Especial CeBIT

Marzo
2006

Agustín López

Ing. Informático

Auditor BS7799 certificado por BSI

www.iso27000.es

ISO27000.es estuvo en la jornada inaugural del CeBIT, que celebró en el presente año 2006 su vigésima edición en Hannover (Alemania).

Tras pasar de largo varios aparcamientos ya completos, conseguimos finalmente refugiarnos de un tiempo frío y desapacible, y que contrasta con el que vivimos el año pasado, en el recinto que alberga los 27 pabellones de exposición y centro de convenciones.

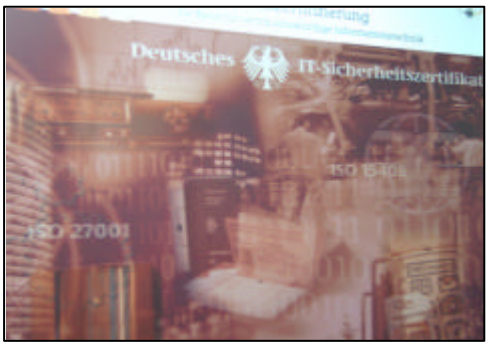
Nos dirigimos en primer lugar al pabellón número 7 que alberga el Centro para la Seguridad de la Información del CEFIS y donde, como ya anunciamos en www.iso27000.es, se ofrecen distintas soluciones avanzadas en seguridad de la información e infraestructuras dedicadas.

The Secure Computer Center

Llegamos a tiempo para el inicio de la visita guiada a esta exposición, ubicada en una amplia esquina y en la que se han aunado los esfuerzos de distintas firmas presentes en el CeBIT. El objetivo es presentar las últimas innovaciones en seguridad que aseguren los accesos de las personas exclusivamente autorizadas a la sala así como alcanzar la disponibilidad y rendimientos máximos de los sistemas alojados y en las condiciones más adversas.

BSI

Tras el bombardeo de datos técnicos, iniciamos una ronda por los pasillos, que nos conduce al amplio expositor de la BSI de Alemania.



La *Bundesamt für Sicherheit in der Informationstechnik* -Oficina Federal para la Seguridad de la Información- fue fundada en 1991 y es un cuerpo especializado neutral e independiente integrado en el Ministerio del Interior (no confundir con *British Standards Institution*).

El visitante se topa con la norma ISO 27000 en los paneles de la BSI, además de los principales hitos necesarios para acceder una organización a la certificación ISO 27001.

Existe una variada selección de información impresa en diferentes folletos de concienciación (en alemán e inglés), aunque reducida para la amplitud del espacio del expositor, pues ha sido acertadamente sustituida por un CD-ROM gratuito donde se recogen (con bastante acierto, como hemos podido posteriormente comprobar) explicaciones con guías prácticas para el uso de aplicaciones y tratamiento de los datos privados de los usuarios.

Asimismo, nos hemos llevado en el bolsillo otro CD-ROM de libre distribución con los contenidos, prácticamente completos y en alemán/inglés, del portal www.bsi.bund.de para poder consultarlos rápidamente en cualquier sitio.

La Oficina presentaba una imagen moderna y alejada del tópico burocrático que se pudiera en principio pensar, aprovechando el espacio real disponible para llamar la atención sobre la distribución gratuita y contenidos de los CDs, además de atender las consultas del público en general.

Para los más interesados, estaba disponible en uno de los ordenadores la última versión 3.1 de la herramienta GSTOOL para labores de auditoría. GSTOOL es un software que proporciona soporte adecuado para la confección de inventarios de activos, estado de cumplimiento actualizado de la normativa de la BSI en todos sus puntos básicos, manejo de documentos de auditoría, así como módulos para la estimación y evaluación de costes para las medidas adoptadas.

TUEV

Salimos del BSI y nos paramos ahora en TUEV, empresa de servicios de inspección técnica y control de calidad, conocida en España principalmente por sus actividades en el sector de Automoción, aunque también se dedica a la evaluación de sistemas ISO14000, OHSAS 18001, ISO 9000 así como BS7799.

Encontramos aquí también información variada sobre normas como BS15000, certificación, seguridad de la información, auditoría y cursos de formación sobre ITIL, entre otros.

Nos confirman que la aparición de la normativa ISO 27001 permitirá un crecimiento en los próximos años tanto de la norma ISO como de las certificaciones propias de BSI Alemania, en función del ámbito regional o europeo/internacional de las propias empresas.

Podríamos encontrar similitudes con la situación en España de la norma UNE 71502 respecto a ISO 27001, aunque los certificados de la BSI tienen en Alemania un peso importante por su trayectoria de 15 años e implicación en la difusión de las prácticas adecuadas para la seguridad de la información y continuidad de negocio en empresas tanto grandes como pequeñas.

BSI también es un mecanismo importante en la promoción de “SecurITy made in Germany” como extensión de la marca de calidad que tradicionalmente identifica a los productos que se producen en este país y se exportan al resto del mundo.

Certificaciones

A lo largo de los diferentes expositores del CeBIT hemos comprobado que las certificaciones empiezan a ser claramente utilizadas como distintivo diferenciador de la competencia y hemos localizado algunos puntos en los que estaban pegados incluso en varias columnas bien a la vista, además de en las mesas de atención a visitantes.

Así mismo, la información de la memoria que recoge las actividades de varias empresas y en distintos sectores, relacionan ya claramente las "buenas prácticas" con los nombres y apellidos de BS 7799, ISO 17799 e ISO 27001.

