricantes. Al elegir equipos basados en estándares, se asegura que equipos distintos puedan interoperar entre si independientemente de quienes sean sus fabricantes.

➢ **¿Es seguro realizar llamadas confidenciales por videoconferencia?**

La mayoría de equipos de vídeo incorporan un sistema de cifrado que permite un alto nivel de seguridad en las conversaciones. El proceso de cifrado se efectúa automáticamente al iniciar una videoconferencia sin que el usuario tenga que realizar ajustes previos, y no afecta a la calidad de la videoconferencia.

➢ **¿Puedo conectar un PC a un equipo de vídeo?**

Algunas EMPRESAS

Aethra Telecommunications
www.aethra.com
ClearOne
www.clearone.com
Codian
www.codian.com
Ezenia! Incorporated
www.ezenia.com
Motion Media Technology
www.motion-media.com
Polycom
www.polycom.com
Radvision
www.radvision.com
Scotty Corporation
www.scottygroup.com
Sony
www.sonypcsone.com
StarView Communications
www.starviewvideo.com
Tandberg
www.tandberg.net
VBrick Systems, Inc.
www.vbrick.com
VCON
www.vcon.com
Vialta's
www.vialta.com
VTEL Products Corporation
www.vtel.com
Wind Currents Technology
www.videophoneconnection.com

un país en marcha

EUSKO JAURLARITZA GOBIERNO VASCO

Gobierno Vasco

El servicio de Video-conferencia actual permite disponer de una sala de reuniones con el servicio de videoconferencia ya incorporado. Este servicio que se encuentra ya operativo y es totalmente funcional, aporta todas las ventajas ya conocidas, como son por ejemplo el ahorro de costes económicos (ya que evita los desplazamientos), el ahorro de tiempo, etc. En este caso, si bien la reserva/solicitud de este servicio está restringida a unos usuarios, cualquier usuario del Gobierno Vasco, que por motivos de su trabajo lo necesite, puede hacer uso de este servicio. Actualmente el servicio de video-conferencia se puede utilizar entre salas ubicadas en centros del propio Gobierno y/o entre centros externos al mismo.

Puede conectar un PC al equipo de vídeo para compartir o mostrar informes recopilados en su ordenador personal a otros participantes de la videoconferencia. La conexión puede realizarse de varios modos dependiendo del equipo utilizado: se puede recurrir a una conexión por la red local, utilizar equipamiento adicional o emplear lo más sencillo, un cable que conecte directamente el equipo y el PC.

- **¿Puedo comunicar con un interlocutor y visualizar su presentación al mismo tiempo durante una videoconferencia?**

La ventaja del vídeo comparado con otros métodos de comunicación es la posibilidad de ver a la persona con quien se está comunicando. Existen soluciones en el mercado que permiten hoy en día visualizar simultáneamente presentaciones y participantes en uno o dos monitores; sin embargo, existen fabricantes que ofrecen además varios formatos para ver ambas imágenes en un único monitor (con todas las ventajas que ello implica) y sin deformar la imagen (especialmente útil en pantallas de formato 16:9) ni perder la resolución original (especialmente crítico en el caso de la resolución XGA de los PCs).

- **¿Puedo contactar con varios interlocutores durante una misma llamada?**

Sí, poder conectar varios puntos al mismo tiempo es uno de los mayores valores añadidos de la videoconferencia. Gracias a la funcionalidad de puente de multiconferencia que pueden incluir algunos equipos, se pueden conectar hasta 6 puntos de vídeo y 5 de audio durante una llamada presionando solamente un botón. También existen puentes de multiconferencia externos que permiten la conexión simultánea de más de 100 puntos. Este tipo de llamadas se denomina **multipunto**, y en ellas se pueden visualizar los participantes y la información que se esté comentando al mismo tiempo. Actualmente, no todos los fabricantes de equipos de videoconferencia disponen de puentes de multiconferencia internos que ofrecen las altas prestaciones de los puentes de videoconferencia externos.