Salimos del CEFIT

Y hemos aprovechado para adentrarnos en un recorrido a través de diversos pabellones y áreas tecnológicas aquí reunidas.

Una colección de Apple, Commodore, MSX, Sinclair ZX81, ZUSE Z 25 de 1961 o un Digital PDP-8, precede a la pasarela de ropa futurista que nos abre el paso a demostraciones en robótica.

Intentamos atajar atravesando una demostración de gafas que mezclan imagen real y sintética pero quedamos bloqueados por un corrillo de prensa, que graba las habilidades paranormales de dos sujetos que controlan un sistema de teclado en el monitor mediante un casco mallado repleto de electrodos.

La BSI alemana reaparece ante nuestros ojos, esta vez fomentando la calidad de los procesos para el desarrollo de proyectos, como la informatización de la administración pública y el tratamiento burocrático de documentación oficial mediante nuevos medios técnicos. Encontramos abundante información sobre el pasaporte electrónico, que se espera para 2007.

Cruzamos el continente asiático formado por pasillos repletos de todo tipo de electrónica, colores y formas y hacemos una parada estratégica para tomar un café, recuperar fuerzas en las piernas y presenciar una charla titulada "espionaje en Alemania".

Lejos de la frivolidad o el espectáculo fácil que se podría esperar, nos presentan el ejemplo de la incorporación de un nuevo empleado a su puesto de trabajo como factor suficiente para que se activen la curiosidad mediante los sentidos de la vista y oído en los compañeros para registrar información sobre el origen, las funciones y la amenaza que pueda representar la nueva incorporación.

Pero las estadísticas indican que con frecuencia cada vez mayor y gracias a los nuevos medios disponibles en el trabajo, crece significativamente el uso de prácticas no éticas e ilegales.

La información se trata de obtener directamente del disco duro o correo del nuevo colaborador con el objeto de confirmar y ampliar los conocimientos sobre sus relaciones laborales y personales con el resto de la plantilla e identificar posibles puntos débiles y amenazas para la carrera profesional propia dentro de la compañía.

De vuelta a los pasillos y reflexionando aún sobre los límites al que las personas somos capaces de llegar en estas situaciones, apuramos las espumas del café en el sector financiero junto a un cajero automático diseccionado, que cruza con un pasillo de promoción de conexiones seguras a servicios de banca en línea mediante medidas de encriptación y biométricas.

Consultamos algunas agencias de auditoría y consultoría a entidades financieras que ofrecen sus servicios en relación a las buenas prácticas de BS 7799, ISO 17799 e ISO 27001 y recorremos el trecho que nos queda, justo a tiempo para presenciar la conferencia "Aplicaciones Web: ¿Puertas traseras de los negocios?" que se celebra allí donde empezamos, en el recinto del CEFIS.

La presentación del Sr. Breitschaft nos descubre un *firewall* avanzado que permite, entre otras cosas, aplicar filtros destinados a evitar el mal mayor de la inyección de código SQL, así como la comprobación de certificados de los clientes implicados en las transacciones con los servicios activos de los servidores.

Se remarca en la presentación que esta es una solución que trata de minimizar dentro de lo posible las consecuencias de las malas prácticas en los proyectos de desarrollo, que se preocupan del aspecto de la seguridad de la información cuando el producto ya está al final de su ciclo de desarrollo o incluso en producción y donde una labor de reprogramación dispara los costes y disponibilidad asociados al producto.

La seguridad no es un producto y debe ser tenida en cuenta desde el principio en el desarrollo de cualquier proyecto (aprovechamos para hacer referencia al artículo "seguridad opcional, seguridad integral" de *ISO27000.es*).

En esencia, continúa la centralización de las bases de datos como estrategia de ahorro en costes de infraestructura y gestión, se amplían las posibilidades de conexión de los usuarios que garanticen su acceso a todo tipo de información de trabajo o de ocio y se protegen las transmisiones de posibles intervenciones mediante sistemas avanzados de encriptación y cifrado.

Por otra parte, la biometría tratará de evitar la suplantación de identidad de las personas y perfiles autorizados.

Los fabricantes de hardware nos han vendido la mejor de las calidades en sus componentes, acompañada de más y mejores sistemas de redundancia que garanticen su disponibilidad y recuperación inmediata a la actividad.

Los desarrolladores de software han incorporado a su discurso promocional de los productos funcionalidades relacionadas con la gestión restringida del acceso a los datos por los usuarios de los sistemas.

El sector de comunicaciones promete conectividad desde cualquier parte desde más terminales, aunque la fiebre inalámbrica ha despertado una conciencia en los usuarios “de ser escuchados” que, parece ser, no existe psicológicamente con la misma intensidad con el uso del hilo.

Las numerosas demostraciones de hacking en vivo por parte de los vendedores de productos relacionados con la seguridad y encriptación se han encargado adecuadamente de desnudar las agendas personales de aquellos visitantes que aún mantienen las configuraciones por defecto en sus dispositivos, para descubrir o reafirmar este sentimiento y la consiguiente necesidad de sus productos.

En general, nos da la impresión de que un público más o menos escarmentado ha llegado por fin a un estadio de madurez tecnológico en el que, tanto los linimentos tecnológicos multiuso de rápida y fácil instalación como las cajas mágicas de retornos de inversión sorprendentes no valen ya, por sí mismos, como argumentos válidos de compra.

Por el contrario, las soluciones presentadas este año se recomiendan instalar allí donde les dejan espacio los marcos definidos por los análisis de necesidades y seguridad previos, como camino lógico y racional para garantizar la efectividad de las inversiones.