- **¿Pueden participar en la misma multiconferencia equipos que se conecten por RDSI y equipos que se conecten sobre IP?**

Sí. Existen hoy día en el mercado equipos que permiten conectarse a distintos anchos de banda y utilizar distintos protocolos de vídeo y audio. Este último punto es especialmente importante si se mezclan en la misma multiconferencia equipos nuevos con equipos antiguos, ya que es posible que estos últimos no soporten los nuevos estándares, y si no se pueden mezclar protocolos, los participantes con equipos nuevos

trabajarían con menor calidad que la que tienen disponible.

➢ **Si todos mis equipos de videoconferencia trabajan sobre IP, ¿cómo puedo comunicarme con otros equipos que sólo tengan RDSI?**

Existen equipos para interconectar los dos mundos: los **gateways**[8]. Cuando un equipo IP quiere conectarse con otro RDSI, o viceversa, bastará con marcar un prefijo para indicarle al gateway que tiene que hacer la conversión; es como si realizas una llamada telefónica externa (fuera de la oficina), y tienes que marcar un prefijo para comunicar con el exterior.

"La mayoría de equipos de video incorporan un sistema de cifrado que permite un alto nivel de seguridad en las conversaciones."

➢ **¿Es necesario llamar a un equipo que trabaje sobre IP por su dirección IP, o tengo alguna otra alternativa?**

Para evitar tener que llamar a un equipo de videoconferencia IP por su dirección IP (lo cual para una persona supone una dificultad el recordar la dirección IP exacta), un equipo de infraestructura llamado **gatekeeper** puede asignar un número o alias a un equipo de videoconferencia, facilitando así las

llamadas entre equipos IP. Algunos equipos, hacen uso además de la que se conoce como "marcación URI" (nombres en lugar de números).

➢ **¿Puedo comunicarme con otros centros por IP si tengo que atravesar un firewall?**

Este también es un aspecto importante a tener en cuenta a la hora de valorar una solución de videoconferencia.

En estos momento existen en el mercado soluciones específicas para ello. Sin embargo, gracias a la tecnología desarrollada por algunos fabricantes para sus productos, éstos haciendo uso de los estándares existentes apenas hay que modificar la configuración del firewall.

➢ **¿Cómo puedo gestionar mis equipos y mi infraestructura de videoconferencia?**

Para gestionar la solución de videoconferencia existen herramientas software específicas desde las que no sólo pueden gestionarse los equipos, sino que también se pueden monitorizar las sesiones de videoconferencia, realizar diagnósticos sobre los equipos, actualizarlos remotamente, y mantener sus directorios de contactos, entre otras muchas posibilidades.

➢ **¿Puedo programar sesiones de videoconferencia con antelación?**

En algunos casos también existen herramientas software para la programación y reservas de recursos de videoconferencia (equipos e infraestructura), muy fáciles de utilizar y que dejan la tecnología oculta al usuario, incluso en el caso de sesiones multipunto.

➢ **¿Existen soluciones de videoconferencia específicas para ciertas aplicaciones?**

Existen soluciones de videoconferencia avanzadas (equipos físicos) que pueden facilitar aplicaciones adicionales para adaptar el equipo a necesidades específicas, como puede ser en el ámbito de la educación, emergencias y/o telemedicina.

➢ **¿Puedo realizar una videoconferencia entre mi teléfono móvil 3G y un equipo de videoconferencia?**

Sí. Dada la gran importancia que este tipo de tecnologías móviles están adquiriendo en los últimos meses (y sobretodo, la que se espera que tengan en el futuro más próximo) distintos fabricantes ya han desarrollado la tecnología y equipos necesarios para que esta comunicación sea posible.

DICCIONARIO

[8] **Gateway**: Pasarela que compatibiliza distintos medios de transmisión. Permite conectar entornos de red IP (H.323) a entornos RDSI (H.320) y viceversa

Otro elemento muy común en este mundo es la denominada Unidad de MultiConferencia (más conocida como **MCU**), la cual es la "pieza" que permite conectar simultáneamente más de dos puntos, para establecer reuniones de videoconferencia multipunto.

un país en marcha

EUSKO JAURLARITZA GOBIERNO VASCO

ALBOAN:

Departamento de Hacienda y Administración Pública

EUSKAL HERRIKO AGINTARITZAREN ALDIZKARIA

BOLETIN OFICIAL DEL PAIS VASCO

El Sistema de Información del BOPV

El pasado mes de octubre el Departamento de Hacienda y Administración Pública puso en producción la nueva versión de la aplicación P43, la cual mecaniza la Confección y Seguimiento del Boletín Oficial del País Vasco (BOPV). Como parte del plan de implantación, previamente a la puesta en marcha de la aplicación, se impartió un curso de formación a los usuarios de los distintos Departamentos y Organismos Autónomos del Gobierno Vasco que la solicitaron, asistiendo un total de 40 personas.

Entre todas las mejoras que proporciona esta nueva versión podemos destacar las siguientes:

- ✓ Es bilingüe en todos sus apartados (a nivel de interface).
- ✓ Permite a los usuarios externos al Gobierno realizar solicitudes vía Internet, permitiéndoles anexar documentos en diferentes formatos (imágenes, PDFs, etc.)
- ✓ Los usuarios solicitantes (tanto del Gobierno como externos), son informados vía correo electrónico sobre si su solicitud ha sido recepcionada, si ha sido publicada (informándole en este caso de la fecha de publicación), o bien, si ha sido anulada.
- ✓ Desde una solicitud ya publicada se permite acceder directamente al PDF que se encuentra almacenado en la Base de Datos documental del boletín.
- ✓ Se aporta una interface para que cualquier otra aplicación que se desarrolle en el Gobierno pueda realizar de forma automática solicitudes al boletín.

La aplicación que en esta ocasión os detallamos, forma parte de un Sistema de Información que agrupa las siguientes áreas:

1.-CONFECCIÓN Y SEGUIMIENTO

Este módulo/aplicación mecaniza en su totalidad el procedimiento establecido tanto para los usuarios de Publicación, como para los usuarios del Servicio del Boletín del Gobierno.

Actualmente existen usuarios repartidos por todos los Dptos y OO.AA. que hacen uso de esta parte del sistema, quedando abierta la posibilidad para que, vía Internet, usuarios externos a la Administración puedan solicitar publicaciones y hacer el seguimiento de las mismas.

Las funcionalidades más relevantes que gracias a este módulo puede realizar un solicitante son:

- Hacer una solicitud pudiendo anexar documentos de diferentes formatos.
- Consultar o buscar las solicitudes realizadas (pudiendo hacer uso de diferentes criterios).
- Recibir de forma automática, por correo electrónico, información de la recepción, publicación o anulación de sus solicitudes.

Por otra parte, el Servicio del boletín podrá:

- Recoger todas las solicitudes, informando al usuario/ solicitante del hecho.
- Estudiar y corregir los textos recibidos.
- Calificar, Traducir, Confeccionar el sumario, Generar los textos a publicar.
- Y por último enviar los textos a la imprenta.

Como dato adicional, indicar que se aporta un interface para que desde cualquier otra aplicación se puedan realizar solicitudes al boletín de forma automática.

2.-PUBLICACIÓN, CONSULTA Y SUSCRIPCIÓN

A finales de 1997, el Dpto. de Hacienda y Admón. Pública con el objeto de presentar una propuesta de optimización del sistema existente, realizó un estudio de la situación del acceso y difusión del BOPV. Siguiendo esta línea, en enero de 1998 se elaboró un documento en el que se especificaba su situación, señalando sus pros y contras, así como una propuesta de mejora.

Esta propuesta consistía en la **Creación de un sistema en Internet/Intranet (en Castellano y Euskera), con prestaciones completas de búsqueda a través de una Base de Datos documental, mediante la cual se pudiese acceder de forma integrada a la visualización y reproducción del boletín en su formato original, posibilitando el acceso tanto a información actual como retrospectiva.** Poco tiempo después, el Gobierno Vasco (a través de un acuerdo de Consejo de Gobierno) aceptó la propuesta y ordenó su desarrollo.

Dada la envergadura del proyecto, éste se dividió en tres partes:

A.- Recuperación de todos los boletines en castellano y euskera de toda la historia del Gobierno Vasco, lo cual abarca un periodo que va desde 1936 hasta el día de la fecha, y su posterior incorporación a una Base de Datos documental (tanto en formato texto como en PDF). El desarrollo de este apartado requirió de muchos recursos ya que hubo que recuperar información de formatos muy diferentes.

B.- Desarrollo e implantación de un sistema bilingüe de acceso a la Base de Datos documental a través de Internet/Intranet (siendo este aspecto un desarrollo novedoso para su tiempo).

C.- Desarrollo e implantación de la suscripción electrónica de difusión selectiva.

Como resultado del desarrollo e implantación de los tres apartados anteriores en estos momentos se cuenta con dos módulos:

➢ 2.1- Publicación y consulta

Las funcionalidades más significativas son:

- Incorporación de los boletines enviados por la imprenta a la Base de Datos documental (tanto en modo texto como en PDF).
- Asignación de descriptores a las disposiciones.
- Asignación de las concordancias normativas a las disposiciones.

En cuanto a las Consultas de los Boletines ya publicados, indicar que el menú de acceso permite consultar por último boletín, o bien por boletines más recientes (presentando en este caso los siete últimos), o eligiendo un año. Una vez elegido el boletín que se quiere consultar, la aplicación expone su sumario, y es entonces cuando seleccionando un elemento del mismo, se presenta la disposición bien en formato texto o en PDF.

También existen varias opciones para buscar un contenido concreto, pudiéndolo hacer por:

Búsqueda simple (donde se permite efectuar una búsqueda por texto libre. Se puede también buscar en todos los años y entonces sólo por texto libre). O bien, por *Búsqueda avanzada* (donde se permite realizar un filtro de las disposiciones que contengan un determinado texto que se encuentre bien en su texto o en su título. Además se puede seguir filtrando por: Órgano emisor, sección, rango, número de disposición, entre fechas de disposición).

➢ 2.2- Suscripción electrónica gratuita.

Uno de los servicios más demandados (y útil para el usuario externo -ciudadano- y/o empresas) es el de la suscripción electrónica gratuita; el cual permite a estos realizar la Solicitud por Internet indicando cuales son las materias sobre las que desea recibir información.

"Actualmente el BOPV cuenta con 6.755 suscriptores por vía electrónica."

Igualmente les permite modificar los datos de la suscripción, así como darse de baja del servicio.

A través de este módulo, **el Servicio del boletín**, puede realizar en primer lugar el Mantenimiento de las suscripciones recibidas, y en segundo lugar, el envío automático vía correo electrónico a los suscriptores (ciudadanos) de la información relativa a las disposiciones a las que éstos se han suscrito; comunicándoles las disposiciones que en el boletín del día se corresponden con las materias que había elegido, pudiendo consultarlas e imprimirlas desde el mismo correo en formato PDF.

Estadísticas: según reflejan los datos estadísticos obtenidos (hasta mediados de noviembre) son 6.755 los usuarios que por vía electrónica se han suscrito a este servicio. Estos suscriptores se reparten de la siguiente manera: Araba 876 (12,96%), Bizkaia 2.772 (41,03%), Gipuzkoa 2.551 (37,76%) y el Resto 556 (8,23%). Por idioma: Castellano 6.216 (92,02%). Euskera 539 (7,98%). Por ocupación: Administración Pública 1.229 (18,20%), Empresa privada 1.921 (28,44%), Particulares 3.605 (53,36%). Por perfiles o temas seleccionados: Contratación 1.471. Ayudas 821. Oposiciones 403, Disposiciones normativas 111, etc.

3.- SUSCRIPCIÓN AL BOPV EN PAPEL

Como curiosidad, indicar que si bien la suscripción en formato papel tiende a desaparecer (ya que el número de suscriptores ha visto reducido su número de forma significante en los últimos meses), a día de hoy todavía existen 899 suscripciones vigentes.

un país en marcha

EUSKO JAURLARITZA GOBIERNO VASCO

¡¡BREVES!!

LAS ESTADÍSTICAS SEGÚN GOOGLE

Google ha puesto en marcha recientemente un sistema de **estadísticas** llamado **"Google Analytics"**, cuyo principal objetivo es dar un valor añadido a los usuarios de AdWords (y clientes de Google). El Analytics esta basado en Urchin (empresa adquirida por Google la pasada primavera). En estos momentos Google ofrece este servicio totalmente gratis para sitios web que sirvan menos de 5 millones de páginas al mes o sean clientes de AdWords.

Para poder hacer uso de este nuevo servicio, únicamente es necesario disponer de una cuenta de Google en Gmail. Posteriormente sólo se tiene que copiar y pegar un código *JavaScript* en todas las páginas que queramos que el servicio registre y esperar 12 horas para poder empezar a ver los informes.

Los informes (que están **orientados a 3 perfiles**: ejecutivo, técnico de marketing y webmaster) ofrecen respuestas claras y rápidas en un formato visual de fácil comprensión. Estos análisis nos permiten saber por ejemplo de dónde provienen nuestras visitas, qué enlaces proporcionan más tráfico, qué páginas están viendo los visitantes, desde qué población/país nos están visitando, cuánto tiempo permanecen en nuestro sitio, qué productos comerciales se han vendido, así como las versiones del navegador, su plataforma, resoluciones de pantalla, colores, idioma, versión flash, java, velocidad de conexión, etc.

Gracias a que "Google Analytics" está integrado en AdWords, nos proporciona información muy relevante sobre cada una de las palabras clave que hemos contratado en AdWords: conocer qué palabras clave atraen a nuestros clientes potenciales a nuestra web, etc. pudiendo de esta forma mejorar el contenido del sitio y optimizar el texto e imágenes de las campañas publicitarias.

El principal inconveniente que actualmente presenta el sistema es que no muestra estadísticas en tiempo real (se actualizan cada 12 horas).

http://adwords.google.es

LAS MEMORIAS DEL FUTURO

Durante 40 años hemos visto cómo las densidades de la memoria se han duplicado cada 18 ó 24 meses, mientras que sus precios permanecían casi fijos (reduciendo cada vez el coste por bit a la mitad).

Queriendo dar un paso más en esta constante evolución, actualmente los expertos estudian la manera de desarrollar una **tecnología universal** para memorias que podría reemplazar en un futuro a las actualmente existentes.

Esa nueva tecnología cambiaría la forma en que se diseñan los ordenadores (ya que una **RAM no volátil** permitiría a los PCs apagarse y encenderse de forma casi instantánea).

A día de hoy las tecnologías más desarrolladas son:

- La **FRAM** (RAM Ferroeléctrica): consiste en una RAM no volátil, que al estar basada en "puntos cuánticos", utiliza menos energía y escribe con más rapidez que DRAM o Flash, además dispone de una larga duración. Su único inconveniente es que es mucho más cara por bit que DRAM.
- La **MRAM** (Magnetoresistiva RAM): es una memoria rápida y no volátil que ofrece una combinación de alta velocidad, gran duración y densidad razonable. Pueden producirse casi con la misma densidad y coste por bit que la memoria flash.

Las tecnologías menos desarrolladas son:

- La **PCM** (Memoria de Cambio de Fase): es no volátil y mucho más rápida que flash (aunque es más lenta que SRAM). Además, para ser competitiva con DRAM, tendría que soportar escrituras ilimitadas.
- La **PMPm** (Programmable Metallization Cell memory): es una alternativa a DRAM no volátil, que utiliza menos energía y ofrece una mayor densidad que DRAM.

Sin embargo, y según algunos expertos, esta tecnología universal puede tardar en llegar entre 10 y 15 años, incluso le será muy difícil el mejorar algunos atributos de las tecnologías actuales. Por eso, se estima que probablemente no podrán competir en el campo del menor coste por bit (al contrario que la DRAM) o con la rapidez de la SRAM, lo que hará que inevitablemente se queden en el espacio que hay entre ambas.